aws

Manual do usuário

Amazon Elastic Compute Cloud

Amazon Elastic Compute Cloud: Manual do usuário

Table of Contents

O que é o Amazon EC2? ... 1
Atributos ... 1
Serviços relacionados ... 2
Acesso ao EC2 ... 4
Definição de preço ... 5
Estimativas, faturamento e otimização de custos ... 6
Recursos ... 7
Tutorial de conceitos básicos ... 8
Etapa 1: executar uma instância ... 10
Etapa 2: conectar-se à instância ... 11
Etapa 3: limpar a instância ... 15
Próximas etapas ... 15
Práticas recomendadas ... 17
Imagens de máquina da Amazon ... 20
Usar uma AMI ... 21
Criar sua própria AMI ... 21
Comprar, compartilhar e vender AMIs ... 22
Cancelar o registro da AMI ... 22
Amazon Linux 2023 e Amazon Linux 2 ... 23
AMIs Windows ... 23
Tipos de AMI ... 24
Permissões de execução ... 24
Armazenamento para o dispositivo raiz ... 25
Tipos de virtualização ... 30
Modos de inicialização ... 33
Executar uma instância ... 34
Parâmetro do modo de inicialização da AMI ... 42
Modo de inicialização do tipo de instância ... 44
Modo de inicialização da instância ... 45
Modo de inicialização do sistema operacional ... 47
Definir modo de inicialização da AMI ... 50
Variáveis UEFI ... 55
UEFI Secure Boot ... 56
Encontrar uma AMI ... 71

Encontrar uma AMI usando o console do Amazon EC2 ... 72
Localizar uma AMI usando o AWS CLI ... 74
Localizar uma AMI usando o AWS Tools for Windows PowerShell ... 74
Encontrar uma AMI usando um parâmetro do Systems Manager ... 75
Encontrar as AMIs mais recentes usando o Systems Manager ... 79
Mais informações para encontrar AMIs ... 81
AMIs compartilhadas ... 81
Provedor verificado ... 81
Encontrar AMIs compartilhadas ... 82
Tornar um AMI pública ... 87
Compartilhar uma AMI com organizações e UOs ... 96
Compartilhar uma AMI com contas específicas da AWS ... 107
Cancelar o compartilhamento de uma AMI com sua conta ... 112
Usar marcadores ... 114
Diretrizes para AMIs em Linux compartilhadas ... 115
AMIs pagas ... 121
Vender sua AMI ... 122
Localizar uma AMI paga ... 123
Comprar uma AMI paga ... 125
Obter o código do produto para sua instância ... 125
Usar suporte pago ... 126
Faturas para AMI pagas e compatíveis ... 127
Gerenciar suas assinaturas do AWS Marketplace ... 127
Ciclo de vida da AMI ... 128
Criar uma AMI ... 128
Modificar uma AMI do ... 202
Copiar um AMI ... 203
Armazenar e restaurar uma AMI ... 214
Descontinuar uma AMI ... 224
Desabilitar uma AMI ... 233
Arquivar snapshots da AMI ... 239
Cancelar o registro de uma AMI (excluir a AMI) ... 239
Automatizar o ciclo de vida da AMI com suporte do EBS ... 249
Criptografia da AMI ... 249
Cenários de execução de instância ... 250
Cenários de cópia de imagem ... 253

Monitorar eventos da AMI ... 256
Eventos da AMI ... 257
Criar uma regra do Amazon EventBridge ... 260
Noções básicas sobre o faturamento da AMI ... 263
Campos de faturamento da AMI ... 264
Localizar informações de faturamento de AMI ... 266
Verificar cobranças da AMI em sua fatura ... 269
Cotas de AMI ... 269
Solicitar um aumento de cota para AMIs ... 271
Instâncias ... 272
Instâncias e AMIs ... 272
Instâncias ... 273
AMIs ... 276
Tipos de instância ... 277
Tipos de instâncias disponíveis ... 278
Especificações de hardware ... 279
Tipos de virtualização de AMI ... 281
Localizar um tipo de instância do ... 282
Obter recomendações ... 284
Alterar o tipo de instância ... 292
Instâncias expansíveis ... 303
Instâncias de GPU ... 358
Instâncias Mac ... 369
Considerações ... 371
Prontidão da instância ... 372
AMIs do macOS do EC2 ... 373
EC2 MacOS Init ... 373
Amazon EC2 System Monitor para macOS ... 373
Recursos relacionados ... 374
Iniciar uma instância Mac ... 374
Conectar-se a instâncias Mac ... 377
Atualizar o sistema operacional e o software em instâncias Mac ... 380
Aumente o tamanho de um volume do EBS na instância do Mac ... 388
Interromper e encerrar a instância do Mac ... 389
Encontrar versões macOS compatíveis para o host dedicado ... 390
Assinar notificações de AMI do macOS ... 391

Recuperar IDs de AMI para macOS ... 393
Notas de lançamento das AMIs do EC2 para macOS ... 394
Otimização de EBS ... 396
Otimizados para EBS por padrão ... 397
Suporte à otimização do EBS ... 466
Obtenha a máxima performance ... 468
Exibir tipos de instâncias compatíveis com a otimização do EBS ... 469
Habilitação da otimização do EBS na execução ... 470
Habilitar a otimização do EBS para uma instância existente ... 471
Opções de compra de instância ... 472
Determinar o ciclo de vida da instância ... 474
Instâncias sob demanda ... 475
Reserved Instances ... 478
Instâncias spot ... 550
Dedicated Hosts ... 655
Dedicated Instances ... 719
Reservas de capacidade ... 728
Ciclo de vida da instância ... 817
Execução da instância ... 820
Início e interrupção da instância ... 820
Hibernação da instância ... 821
Reinicialização da instância ... 822
Encerramento de instância ... 822
Diferenças entre reinicialização, interrupção, hibernação e encerramento ... 823
Executar ... 825
Interromper e iniciar ... 913
Hibernar ... 922
Reinicializar ... 954
Encerrar ... 956
Retirada ... 967
Resiliência de instância ... 972
Trabalhar com metadados de instância ... 982
Usar IMDSv2 ... 983
Configurar as opções de metadados da instância ... 993
Recuperar metadados da instância ... 1020
Trabalhar com dados do usuário da instância ... 1042

Executar comandos no lançamento ... 1046
Recuperar dados dinâmicos ... 1073
Categorias de metadados da instância ... 1074
Exemplo do Linux: valor do índice de execução da AMI ... 1092
Documentos de identidade da instância ... 1097
Perfis de identidade da instância ... 1163
Conexão com a instância do EC2 ... 1164
Conecte-se à sua instância do Linux ... 1165
Conectar-se à sua instância do Windows do ... 1239
Conectar-se usando o Gerenciador de sessões ... 1252
Conectar usando o EC2 Instance Connect Endpoint ... 1254
Conectar sua instância a um recurso ... 1281
Identificar instâncias do ... 1326
Inspecione o UUID do sistema ... 1326
Inspecione o identificador de geração da máquina virtual do sistema ... 1328
Gerenciamento das configurações do sistema ... 1334
Definir o horário ... 1334
Controle do estado do processador ... 1357
Otimizar as opções de CPU ... 1359
AMD SEV-SNP ... 1484
Adição de componentes do sistema do Windows ... 1490
Gerenciamento de usuários do sistema do Linux ... 1496
Definição da senha do administrador do Windows ... 1500
Gerenciamento de drivers de dispositivo ... 1502
Instalar drivers NVIDIA ... 1502
Instalar drivers AMD ... 1539
Drivers PV do Windows ... 1549
Drivers de NVMe da AWS do Windows ... 1585
Configuração da instância do Windows ... 1594
Definição de agentes de inicialização do Windows ... 1594
Uso do EC2 Fast Launch para o Windows ... 1766
Uso de aceleradores Elastic Graphics no Windows ... 1791
Instalação do WSL no Windows ... 1813
Atualizar instâncias do Windows ... 1815
Realizar uma atualização no local ... 1816
Realizar uma atualização automatizada ... 1820

Migração para um tipo de instância da geração atual ... 1832
Migrar o Microsoft SQL Server do Windows para o Linux ... 1842
Solucionar problemas de uma atualização ... 1842
Frotas ... 1844
EC2 Fleet ... 1845
Limitações da Frota do EC2 ... 1847
Instâncias expansíveis ... 1847
Tipos de solicitação da Frota do EC2 ... 1848
Estratégias de configuração da Frota do EC2 ... 1876
Trabalhar com Frotas do EC2 ... 1916
Frota spot ... 1944
Tipos de solicitação da frota spot ... 1944
Estratégias de configuração de frota spot ... 1945
Trabalhar com frotas spot ... 1985
Métricas do CloudWatch para frota spot ... 2019
Escalabilidade automátia para frota spot ... 2023
Monitorar eventos da frota ... 2033
Tipos de evento de Frota do EC2 ... 2034
Tipos de evento de frota spot ... 2040
Criar uma regra de EventBridge ... 2047
Tutoriais ... 2058
Tutorial: Usar a Frota do EC2 com ponderação de instâncias ... 2059
Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal . 2063
Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas 2064
Tutorial : iniciar instâncias em blocos de capacidade ... 2071
Tutorial: Usar frota spot com ponderação de instâncias ... 2073
Exemplos de configuração ... 2077
Exemplos de configuração de Frota do EC2 ... 2077
Exemplos de configuração de frota spot ... 2097
Quotas da frota ... 2116
Solicitar um aumento de cota para a capacidade pretendida ... 2118
Monitor ... 2119
Monitoramento automático e manual ... 2120
Ferramentas de monitoramento automatizadas ... 2121
Ferramentas de monitoramento manual ... 2122
Melhores práticas de monitoramento ... 2123

Monitorar o status das instâncias ... 2124
Verificações de status de instâncias ... 2124
Eventos de alteração de estado ... 2133
Eventos agendados ... 2136
Monitorar instâncias usando o CloudWatch ... 2169
Alarmes de instância ... 2169
Habilitar o monitoramento detalhado ... 2170
Listar métricas disponíveis ... 2173
Baixar e configurar o atendente do CloudWatch ... 2199
Obter estatísticas para métricas ... 2203
Representar métricas em gráficos ... 2213
Criar um alarme ... 2214
Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância ... 2215
Automatizar usando o EventBridge ... 2229
Tipos de eventos do Amazon EC2 ... 2230
Log chamadas de API usando o CloudTrail ... 2231
Informações sobre a API do Amazon EC2 no CloudTrail ... 2231
Compreensão das entradas do arquivo de log da API do Amazon EC2 ... 812
Auditar conexões por meio do EC2 Instance Connect ... 2234
Monitorar as aplicações .NET e SQL Server ... 2235
Acompanhar seu uso do nível gratuito ... 2236
Redes ... 2240
A VPC abrange as zonas de disponibilidade e a zona Wavelength. ... 2241
Regiões ... 2242
Zonas de disponibilidade ... 2248
zonas locais ... 2253
Zonas do Wavelength ... 2256
AWS Outposts ... 2259
Endereçamento IP de instâncias ... 2261
Endereços IPv4 privados ... 2262
Endereços IPv4 públicos ... 2263
Otimização de endereço IPv4 público ... 2264
Endereços IP elásticos (IPv4) ... 2266
Endereços IPv6 ... 2266
Trabalhar com os endereços IPv4 para as instâncias ... 2268
Trabalhar com os endereços IPv6 para as instâncias ... 2271

Vários endereços IP ... 2274
Diversos endereços IPv4 privados para o Windows ... 2284
Hostnames de instância do EC2 ... 2291
Endereços locais de link ... 2291
Tipos de nome de host de instância ... 2292
Tipos de nomes de host do EC2 ... 2292
Onde encontrar o nome do recurso e o nome de IP ... 2294
Como decidir se deseja escolher o nome do recurso ou o nome de IP ... 2296
Modificar configurações de tipo de nome de host e nome de host DNS ... 2297
Traga seus próprios endereços IP ... 2299
Definições BYOIP ... 2300
Requisitos e cotas ... 2301
Pré-requisitos de integração ... 2302
Integração do BYOIP ... 2310
Trabalhar com o intervalo de endereços ... 2315
Validar o BYOIP ... 2316
Disponibilidade regional ... 2321
Disponibilidade da zona local ... 2321
Saiba mais ... 2322
Endereços IP elásticos ... 2322
Definição de preço de endereços IP elásticos ... 2322
Noções básicas sobre endereços IP elásticos ... 2322
Trabalhar com endereços IP elásticos ... 2324
Cota de endereços IP elásticos ... 2340
Interfaces de rede ... 2341
Conceitos básicos da interface de rede ... 2342
Placas de rede ... 2344
Endereços IP por interface de rede por tipo de instância ... 2346
Trabalhar com interfaces de rede ... 2348
Melhores práticas para configurar interfaces de rede ... 2360
Cenários para interfaces de rede ... 2362
Interfaces de rede gerenciadas pelo solicitante ... 2366
Atribuir prefixos ... 2368
Largura de banda de rede ... 2385
Largura de banda disponível da instância ... 2385
Monitorar largura de banda da instância ... 2388

Redes avançadas ... 2389
Suporte a redes avançadas ... 2389
Elastic Network Adapter (ENA) ... 2390
ENA Express ... 2421
Intel 82599 VF ... 2444
Métricas de performance da rede ... 2457
Solução de problemas do ENA no Linux ... 2467
Solução de problemas do driver do ENA do Windows ... 2482
Aprimore a latência de rede para instâncias do Linux ... 2504
Considerações sobre a performance do Nitro ... 2508
Otimização do desempenho da rede em instâncias do Windows ... 2516
Elastic Fabric Adapter ... 2518
Conceitos básicos de EFA ... 2519
Interfaces e bibliotecas compatíveis ... 2520
Tipos de instâncias compatíveis ... 2520
Sistemas operacionais compatíveis ... 2522
Limitações de EFA ... 2523
Preços do EFA ... 2523
Começar a usar instâncias P5 e EFA ... 2523
Conceitos básicos do EFA e MPI ... 2528
Conceitos básicos do EFA e NCCL ... 2545
Trabalhar com EFA ... 2575
Monitorar um EFA ... 2579
Verificar o instalador EFA usando uma soma de verificação ... 2580
Topologia da instância ... 2592
Como funciona ... 2593
Pré-requisitos ... 2596
Exemplos ... 2598
Grupos de posicionamento ... 2610
Estratégias de posicionamento ... 2611
Regras e limitações ... 2615
Trabalho com grupos de posicionamento ... 2618
Compartilhar um grupo de posicionamento ... 2631
Grupos de posicionamento no AWS Outposts ... 2638
Conexão MTU ... 2639
Frames jumbo (9001 MTU) ... 2640

Path MTU Discovery ... 2641
Verificar o MTU do caminho entre dois hosts ... 2642
Verificação da MTU para a instância ... 2643
Definição da MTU para a instância ... 2645
Solução de problemas ... 2648
Nuvens privadas virtuais ... 2648
Suas VPCs padrão ... 2648
Criar VPCs adicionais ... 2649
Acessar a Internet diretamente de suas instâncias ... 2650
Sub-redes compartilhadas ... 2651
Sub-redes somente IPv6 ... 2651
Segurança ... 2652
Proteção de dados ... 2653
Segurança de dados do Amazon EBS ... 2654
Criptografia em repouso ... 2654
Criptografia em trânsito ... 2656
Segurança da infraestrutura ... 2658
Isolamento de rede ... 2658
Isolamento em hosts físicos ... 2659
Controlar o tráfego de rede ... 2659
Resiliência ... 2662
Validação de conformidade ... 2663
Identity and Access Management ... 2664
Acesso à rede para a instância ... 2665
Atributos de permissões do Amazon EC2 ... 2665
IAM e Amazon EC2 ... 2666
Políticas do IAM ... 2667
Políticas gerenciadas pela AWS ... 2738
Funções do IAM ... 2742
AWS PrivateLink ... 2760
Criar um VPC endpoint de interface ... 2761
Criar uma política de endpoint ... 2761
Gerenciamento de atualizações ... 2763
Práticas recomendadas de segurança para instâncias do Windows ... 2763
Práticas recomendadas de segurança de alto nível ... 2763
Gerenciamento de atualizações ... 2765

Gerenciamento de configuração ... 2767
Gerenciamento de alterações ... 2768
Auditoria e responsabilidade para instâncias do Windows do Amazon EC2 ... 2769
Pares de chaves ... 2770
Criar um par de chaves ... 2771
Marcar um par de chaves ... 2780
Descrever seus pares de chaves ... 2782
Excluir o par de chaves ... 2791
Adição ou remoção de uma chave pública na instância do Linux ... 2792
Verificar a impressão digital ... 2794
Grupos de segurança ... 2797
Regras de grupos de segurança ... 2798
Acompanhamento da conexão ... 2801
Grupos de segurança padrão e personalizados ... 2807
Trabalhar com grupos de segurança ... 2809
Regras de grupo de segurança para diferentes casos de uso ... 2819
NitroTPM ... 2827
Considerações ... 2828
Pré-requisitos ... 2828
Criar uma AMI Linux para suporte ao NitroTPM ... 2830
Verifique se a AMI está habilitada para o NitroTPM ... 2831
Habilitar ou interromper o uso do NitroTPM em uma instância ... 2832
Recuperar a chave pública de endosso ... 2834
Credential Guard para instâncias do Windows ... 2836
Pré-requisitos ... 2836
Inicialização de uma instância compatível ... 2837
Desabilitação da integridade da memória ... 2838
Ativação do Credential Guard ... 2839
Verificação se o Credential Guard está em execução ... 2841
Armazenamento ... 2843
Amazon EBS ... 2844
Armazenamento de instâncias ... 2845
Volume de armazenamento de instâncias e vida útil dos dados ... 2846
Volumes de armazenamento de instâncias ... 2849
Adicionar volumes de armazenamento de instâncias ... 2851
Volumes de armazenamento de instâncias SSD ... 2858

Volumes de troca de armazenamento de instância para instâncias do Linux 2862
Otimização do desempenho do disco em instâncias do Linux 2866
Armazenamento de arquivos 2868
Amazon S3 2868
Amazon EFS 2871
Amazon FSx 2875
Amazon File Cache 2881
Limites de volumes de instância 2881
Limites de volume para instâncias criadas no Nitro System 2882
Limites de volume para instâncias baseadas em Xen 2884
Volume do dispositivo raiz 2886
Tipo do volume de raiz 2886
Escolha de uma AMI do Linux por tipo de volume raiz 2889
Determinação do tipo de dispositivo raiz da instância do Linux 2890
Alterar o volume raiz para persistir 2891
Alterar o tamanho inicial do volume raiz 2895
Substituir um volume raiz 2896
Nomes de dispositivos 2908
Nomes de dispositivos disponíveis 2909
Considerações sobre nomes de dispositivos 2911
Mapeamentos de dispositivos de blocos 2913
Conceitos de mapeamento de dispositivos de blocos 2913
Mapeamento de dispositivos de blocos da AMI 2917
Mapeamento de dispositivos de blocos de instância 2921
Mapear discos para volumes 2929
Listar volumes do NVMe 2931
Listar volumes 2936
Snapshots do EBS do VSS 2945
O que é o VSS? 2946
Pré-requisitos 2948
Criar snapshots do VSS 2964
Solucionar problemas de snapshots do EBS baseados no Windows VSS 2976
Restaurar volumes por meio de snapshots do VSS 2981
Histórico de versões 2981
Prevenção de gravação interrompida para instâncias do Linux 2985
Definição de preço 2986

Tamanhos de blocos e alinhamentos de limites de blocos compatíveis ... 2986
Requisitos ... 2987
Verifique o suporte e a configuração de prevenção de gravação interrompida ... 2988
Configure sua pilha de software para evitar gravações interrompidas ... 2990
Recursos e tags ... 2992
Lixeira ... 2992
Como funciona? ... 2993
Atributos suportados ... 2994
Considerações ... 2995
Cotas ... 2998
Serviços relacionados ... 2998
Definição de preço ... 2999
Permissões obrigatórias do IAM ... 2999
Trabalhar com regras de retenção ... 3004
Trabalhar com recursos na Lixeira ... 3019
Monitorar a Lixeira ... 3030
Localizações de recursos ... 3049
IDs de recursos ... 3051
Listar e filtrar seus recursos ... 3052
Etapas do console ... 3052
Etapas da CLI e da API ... 3059
Visão global (entre regiões) ... 3062
Visualização Global ... 3062
Marcar com tag os recursos do ... 3065
Conceitos Básicos de Tags ... 3066
Marcar com tag os recursos do ... 3067
Restrições de tags ... 3072
Gerenciamento de tags e acesso ... 3073
Marcar com tag recursos para faturamento ... 3073
Trabalhar com tags usando o console ... 3074
Trabalhar com tags usando a linha de comando ... 3080
Trabalho com tags de instância em metadados de instância ... 3085
Adicionar tags a um recurso usando o CloudFormation ... 3088
Service Quotas ... 3089
Visualizar as cotas atuais ... 3090
Solicitar um aumento ... 3091

Restrição para e-mails enviados usando a porta 25 3091
Solução de problemas 3092
Problemas comuns com instâncias do Windows 3092
Os volumes do EBS não são inicializados no Windows Server 2016 e 2019 3093
Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM) 3094
A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado 3097
Não foi possível obter o resultado do console 3098
Windows Server 2012 R2 não disponível na rede 3098
Colisão de assinatura em disco 3099
Mensagens comuns com instâncias do Windows 3100
"A senha não está disponível" 3101
"A senha ainda não está disponível" 3102
"Não é possível recuperar a senha do Windows" 3102
"Esperando o serviço de metadados" 3102
"Não é possível ativar o Windows" 3107
"O Windows não é genuíno (0x80070005)" 3109
"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença" ... 3109
“Algumas configurações são gerenciadas pela sua organização” 3110
Solucionar problemas de execução 3110
Nome de dispositivo inválido 3111
Limite de instâncias excedido 3112
Capacidade insuficiente da instância 3112
A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis. 3113
A instância é encerrada imediatamente 3114
Permissões insuficientes 3115
Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows) 3116
Conecte-se à sua instância do Linux 3117
Causas comuns de problemas de conexão 3118
Erro ao se conectar à sua instância: limite de tempo da conexão atingido 3120
Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA 3123
Erro: Chave do usuário não reconhecida pelo servidor 3124
Erro: permissão negada ou conexão fechada pela porta 22 de [instância] 3126
Erro: arquivo de chave privada desprotegido 3129

Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----" ... 3130
Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis ... 3131
Não é possível fazer o ping da instância ... 3132
Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor) ... 3132
Erro: falha na validação da chave do host para EC2 Instance Connect ... 3133
Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect ... 3135
Perdi minha chave privada. Como posso me conectar à minha instância do Linux? ... 3135
Conectar-se à sua instância do Windows do ... 3143
O Remote Desktop não pode se conectar ao computador remoto ... 3143
Erro ao usar o cliente RDP do macOS ... 3148
O RDP exibe uma tela preta em vez da área de trabalho ... 3148
Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador ... 3149
Resolução de problemas do desktop remoto usando o AWS Systems Manager ... 3149
Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto ... 3153
Perdi minha chave privada. Como posso me conectar à minha instância do Windows? ... 3154
Redefinir uma senha de administrador do Windows perdida ou expirada ... 3155
Redefinir com o EC2Launch v2 ... 3156
Redefinir usando o EC2Config ... 3161
Redefinir usando o EC2Launch ... 3168
Solucionar problemas de uma instância não acessível ... 3174
Reinicialização da instância ... 3174
Saída do console da instância ... 3174
Fazer uma captura de tela de uma instância inacessível ... 3176
Capturas de tela comuns para instâncias do Windows ... 3178
Recuperação da instância quando um computador host falhar ... 3188
Parar a instância ... 3188
Forçar a parada da instância ... 3189
Para criar uma instância de substituição ... 3190
Encerrar a instância ... 3192
A instância é encerrada imediatamente ... 3192
Encerramento atrasado da instância ... 3192
Instância encerrada ainda sendo exibida ... 3193

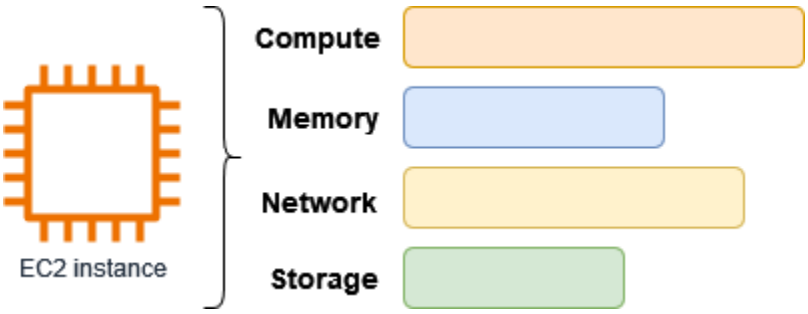
Erro: a instância não pode ser encerrada. Modifique seu atributo de instância 'disableApiTermination' 3193
Instâncias executadas ou encerradas automaticamente 3193
Falha nas verificações de status no Linux 3194
Analisar informações de verificação de status 3195
Recuperar os logs do sistema 3196
Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux 3196
Sem memória: encerrar processo 3198
ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória) 3199
Erro de E/S (falha de dispositivo de blocos) 3200
ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado) 3202
request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) 3203
"FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI) 3204
"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) 3205
ERRO Kernel inválido (kernel incompatível com EC2) 3207
fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado) 3208
Erro geral ao montar os sistemas de arquivos (falha na montagem) 3211
VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) 3213
Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) 3214
XENBUS: Dispositivo sem driver… 3216
…dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) 3217
O fsck morreu com status de saída… (Dispositivo ausente) 3218
Prompt do GRUB (grubdom>) 3219
Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) 3222
Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) 3224
XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) 3225

Solução de problemas de inicialização da instância do Linux usando o volume errado 3226
Solução de problemas de Sysprep 3228
EC2Rescue for Linux 3230
Instalar o EC2Rescue para Linux 3231
(Opcional) Verifique a assinatura de EC2Rescue para Linux 3232
Trabalhar com EC2Rescue para Linux 3235
Desenvolver módulos do EC2Rescue 3238
EC2Rescue for Windows Server 3245
Usar a GUI 3246
Usar a linha de comando. 3252
Usar o Systems Manager 3261
Console de série do EC2 3265
Pré-requisitos 3266
Configurar o acesso ao Console de Série do EC2 3273
Conectar-se ao Console de Série do EC2 3282
Desconecte-se do Console de Série do EC2 3292
Solucionar problemas da instância usando o Console de Série do EC2 3292
Enviar uma interrupção para diagnóstico 3302
Tipos de instâncias compatíveis 3303
Pré-requisitos 3303
Enviar uma interrupção para diagnóstico 3307
Histórico do documentos 3308
Histórico para 2018 e para os anos anteriores 3336

O que é o Amazon EC2?

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação escalável sob demanda na Nuvem Amazon Web Services (AWS). O uso do Amazon EC2 reduz os custos de hardware para que você possa desenvolver e implantar aplicações com mais rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento. Você pode adicionar capacidade (aumentar a escala verticalmente) para lidar com tarefas de computação pesada, como processos mensais ou anuais ou picos no tráfego do site. Quando o uso diminui, você pode reduzir a capacidade (reduzir a escala verticalmente) de novo.

Uma instância do EC2 é um servidor virtual na Nuvem AWS. Quando executa uma instância do EC2, o tipo de instância que você especifica determina o hardware disponível para sua instância. Cada tipo de instância oferece um equilíbrio diferente entre recursos de computação, memória, armazenamento e rede. Para obter mais informações, consulte o Guia de tipos de instância do Amazon EC2.



Recursos do Amazon EC2

O Amazon EC2 fornece os seguintes recursos de alto nível:

Instâncias

Servidores virtuais.

Imagens de máquina da Amazon (AMIs)

Os modelos pré-configurados para suas instâncias que empacotam os componentes de que você precisa para seu servidor (incluindo o sistema operacional e software adicional).

Tipos de instância

Várias configurações de capacidade de CPU, memória, armazenamento e redes e hardware gráfico para suas instâncias.

Volumes do Amazon EBS

Volumes de armazenamento persistentes para seus dados usando o Amazon Elastic Block Store (Amazon EBS).

Volumes de armazenamento de instâncias

Volumes de armazenamento para dados temporários que são excluídos quando você interrompe, hiberna ou encerra sua instância.

Pares de chaves

Proteja informações de login de suas instâncias. A AWS armazena a chave pública, e você armazena a chave privada em um lugar seguro.

Grupos de segurança

Um firewall virtual que permite especificar os protocolos, as portas e os intervalos de IP de origem que podem alcançar suas instâncias e os intervalos de IP de destino aos quais suas instâncias podem se conectar.

O Amazon EC2 é compatível com o processamento, o armazenamento e a transmissão de dados de cartão de crédito por um comerciante ou um provedor de serviços e foi validada como em conformidade com o Data Security Standard (DSS, Padrão de segurança de dados) da Payment Card Industry (PCI, Padrão de cartão de crédito). Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com o PCI da AWS, consulte Nível 1 do PCI DSS.

Serviços relacionados

Serviços para uso com o Amazon EC2

Você pode usar outra Serviços da AWS com as instâncias que você implanta usando o Amazon EC2.

Amazon EC2 Auto Scaling

Ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para processar a carga da aplicação.

AWS Backup

Automatize o backup de suas instâncias do Amazon EC2 e dos volumes do Amazon EBS anexados a elas.

Amazon CloudWatch

Monitore suas instâncias e os volumes do Amazon EBS.

Elastic Load Balancing

Distribua automaticamente o tráfego de entrada da aplicação entre várias instâncias.

Amazon GuardDuty

Detecte o uso potencialmente não autorizado ou mal-intencionado de suas instâncias do EC2.

EC2 Image Builder

Automatize a criação, o gerenciamento e a implantação de imagens de servidor personalizadas, seguras e atualizadas.

AWS Launch Wizard

Dimensione, configure e implante recursos da AWS para aplicações de terceiros sem precisar identificar e provisionar recursos da AWS individuais manualmente.

AWS Systems Manager

Execute operações em grande escala em instâncias do EC2 com essa solução segura de gerenciamento de ponta a ponta.

Serviços adicionais de computação

Você pode iniciar instâncias usando outro serviço de computação da AWS em vez de usar o Amazon EC2.

Amazon Lightsail

Crie sites ou aplicativos da Web usando Amazon Lightsail uma plataforma em nuvem que fornece os recursos necessários para implantar seu projeto rapidamente, por um preço mensal baixo e

previsível. Para comparar o Amazon EC2 e o Lightsail, consulte Amazon Lightsail ou Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Implante, gerencie e escale aplicações em contêineres em um cluster de instâncias do EC2. Para obter mais informações, consulte Escolher um serviço de contêiner da AWS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Execute as aplicações do Kubernetes na AWS. Para obter mais informações, consulte Escolher um serviço de contêiner da AWS.

Acessar o Amazon EC2

Você pode criar e gerenciar as instâncias do Amazon EC2 usando as seguintes interfaces:

Console do Amazon EC2

Uma interface Web simples para criar e gerenciar instâncias e recursos do Amazon EC2. Depois de cadastrar-se em uma conta da AWS, você pode acessar o console do Amazon EC2 fazendo login no AWS Management Console e selecionando EC2 na página inicial do console.

AWS Command Line Interface

Permite interagir com serviços da AWS usando comandos no shell da linha de comando. É compatível com Windows, Mac e Linux. Para obter mais informações sobre a AWS CLI, consulte o Guia do usuário da AWS Command Line Interface. Você pode encontrar os comandos do Amazon EC2 na AWS CLI Command Reference.

AWS CloudFormation

O Amazon EC2 permite a criação de recursos usando o AWS CloudFormation. Você cria um modelo, em JSON ou YAML, que descreve seus recursos da AWS, e o AWS CloudFormation provisiona e configura esses recursos para você. Você pode reutilizar seus modelos do CloudFormation para provisionar os mesmos recursos várias vezes, seja na mesma região e conta ou em várias regiões e contas. Para obter mais informações sobre os tipos de recurso e as propriedades do Amazon EC2, consulte EC2 resource type reference no Guia do usuário do AWS CloudFormation.

SDKs da AWS

Se você preferir criar aplicações usando APIs específicas de uma linguagem em vez de enviar uma solicitação via HTTP ou HTTPS, a AWS fornece bibliotecas, código de exemplo, tutoriais e outros recursos para desenvolvedores de software. Essas bibliotecas fornecem funções básicas que automatizam tarefas, como assinatura criptografada de suas solicitações, novas tentativas de solicitações e tratamento das respostas de erro, facilitando para que você comece rapidamente. Para obter mais informações, consulte Ferramentas para criar na AWS.

AWS Tools for PowerShell

Um conjunto de módulos do PowerShell criados com base na funcionalidade exposta pelo AWS SDK for .NET. As ferramentas para PowerShell permitem que você execute scripts para operações em seus recursos da AWS usando a linha de comando do PowerShell. Para começar a usar, consulte o Guia do usuário da AWS Tools for Windows PowerShell. Você pode encontrar os cmdlets para o Amazon EC2, na AWS Tools for PowerShell Cmdlet Reference.

API de consulta

A Amazon EC2 fornece uma API de consulta. Essas são solicitações HTTP ou HTTPS que usam verbos HTTP GET ou POST e um parâmetro de consulta chamado `Action`. Para obter mais informações sobre as ações de API para o Amazon EC2, consulte Ações no Amazon EC2 API Reference.

Definição de preço do Amazon EC2

O Amazon EC2 fornece as seguintes opções de preços:

Nível gratuito

Você pode começar gratuitamente com o Amazon EC2. Para explorar as opções do nível gratuito, consulte Nível gratuito da AWS.

Instâncias sob demanda

Pague pelas instâncias que você usar por segundo, com um mínimo de 60 segundos, sem qualquer compromisso de longo prazo ou pagamentos adiantados.

Savings Plans

É possível reduzir os custos do Amazon EC2 se comprometendo com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos.

Reserved Instances

É possível reduzir os custos do Amazon EC2 se comprometendo com uma configuração específica de instância, incluindo o tipo de instância e a região, por um período de vigência de um ou de três anos.

Spot Instances

Solicite instâncias do EC2 não utilizadas, o que pode reduzir os custos do Amazon EC2 significativamente.

Hosts dedicados

Reduza os custos usando um servidor físico do EC2 totalmente dedicado ao seu uso, sob demanda ou como parte de um Savings Plan. Você pode usar suas licenças de software existentes vinculadas ao servidor e obter ajuda para atender aos requisitos de conformidade.

On-Demand Capacity Reservations

Reserve capacidade de computação para suas instâncias do EC2 em uma zona de disponibilidade específica por qualquer tempo de duração.

Cobrança por segundo

Elimina o custo de minutos e segundos não utilizados da sua fatura.

Para obter uma lista completa de cobranças e preços do Amazon EC2 e mais informações sobre modelos de compra, consulte Preço do Amazon EC2.

Estimativas, faturamento e otimização de custos

Para criar estimativas para seus casos de uso da AWS, use a AWS Pricing Calculator.

Para estimar o custo de transformar as workloads da Microsoft em uma arquitetura moderna que usa serviços de código aberto e nativos da nuvem implantados na AWS, use a Calculadora de Modernização da AWS para workloads da Microsoft.

Para ver sua fatura, acesse o Painel de gerenciamento de custos e faturamento no console do AWS Billing and Cost Management. Sua fatura contém links para relatórios de uso que fornecem detalhes sobre sua conta. Para saber mais sobre o faturamento da conta da AWS, consulte o Guia do usuário do AWS Billing and Cost Management.

Se tiver dúvidas sobre faturamento, contas e eventos da AWS, entre em contato com o Suporte da AWS.

Para calcular o custo de um exemplo de ambiente provisionado, consulte Centro de informações sobre economia da nuvem. Ao calcular o custo de um ambiente provisionado, lembre-se de incluir custos incidentais, como armazenamento de snapshots para volumes do EBS.

Você pode otimizar o custo, a segurança e a performance do seu ambiente da AWS usando o AWS Trusted Advisor.

É possível usar o AWS Cost Explorer para analisar o custo e o uso das instâncias do EC2. Você pode visualizar dados dos últimos 13 meses e prever o provável valor que você gastará nos próximos 12 meses. Para obter mais informações, consulte Analyzing your costs with AWS Cost Explorer no Guia do usuário do AWS Cost Management.

Recursos

- Recursos do Amazon EC2
- AWS re:Post
- AWS Skill Builder
- Suporte do AWS
- Tutoriais práticos
- Hospedagem na Web
- Windows na AWS

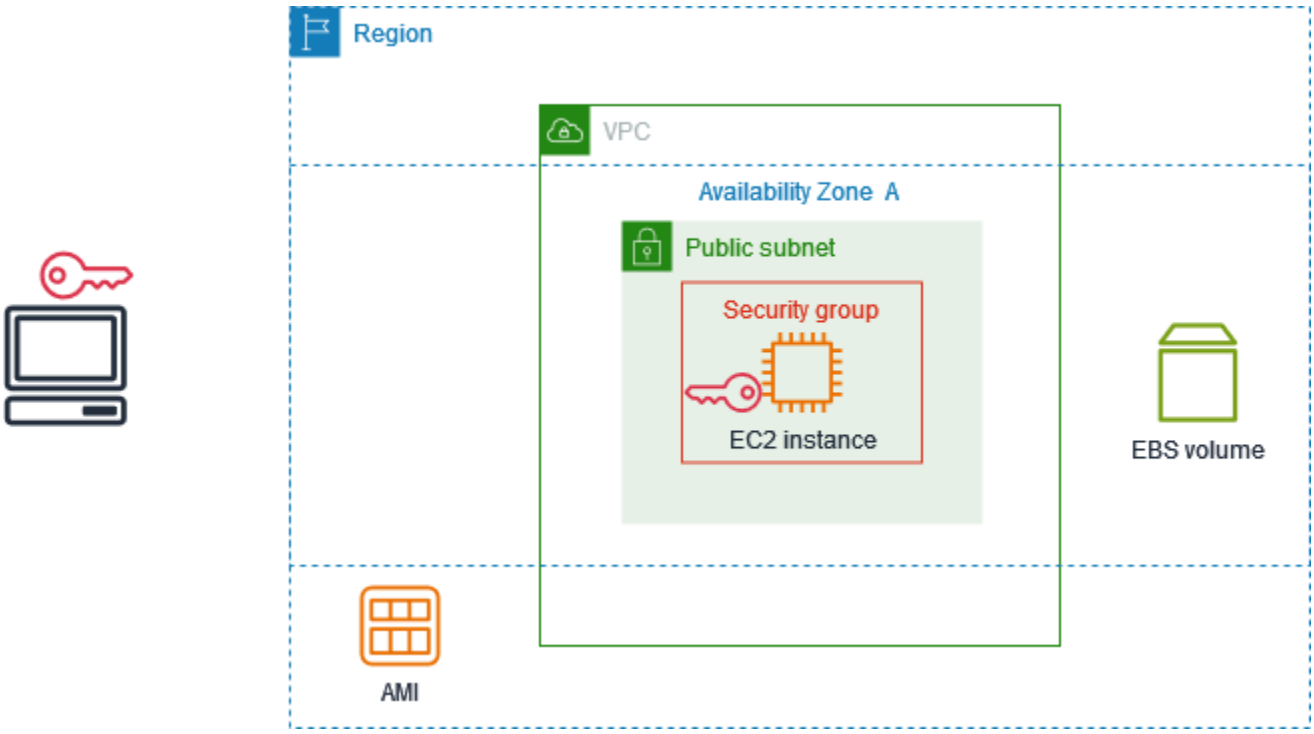
Comece a usar o Amazon EC2

Use este tutorial para começar a usar o Amazon Elastic Compute Cloud (Amazon EC2). Você aprenderá como iniciar e se conectar a uma instância do EC2. Uma instância é um servidor virtual na Nuvem AWS. Com o Amazon EC2 é possível definir e configurar o sistema operacional e as aplicações que são executadas em sua instância.

Visão geral

O seguinte diagrama mostra os principais componentes que você usará neste tutorial:

- Uma imagem: um modelo que contém o software a ser executado na instância, como o sistema operacional.
- Um par de chaves: um conjunto de credenciais de segurança que você usa para provar a identidade ao realizar a conexão com a instância. A chave pública está na instância e a chave privada está no computador.
- Uma rede: uma nuvem privada virtual (VPC) é uma rede virtual dedicada à Conta da AWS. Para ajudar você a começar a usar rapidamente, a conta é equipada com uma VPC padrão em cada Região da AWS, e cada VPC padrão tem uma sub-rede padrão em cada zona de disponibilidade.
- Um grupo de segurança: atua como um firewall virtual para controlar o tráfego de entrada e de saída.
- Um volume do EBS: exigimos um volume raiz para a imagem. Como opção, é possível adicionar volumes de dados.



Custo para este tutorial

Quando você se cadastra na AWS, pode começar a usar o Amazon EC2 com o Nível gratuito da AWS. Se você criou a Conta da AWS há menos de 12 meses e ainda não excedeu os benefícios do nível gratuito para o Amazon EC2, não custará nada concluir este tutorial, pois ajudamos você a selecionar opções que estão dentro dos benefícios do nível gratuito. Caso contrário, você incorrerá em taxas de utilização padrão do Amazon EC2 desde o momento em que executar a instância até encerrar a instância (que é a tarefa final deste tutorial), mesmo que ela permaneça ociosa.

Para obter instruções sobre como determinar se você é elegível para o nível gratuito, consulte the section called “Acompanhar seu uso do nível gratuito”.

Tarefas

- Etapa 1: executar uma instância
- Etapa 2: conectar-se à instância
- Etapa 3: limpar a instância
- Próximas etapas

Etapa 1: executar uma instância

É possível iniciar uma instância do EC2 usando o AWS Management Console conforme descrito no procedimento a seguir. Este tutorial tem como objetivo ajudar você a iniciar rapidamente sua primeira instância dentro dos benefícios do nível gratuito, por isso não abrange todas as opções possíveis.

Como iniciar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, exibimos a Região da AWS atual. Por exemplo, Ohio. Você pode usar a região selecionada ou, opcionalmente, selecionar uma região mais próxima de você.
3. No painel do console do EC2, no painel Iniciar instância, escolha Iniciar instância.
4. Em Name and tags (Nome e etiquetas), em Name (Nome), insira um nome descritivo para a instância.
5. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e SO [imagem de máquina da Amazon]), faça o seguinte:
   a. Escolha Início rápido e, em seguida, selecione o sistema operacional (SO) da sua instância. Para sua primeira instância do Linux, recomendamos escolher o Amazon Linux.
   b. Em Imagem de máquina da Amazon (AMI), selecione uma AMI marcada como qualificada para o nível gratuito.
6. Em Tipo de instância, para Tipo de instância, escolha `t2.micro`, que é qualificado para o nível gratuito. Nas regiões em que `t2.micro` não está disponível, o tipo `t3.micro` é qualificado para o nível gratuito.
7. Em Par de chaves (login), para Nome do par de chaves, escolha um par de chaves existente ou selecione Criar novo par de chaves para criar seu primeiro par de chaves.

   > **Warning**
   >
   > Se você escolher Prosseguir sem um par de chaves (não recomendado), não será possível realizar a conexão com a instância usando os métodos descritos neste tutorial.

8. Em Configurações de rede, observe que selecionamos a VPC padrão, selecionamos a opção de usar a sub-rede padrão em uma zona de disponibilidade que escolhemos para você e configuramos um grupo de segurança com uma regra que permite conexões com a instância de

qualquer lugar. Para sua primeira instância, recomendamos usar as configurações padrão. Caso contrário, é possível atualizar as configurações de rede da seguinte forma:

- (Opcional) Para usar uma sub-rede padrão específica, escolha Editar e, em seguida, selecione uma sub-rede.
- (Opcional) Para usar uma VPC diferente, escolha Editar e, em seguida, selecione uma VPC existente. Se a VPC não estiver configurada para acesso público por parte da Internet, você não conseguirá se conectar à instância.
- (Opcional) Para restringir o tráfego de conexão de entrada para uma rede específica, escolha Personalizado em vez de Qualquer lugar e insira o bloco CIDR da sua rede.
- (Opcional) Para usar um grupo de segurança diferente, escolha Selecionar grupo de segurança existente e escolha um grupo de segurança existente. Se o grupo de segurança não tiver uma regra que permita o tráfego de conexão da sua rede, você não conseguirá se conectar à instância. Para uma instância do Linux, você deve permitir o tráfego SSH. Para uma instância do Windows, você deve permitir o tráfego RDP.

9. Em Configurar armazenamento, observe que configuramos um volume raiz, mas nenhum volume de dados. Isto é suficiente para fins de teste.
10. Revise um resumo da configuração da instância no painel Summary (Resumo) e, quando você estiver pronto, escolha Launch instance (Iniciar instância).
11. Se a inicialização ocorrer com êxito, escolha o ID da instância na notificação de Êxito para abrir a página Instâncias e monitorar o status da inicialização.
12. Marque a caixa de seleção para a instância. O estado inicial da instância é `pending`. Depois que a instância é iniciada, seu estado muda para `running`. Escolha a guia Status e alarmes. Depois que a instância for aprovada nas verificações de status, ela estará pronta para receber solicitações de conexão.

Etapa 2: conectar-se à instância

O procedimento usado dependerá do sistema operacional da instância. Se você não puder se conectar à sua instância, consulte Solução de problemas de conexão com a instância do Linux para obter assistência.

Instâncias do Linux

É possível se conectar à instância do Linux usando qualquer cliente SSH. Se você estiver executando o Windows em seu computador, abra um terminal e execute o comando `ssh` para

verificar se um cliente SSH está instalado. Se o comando não for encontrado, instale o OpenSSH para Windows.

Para se conectar à sua instância usando SSH

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.
4. Na página Conectar-se à instância, escolha a guia Cliente SSH.
5. (Opcional) Se você criou um par de chaves ao iniciar a instância e fez download da chave privada (arquivo .pem) em um computador em execução no Linux ou no macOS, execute o comando chmod de exemplo para definir as permissões para a chave privada.
6. Copie o comando SSH de exemplo. Veja a seguir um exemplo em que *key-pair-name*.pem é o nome do arquivo de chave privada, *ec2-user* é o nome do usuário associado à imagem, e a string após o símbolo @ é o nome DNS público da instância.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. Em uma janela de terminal do computador, execute o comando ssh que você salvou na etapa anterior. Se o arquivo de chave privada não estiver no diretório atual, você deverá especificar o caminho completo para o arquivo de chave neste comando.

   Esta é uma resposta de exemplo:

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital da instância contida na saída do console ao iniciar uma instância pela primeira vez. Para obter a saída do console, escolha Ações, Monitorar e solucionar problemas e Obter log do sistema. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se corresponderem, continue para a próxima etapa.
9. Digite **yes**.

   Esta é uma resposta de exemplo:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Instâncias do Windows

Para se conectar a uma instância do Windows, é necessário recuperar a senha do administrador e usar essa senha ao se conectar à sua instância usando o desktop remoto. Após a execução da instância, leva alguns minutos para que a senha fique disponível.

O nome de usuário padrão correspondente à conta de administrador depende do idioma do sistema operacional (SO) contido na AMI. Para verificar o nome de usuário correto, identifique o idioma do sistema operacional da sua AMI e escolha o nome de usuário correspondente. Por exemplo, para um sistema operacional em inglês, o nome de usuário será `Administrator`, para um sistema operacional francês, será `Administrateur` e para um sistema operacional português, será `Administrador`. Se uma versão de idioma do sistema operacional não tiver um nome de usuário no mesmo idioma, escolha o nome de usuário `Administrator (Other)`. Para obter mais informações, consulte Localized Names for Administrator Account in Windows (Nomes localizados da conta de administrador no Windows) no Microsoft TechNet Wiki.

Se você associou sua instância a um domínio, poderá se conectar a sua instância usando credenciais de domínio definidas no AWS Directory Service. Na tela de login do Desktop Remoto, em vez de usar o nome do computador local e a senha gerada, use o nome de usuário totalmente qualificado para o administrador (por exemplo, **`corp.example.com\Admin`**) e a senha dessa conta.

Se você receber um erro ao tentar se conectar à instância, consulte the section called “O Remote Desktop não pode se conectar ao computador remoto”.

Para se conectar à sua instância do Windows usando um cliente RDP

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.
4. Na página Conectar à instância, escolha a guia Cliente RDP.
5. Em Nome de usuário, escolha o nome de usuário padrão para a conta do administrador. O nome de usuário escolhido deverá corresponder ao idioma do sistema operacional (SO) contido na

AMI que você usou para executar a instância. Se não houver um nome de usuário no mesmo idioma do seu sistema operacional, escolha Administrador (Outro).

6. Escolha Obter senha.
7. Na página Obter senha do Windows, faça o seguinte:

   a. Escolha Fazer upload de arquivo de chave privada e localize o arquivo de chave privada (`.pem`) que especificou ao executar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.

   b. Escolha Descriptografar senha. A página Obter senha do Windows será fechada e a senha padrão do administrador para a instância será exibida em Senha, substituindo o link Obter senha exibido anteriormente.

   c. Copie e salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.

8. Escolha Download remote desktop file (Fazer download de arquivo do desktop remoto). Quando terminar o download do arquivo, escolhaCancel (Cancelar) para retornar à página Instances (Instâncias). Navegue até o diretório de downloads e abra o arquivo do RDP.
9. Você pode receber um aviso de que o editor da conexão remota é desconhecido. Escolha Connect (Conectar) para se conectar à sua instância.
10. A conta de administrador é escolhida por padrão. Cole a senha que você copiou anteriormente e, em seguida, escolha OK.
11. Por causa da natureza de certificados autoassinados, talvez você receba um aviso indicando que não foi possível autenticar o certificado de segurança. Execute um destes procedimentos:

    - Se você confia no certificado, escolha Sim para realizar a conexão com a instância.
    - [Windows] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Visualizar certificado e, em seguida, escolha Impressão digital na guia Detalhes. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
    - [Mac OS X] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Mostrar certificado, expanda Detalhes e selecione Impressões digitais de SHA1. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.

Etapa 3: limpar a instância

Após concluir a instância que você criou para este tutorial, você deverá limpar encerrando a instância. Se você quiser realizar outras ações com essa instância antes de limpá-la, consulte Próximas etapas.

> **Important**
>
> Encerrar uma instância significa excluí-la efetivamente, pois você não poderá mais reconectá-la depois dessa ação.

Se você iniciou uma instância que não está no Nível gratuito da AWS, não incorrerá mais em custos para ela assim que o status dela passar a instância de `shutting down` para `terminated`. Para manter sua instância para depois, sem a cobrança de taxas, será possível interromper a instância agora e iniciá-la novamente mais tarde. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

Para encerrar sua instância

1. No painel de navegação, escolha Instances (Instâncias). Na lista de instâncias, selecione a instância.
2. Escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
3. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

   O Amazon EC2 desliga e encerra sua instância. Depois que a instância for encerrada, ela permanecerá visível no console por um curto período e a entrada será automaticamente excluída. Você não pode remover a instância encerrada da exibição do console.

Próximas etapas

Depois de iniciar a instância, você pode querer explorar as seguintes etapas:

- Aprenda a monitorar o uso do nível gratuito para evitar surpresas na cobrança. Para ter mais informações, consulte the section called “Acompanhar seu uso do nível gratuito”.

- Configure um alarme do CloudWatch para notificá-lo caso seu uso ultrapasse o Nível gratuito. Para obter mais informações, consulte Rastreamento do uso do nível gratuito da AWS no Guia do usuário do AWS Billing.
- Adicione um volume do EBS. Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2.
- Saiba como gerenciar remotamente a instância do EC2 utilizando o comando Run. Para obter mais informações, consulte Comando AWS Systems Manager Run no Guia do usuário do AWS Systems Manager.
- Saiba mais sobre as opções de compra de instâncias. Para ter mais informações, consulte Opções de compra de instância.
- Obtenha conselho sobre tipos de instâncias. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma nova workload.

Melhores práticas do Amazon EC2

Para garantir os resultados máximos com a execução do Amazon EC2, sugerimos executar as práticas recomendadas a seguir.

Segurança

- Gerencie o acesso a recursos e APIs da AWS usando federação de identidades com um provedor de identidades e perfis do IAM sempre que possível. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.
- Implemente as regras menos permissivas para o security group. Para obter mais informações, consulte Regras de grupos de segurança.
- Corrija, atualize e proteja regularmente o sistema operacional e os aplicativos em sua instância. Para ter mais informações, consulte Gerenciamento de atualizações. Para obter diretrizes específicas para sistemas operacionais do Windows, consulte Práticas recomendadas de segurança para instâncias do Windows.
- Use o Amazon Inspector para descobrir e verificar automaticamente instâncias do Amazon EC2 em busca de vulnerabilidades de software e exposição não intencional da rede. Para obter mais informações, consulte o Guia do usuário do Amazon Inspector.
- Use controles do AWS Security Hub para monitorar seus recursos do Amazon EC2 em relação às melhores práticas e padrões de segurança. Para obter mais informações sobre o uso do Security Hub, consulte Controles do Amazon Elastic Compute Cloud no Guia do usuário do AWS Security Hub.

Armazenamento

- Compreenda as implicações do tipo de dispositivo raiz para a persistência, o backup e a recuperação de dados. Para obter mais informações, consulte Armazenamento para o dispositivo raiz.
- Use volumes do Amazon EBS separados para o sistema operacional e para seus dados. Verifique se o volume com seus dados persiste depois do encerramento de uma instância. Para obter mais informações, consulte Preservação de dados quando uma instância for encerrada.
- Use o armazenamento de instâncias disponível para que sua instância armazene dados temporários. Lembre-se de que os dados armazenados em um armazenamento de instâncias são excluídos quando você interrompe, hiberna ou encerra uma instância. Se você usar o

armazenamento de instâncias para armazenamento de bancos de dados, verifique se você tem um cluster com um fator de replicação que garanta tolerância a falhas.

- Criptografe volumes e snapshots do EBS. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

Gerenciamento de recursos

- Use os metadados da instância e as tags personalizadas dos recursos para acompanhar e identificar os recursos da AWS. Para obter mais informações, consulte Trabalhar com metadados de instância e Marcar com tag os recursos do Amazon EC2.
- Visualize seus limites atuais para o Amazon EC2. Planeje a solicitação de aumentos dos limites com antecedência antes que sejam necessários. Para ter mais informações, consulte Service Quotas do Amazon EC2.
- Use AWS Trusted Advisor para inspecionar seu ambiente da AWS e fazer recomendações quando houverem oportunidades para economizar dinheiro, melhorar a performance do sistema ou ajudar a corrigir falhas de segurança. Para obter mais informações, consulte AWS Trusted Advisor no Guia de Usuário AWS Support.

Backup e recuperação

- Faça backup de seus volumes do EBS regularmente usando Snapshots do Amazon EBS e crie uma Imagem de máquina da Amazon (AMI) de sua instância para salvar a configuração como um modelo para executar futuras instâncias. Para obter mais informações sobre os serviços da AWS que ajudam a realizar esse caso de uso, consulte AWS Backup e o Amazon Data Lifecycle Manager.
- Implante os componentes essenciais de seu aplicativo em várias zonas de disponibilidade e replique os dados adequadamente.
- Crie seus aplicativos para lidarem com o endereçamento IP dinâmico quando sua instância for reiniciada. Para obter mais informações, consulte Endereçamento IP de instâncias do Amazon EC2.
- Monitorar e responder a eventos. Para obter mais informações, consulte Monitorar o Amazon EC2.
- Certifique-se de que você está preparado para lidar com failover. Para uma solução básica, é possível anexar manualmente uma interface de rede ou um endereço IP elástico para uma instância de substituição. Para obter mais informações, consulte Interfaces de rede elástica. Para

uma solução automatizada, é possível usar o Amazon EC2 Auto Scaling. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

- Teste regularmente o processo de recuperação de suas instâncias e dos volumes do Amazon EBS para garantir que dados e serviços sejam restaurados com êxito.

Redes

- Defina a vida útil (TTL) de seus aplicativos como 255, para IPv4 e IPv6. Se você usar um valor menor, a TTL poderá expirar enquanto o tráfego do aplicativo estiver em trânsito, causando problemas de acessibilidade para as instâncias.

Imagens de máquina da Amazon (AMIs)

Uma Imagem de máquina da Amazon (AMI) é uma imagem fornecida pela AWS que contém as informações necessárias para iniciar uma instância. Especifique uma AMI ao iniciar uma instância. É possível iniciar várias instâncias em uma única AMI quando precisar de várias instâncias com a mesma configuração. É possível usar AMIs diferentes para iniciar instâncias quando precisar de instâncias com configurações diferentes.

Uma AMI inclui o seguinte:

- Um ou mais snapshots do Amazon Elastic Block Store (Amazon EBS) ou, para AMIs com suporte de armazenamento de instâncias, um modelo para o volume raiz da instância (por exemplo, um sistema operacional, um servidor da aplicação e aplicações).
- Permissões de execução que controlam quais contas da AWS podem usar a AMI para executar instâncias.
- Um mapeamento de dispositivos de blocos que especifica os volumes a serem anexados à instância quando ela for executada.

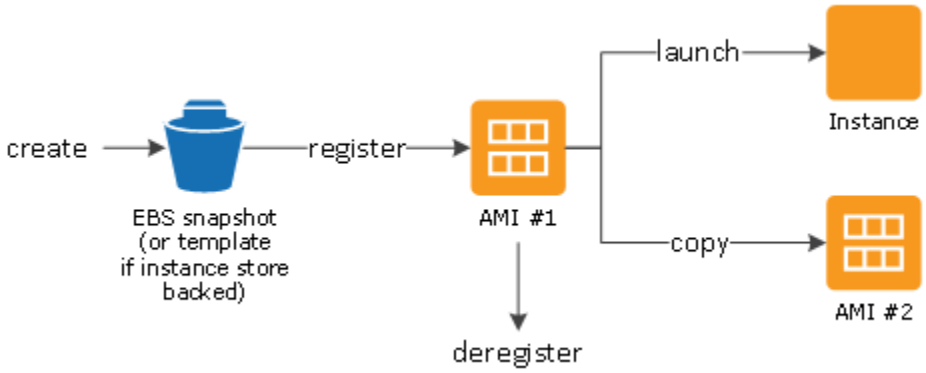
Tópicos da imagem de máquina da Amazon (AMI)

- Usar uma AMI
- Criar sua própria AMI
- Comprar, compartilhar e vender AMIs
- Cancelar o registro da AMI
- Amazon Linux 2023 e Amazon Linux 2
- AMIs Windows
- Tipos de AMI
- Tipos de virtualização de AMI
- Modos de inicialização do Amazon EC2
- Encontrar uma AMI
- AMIs compartilhadas
- AMIs pagas
- Ciclo de vida da AMI
- Usar criptografia com AMIs com EBS

- Monitorar eventos da AMI usando o Amazon EventBridge
- Noções básicas sobre as informações de faturamento da AMI
- Cotas de AMI

Usar uma AMI

O diagrama a seguir resume o ciclo de vida da AMI. Após criar e registrar uma AMI, é possível usá-la para executar novas instâncias. (Também é possível executar instâncias em uma AMI se o proprietário da AMI conceder permissões de execução a você.) É possível copiar uma AMI na mesma região da AWS ou para regiões da AWS diferentes. Quando não precisar mais de uma AMI, será possível cancelar o registro dela.



É possível pesquisar uma AMI que atenda aos critérios para sua instância. É possível pesquisar AMIs fornecidas pela AWS ou AMIs fornecidas pela comunidade. Para obter mais informações, consulte Tipos de AMI e Encontrar uma AMI.

Depois de iniciar uma instância em uma AMI, é possível se conectar a ela. Quando você está conectado a uma instância, é possível usá-la da mesma forma como usa outro servidor. Para obter informações sobre a execução, a conexão e o uso de sua instância, consulte Comece a usar o Amazon EC2.

Criar sua própria AMI

Você pode iniciar uma instância usando uma AMI existente, personalizar a instância (por exemplo, instalar software na instância) e salvar essa configuração atualizada como uma AMI personalizada. Entre as instâncias executadas nessa AMI personalizada estão as personalizações que você fez quando criou a AMI.

O dispositivo de armazenamento raiz da instância determina o processo que você segue para criar uma AMI. O volume raiz de uma instância é um volume do Amazon Elastic Block Store (Amazon EBS) ou um volume de armazenamento de instâncias. Para obter mais informações sobre volumes de dispositivos raiz, consulte Volume raiz da instância do Amazon EC2.

- Para criar uma AMI baseada no Amazon EBS, consulte Criação de uma AMI baseada no Amazon EBS.
- Para criar uma AMI com armazenamento de instâncias, consulte Criar uma AMI em Linux com armazenamento de instâncias.

Para ajudar a categorizar e gerenciar suas AMIs, é possível atribuir tags personalizadas a elas. Para obter mais informações, consulte Marcar com tag os recursos do Amazon EC2.

Comprar, compartilhar e vender AMIs

Após criar uma AMI, é possível mantê-la privada para que somente você possa o usá-la ou pode compartilhá-la com uma lista especificada de contas da AWS. Também é possível tornar pública sua AMI personalizada para que a comunidade possa usá-la. A criação de uma AMI segura, protegida e utilizável para consumo público é um processo bastante direto, quando você segue algumas diretrizes simples. Para obter informações sobre como criar e usar AMIs compartilhadas, consulte AMIs compartilhadas.

É possível comprar AMIs de terceiros, incluindo AMIs fornecidas com contratos de serviço de organizações como a Red Hat. Também é possível criar uma AMI e vendê-la para outros usuários do Amazon EC2. Para obter mais informações sobre como comprar ou vender AMIs, consulte AMIs pagas.

Cancelar o registro da AMI

É possível cancelar o registro de uma AMI, quando não precisar mais dela. Depois de cancelar o registro de uma AMI, ela não poderá ser usada para executar novas instâncias. As instâncias existentes executadas na AMI não são afetadas. Para ter mais informações, consulte Cancelar o registro de uma AMI (excluir a AMI).

Amazon Linux 2023 e Amazon Linux 2

A versão mais recente do Amazon Linux, AL2023, é otimizada para o Amazon EC2 e é fornecida sem custo adicional aos usuários do Amazon EC2. Os recursos do AL2023 incluem uma cadência de lançamento previsível, atualizações frequentes e suporte de longo prazo.

Para obter mais informações sobre recursos do AL2023 e a execução de uma AMI do AL2023, consulte:

- Recursos do AL2023
- Comece a usar o AL2023

O Amazon Linux 2 (AL2) fornece um ambiente de execução estável, seguro e de alta performance para aplicações executadas no Amazon EC2. Para obter mais informações sobe o Amazon Linus 2, consulte Amazon Linux 2 on Amazon EC2 no Amazon Linux 2 User Guide.

> **Note**
>
> O Amazon Linux AMI foi descontinuado em 31 de dezembro de 2023 e não recebe atualizações de segurança nem correções de erros a partir de 1º de janeiro de 2024. Para obter mais informações sobre a descontinuação do Amazon Linux AMI e o suporte para manutenção, consulte a postagem do blog Update on Amazon Linux AMI end-of-life. Recomendamos que você atualize as aplicações para o AL2023, o que inclui suporte de longo prazo até 2028.

AMIs Windows

A AWS oferece um conjunto de AMIs publicamente disponíveis que contêm configurações de software específicas à plataforma Windows. Usando essas AMIs, é possível começar a criar e a implantar suas aplicações rapidamente com o Amazon EC2. Primeiro, escolha a AMI que atende a seus requisitos específicos e execute uma instância usando essa AMI. Você recupera a senha da conta do administrador e faz login na instância usando a Conexão de Desktop Remoto, exatamente da mesma forma como com qualquer outro servidor do Windows. Para obter mais informações sobre as AMIs do AWS Windows, consulte a Referência da AMI do AWS Windows.

Ao iniciar uma instância de uma AMI do Windows, o dispositivo raiz da instância do Windows é um volume do Amazon Elastic Block Store (Amazon EBS). As AMIs do Windows não são compatíveis com o armazenamento de instâncias no dispositivo raiz.

As AMIs do Windows que foram configuradas para inicialização mais rápida com o EC2 Fast Launch são provisionadas previamente, usando snapshots para iniciar as instâncias com até 65% mais rapidez. Para saber mais sobre o EC2 Fast Launch, consulte Uso do EC2 Fast Launch para as instâncias do Windows.

> **Note**
>
> A Microsoft não oferece mais suporte às versões do Windows Server anteriores ao Windows Server 2016. Recomendamos executar novas instâncias do EC2 usando uma versão compatível do Windows Server. Se você tiver instâncias do EC2 existentes nas quais haja uma versão incompatível do Windows Server em execução, recomendamos atualizar essas instâncias para uma versão compatível do Windows Server. Para ter mais informações, consulte Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server..

Tipos de AMI

É possível selecionar uma AMI para uso com base nas seguintes características:

- Região (consulte A VPC abrange as zonas de disponibilidade e a zona Wavelength.)
- Sistema operacional
- Arquitetura (32 bits ou 64 bits)
- Permissões de execução
- Armazenamento para o dispositivo raiz

Permissões de execução

O proprietário de uma AMI determina sua disponibilidade especificando permissões de execução. As permissões de execução entram nas seguintes categorias.

Permissão de execução	Descrição
pública	O proprietário concede permissões de execução a todas as contas da AWS.
explícita	O proprietário concede permissões de execução a contas, organizações ou unidades organizacionais (UOs) específicas da AWS.
implícita	O proprietário tem permissões de execução implícitas para uma AMI.

A Amazon e a comunidade do Amazon EC2 fornecem uma grande seleção de AMIs públicas. Para obter mais informações, consulte AMIs compartilhadas. Os desenvolvedores podem cobrar por suas AMIs. Para obter mais informações, consulte AMIs pagas.

Armazenamento para o dispositivo raiz

Todas as AMIs são categorizadas como com Amazon EBS ou com armazenamento de instâncias.

- AMI baseada no Amazon EBS: o dispositivo raiz de uma instância iniciada na AMI é um volume do Amazon Elastic Block Store (Amazon EBS) criado de um snapshot do Amazon EBS. Compatível com as AMIs do Linux e do Windows.
- AMI baseada no armazenamento de instâncias: o dispositivo raiz de uma instância iniciada a partir da AMI é um volume de armazenamento de instâncias criado com base em um modelo armazenado no Amazon S3. Compatível somente com as AMIs do Linux. As AMIs do Windows não são compatíveis com o armazenamento de instâncias no dispositivo raiz.

Para ter mais informações, consulte Volume raiz da instância do Amazon EC2.

A tabela a seguir resume as diferenças importantes ao usar os dois tipos de AMIs.

Característica	AMI baseada no Amazon EBS	AMI com armazenamento de instâncias da Amazon
Tempo de inicialização para uma instância	Geralmente menos que 1 minuto	Geralmente menos que 5 minutos

Característica	AMI baseada no Amazon EBS	AMI com armazenamento de instâncias da Amazon
Limite de tamanho para um dispositivo raiz	64 TiB	10 GiB
Volume do dispositivo raiz	Volume do EBS	Volumes de armazenamento de instâncias
Persistência de dados	Por padrão, o volume raiz é excluído quando a instância é encerrada.* Os dados em todos os outros volumes do EBS persistem após o encerramento da instância, por padrão.	Os dados em qualquer volume do armazenamento de instâncias persistem apenas durante a vida útil da instância.
Modificações	O tipo de instância, o kernel, o disco da RAM e os dados do usuário podem ser alterados enquanto a instância está parada.	Os atributos de instância são fixos durante a vida útil de uma instância.
Cobranças	Você é cobrado pelo uso de instância, uso de volume do EBS; e pelo armazenamento da AMI como um snapshot do EBS.	Você é cobrado pelo uso da instância e pelo armazenamento da AMI no Amazon S3.
Criação/empacotamento da AMI	Usa um único comando/chamada	Requer instalação e uso de ferramentas de AMI

Característica	AMI baseada no Amazon EBS	AMI com armazenamento de instâncias da Amazon
Estado parado	Pode estar em um estado interrompido. Mesmo quando a instância é interrompida e não está em execução, o volume raiz permanece no Amazon EBS	Não pode estar em um estado interrompido. Há instâncias em execução ou encerradas

* Por padrão, os volumes raiz do EBS têm o sinalizador `DeleteOnTermination` definido como `true`. Para obter informações sobre como alterar esse sinalizador para que o volume persista depois do encerramento, consulte Alterar o volume raiz para persistir.

** Compatível apenas com `io2` EBS Block Express. Para obter mais informações, consulte Volumes SSD do Block Express com IOPS provisionadas no Guia do usuário do Amazon EBS.

Determinar o tipo de dispositivo raiz da AMI

Para determinar o tipo de dispositivo raiz de uma AMI usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMIs e, em seguida, selecione a AMI.
3. Na guia Details (Detalhes), marque o valor de Root Device Type (Tipo de dispositivo raiz) da seguinte maneira:
   - `ebs`: esta é uma AMI baseada no EBS.
   - `instance store`: esta é uma AMI baseada no armazenamento de instâncias.

Para determinar o tipo de dispositivo raiz de uma AMI usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Estado parado

É possível interromper uma instância que tenha um volume do EBS como dispositivo raiz, mas não é possível interromper uma instância que tenha um volume de armazenamento de instâncias como dispositivo raiz.

Parar faz com que a instância pare de executar (seu status muda de `running` para `stopping` e para `stopped`). Uma instância parada persiste no Amazon EBS, o que permite que ela seja reiniciada. Parar é diferente de encerrar. Você não pode reiniciar uma instância encerrada. Como as instâncias com um volume de armazenamento de instâncias como dispositivo raiz não podem ser interrompidas, elas estão em execução ou terminadas. Para obter mais informações sobre o que acontece e o que é possível fazer enquanto uma instância está parada, consulte Início e interrupção de instâncias do Amazon EC2.

Persistência e armazenamento de dados padrão

As instâncias que usam um volume de armazenamento de instâncias como dispositivo raiz automaticamente têm armazenamento de instâncias disponível (o volume raiz contém a partição raiz e é possível armazenar dados adicionais). É possível adicionar armazenamento persistente à instância anexando um ou mais volumes do EBS. Todos os dados em um volume de armazenamento de instâncias são excluídos quando a instância falha ou é encerrada. Para ter mais informações, consulte Volume de armazenamento de instâncias e vida útil dos dados.

As instâncias que usam o Amazon EBS como dispositivo raiz automaticamente têm um volume do EBS associado. O volume aparece em sua lista de volumes como qualquer outro. Com a maioria dos tipos de instância, as instâncias que têm um volume do EBS como dispositivo raiz não têm volumes de armazenamento de instâncias por padrão. É possível adicionar volumes de armazenamento de instâncias ou volumes do EBS adicionais usando um mapeamento de dispositivos de blocos. Para obter mais informações, consulte Mapeamentos de dispositivos de blocos.

Tempos de inicialização

As instâncias executadas a partir de uma AMI baseada no Amazon EBS são executadas mais rapidamente do que as instâncias executadas a partir de uma AMI com armazenamento de instâncias. Quando você executa uma instância a partir de um AMI com armazenamento de instâncias, todas as partes precisam ser recuperadas do Amazon S3 para que a instância fique disponível. Com uma AMI baseada no Amazon EBS, apenas as partes necessárias para inicializar a instância precisam ser recuperadas do snapshot para que a instância fique disponível. Contudo,

a performance de uma instância que usa um volume do EBS para seu dispositivo raiz é mais lento por um breve período enquanto as partes restantes são recuperadas do snapshot e carregadas no volume. Quando você para e reinicia a instância, ela é executada rapidamente, porque o estado é armazenado em um volume do EBS.

Criação de AMIs

Para criar AMIs do Linux com armazenamento de instâncias, crie uma AMI de sua instância na própria instância usando as ferramentas de AMI do Amazon EC2. Observe que as AMIs do Windows não oferecem suporte ao armazenamento de instância para o dispositivo raiz.

A criação de AMIs é muito mais fácil para AMIs com suporte do Amazon EBS. A ação da API `CreateImage` cria a AMI com Amazon EBS e a registra. Há também um botão no AWS Management Console que permite criar uma AMI em uma instância em execução. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Como você é cobrado

Com as AMIs com suporte do armazenamento de instâncias, você é cobrado pelo uso da instância e para armazenar a AMI no Amazon S3. Com as AMIs com suporte de Amazon EBS, você é cobrado pelo uso da instância, pelo uso e armazenamento de volume do EBS; e por armazenar a AMI como um snapshot do EBS.

Nas AMIs com armazenamento de instâncias do Amazon EC2, toda vez que você personaliza uma AMI e cria uma nova, todas as partes são armazenadas no Amazon S3 para cada AMI. Portanto, o volume de armazenamento de cada AMI personalizada é o tamanho completo da AMI. Para AMIs baseadas no Amazon EBS, sempre que você personaliza uma AMI e cria um nova, apenas as alterações são armazenadas. Portanto, o espaço de armazenamento ocupado pelas AMIs subsequentes que você personaliza após a primeira é muito menor, resultando em cobranças menores de armazenamento de AMI.

Quando uma instância com um volume EBS como raiz é interrompida, o uso da instância não é cobrado, porém, o armazenamento do volume ainda é cobrado de você. Assim que você iniciar a sua instância, cobraremos por um mínimo de um minuto por uso. Após um minuto, cobraremos apenas pelos segundos que você usar. Por exemplo, se você executar uma instância por 20 segundos e, em seguida, interrompê-la, cobraremos por um minuto completo. Se você executar uma instância por 3 minutos e 40 segundos, cobraremos exatamente por esse tempo de uso. Nós cobramos por cada segundo, com um mínimo de um minuto, que você mantenha a instância em execução, mesmo que a instância permaneça ociosa e você não se conecte a ela.

Tipos de virtualização de AMI

As Imagens de máquina da Amazon usam um dos dois tipos de virtualização: paravirtual (PV) ou máquina virtual de hardware (HVM). As diferenças principais entre as AMIs PV e HVM são a maneira como elas inicializam e se podem aproveitar extensões especiais de hardware (CPU, rede e armazenamento) para melhor performance. As AMIs do Windows são AMIs HVM.

Para melhor performance, recomendamos que você use os tipos de instância da geração atual e AMIs HVM quando executar suas instâncias. Para obter mais informações sobre os tipos de instâncias da atual geração, consulte Tipos de instância do Amazon EC2. Se você estiver usando tipos de instância da geração anterior e quiser fazer uma atualização, consulte Caminhos de atualização e Alterar o tipo de instância.

A tabela a seguir compara AMIs de HVM e PV.

	HVM	PV
Descrição	As AMIs HVM são apresentadas com um conjunto totalmente virtualizado de hardware e inicialização ao executar o registro de inicialização mestre do dispositivo de blocos raiz da sua imagem. Esse tipo de virtualização permite a execução de um sistema operacional diretamente em uma máquina virtual, sem qualquer modificação, como se tivesse sido executada em hardware bare metal. O sistema do host Amazon EC2 emula algum ou todos os hardwares subjacentes apresentados ao guest.	As AMIs PV são inicializadas com um bootloader especial chamado PV-GRUB, que começa o ciclo de inicialização e encadeia e carrega o kernel especificado no arquivo `menu.lst` da sua imagem. Os convidados paravirtuais podem ser executados em hardware de host que não é explicitamente compatível para virtualização. Historicamente, os guests PV têm melhor performance que os guests HVM em muitos casos, mas devido a aprimoramentos na virtualização de HVM e disponibilidade de drivers PV para AMIs HVM, isso não é mais verdadeiro. Para obter mais informações sobre o PV-

	HVM	PV
		GRUB e seu uso no Amazon EC2, consulte User provided kernels.
Suporte para extensões de hardware	Sim. Ao contrário de guests PV, os guests HVM podem aproveitar as extensões de hardware que fornecem acesso rápido ao hardware subjacente no sistema host. Para obter mais informaçõ es sobre as extensões de virtualização de CPU disponíveis no Amazon EC2, consulte Tecnologia de virtualização Intel no site da Intel. As AMIs HVM são necessári as para aproveitar as maiores capacidades de rede e processamento de GPU. Para passar instruções à rede especializada e a dispositi vos de GPU, o SO precisa ter acesso à plataforma de hardware nativa; a virtualiz ação de HVM dá esse acesso. Para ter mais informações, consulte Redes aperfeiçoadas no Amazon EC2.	Não, eles não podem beneficiar-se de extensões de hardware especiais, como rede avançada ou processam ento de GPU.

	HVM	PV
Tipos de instâncias compatíveis	Todos os tipos de instância da geração atual são compatíveis com AMIs HVM.	Os seguintes tipos de instância da geração anterior são compatíveis com AMIs PV: C1, C3, M1, M3, M2 e T1. Os tipos de instância da geração atual não são compatíveis com AMIs PV.
Regiões compatíveis	Todas as regiões são compatíveis com instâncias HVM.	Ásia-Pacífico (Tóquio), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Europa (Frankfurt), Europa (Irlanda), América do Sul (São Paulo), US East (N. Virginia), Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon)
Como encontrar	Verifique se o tipo de virtualização da AMI está definido como `hvm` usando o console ou o comando describe-images. Para ter mais informações, consulte Encontrar uma AMI.	Verifique se o tipo de virtualização da AMI está definido como `paravirtual` usando o console ou o comando describe-images. Para ter mais informações, consulte Encontrar uma AMI.

PV em HVM

Os guests paravirtuais tradicionalmente se saem melhor com operações de armazenamento e rede que os guests de HVM, pois podem aproveitar drivers especiais para E/S que evitaram as despesas gerais de emulação de hardware de rede e de disco, enquanto os guests HVM tiveram de converter essas instruções para o hardware emulado. Agora, esses drivers PV estão disponíveis para guests HVM, de forma que os sistemas operacionais que não puderem ser movidos para execução em um ambiente paravirtualizado ainda poderão ver vantagens de performance no armazenamento e na E/S de rede usando-os. Com esses drivers de PV em HVM, os convidados recebem performance igual, ou melhor, que os guests paravirtuais.

Modos de inicialização do Amazon EC2

Quando um computador é inicializado, o primeiro software executado é responsável por inicializar a plataforma e fornecer uma interface para que o sistema operacional execute operações específicas da plataforma.

No Amazon EC2, há suporte para duas variantes do software do modo de inicialização: Unified Extensible Firmware Interface (UEFI) e BIOS legado.

Possíveis parâmetros do modo de inicialização em uma AMI

Uma AMI pode ter um dos seguintes valores de parâmetro de modo de inicialização: `uefi`, `legacy-bios` ou `uefi-preferred`. O parâmetro de modo de inicialização da AMI é opcional. Para AMIs sem parâmetro de modo de inicialização, as instâncias executadas a partir delas usam o valor de modo de inicialização padrão do tipo de instância.

Objetivo do parâmetro de modo de inicialização da AMI

O parâmetro de modo de inicialização da AMI sinaliza ao Amazon EC2 qual modo de inicialização usar ao iniciar uma instância. Quando o parâmetro de modo de inicialização é definido como `uefi`, o EC2 tenta iniciar a instância em UEFI. Se o sistema operacional não estiver configurado para oferecer suporte a UEFI, a execução da instância não terá êxito.

Parâmetro de modo de inicialização preferencial UEFI

É possível criar AMIs que suportem UEFI e Legacy BIOS usando o parâmetro `uefi-preferred` do modo de inicialização. Quando o parâmetro de modo de inicialização é definido como `uefi-preferred`, e se o tipo de instância oferecer suporte a UEFI, a instância será iniciada em UEFI. Se o tipo de instância não for compatível com UEFI, ela será iniciada em BIOS legado.

> **Warning**
>
> Alguns recursos, como o UEFI Secure Boot, só estão disponíveis em instâncias que inicializadas em UEFI. Quando você usa o parâmetro do modo de inicialização `uefi-preferred` da AMI com um tipo de instância que não ofereça suporte a UEFI, a instância será iniciada como BIOS legado e o recurso dependente de UEFI será desativado. Se você confia na disponibilidade de um recurso dependente de UEFI, defina o parâmetro do modo de inicialização da AMI como `uefi`.

Modos de inicialização padrão para tipos de instância

- Tipos de instância Graviton: UEFI
- Tipos de instância Intel e AMD: BIOS legado

Como executar tipos de instâncias Intel e AMD em UEFI

Most Intel and AMD instance types pode ser executado em UEFI e BIOS herdado. Para usar UEFI, é preciso selecionar uma AMI com o parâmetro de modo de inicialização definido como `uefi` ou `uefi-preferred`, e o sistema operacional contido na AMI deve ser configurado para oferecer suporte a UEFI.

Tópicos do modo de inicialização

- Executar uma instância
- Determinar o parâmetro de modo de inicialização de uma AMI
- Determinar os modos de inicialização compatíveis com um tipo de instância
- Determinar o modo de inicialização de uma instância
- Determina o modo de inicialização do sistema operacional
- Definir o modo de inicialização de uma AMI
- Variáveis UEFI
- UEFI Secure Boot

Executar uma instância

É possível iniciar uma instância no modo de inicialização UEFI ou BIOS legado.

Tópicos

- Limitações
- Considerações
- Requisitos para iniciar uma instância em UEFI

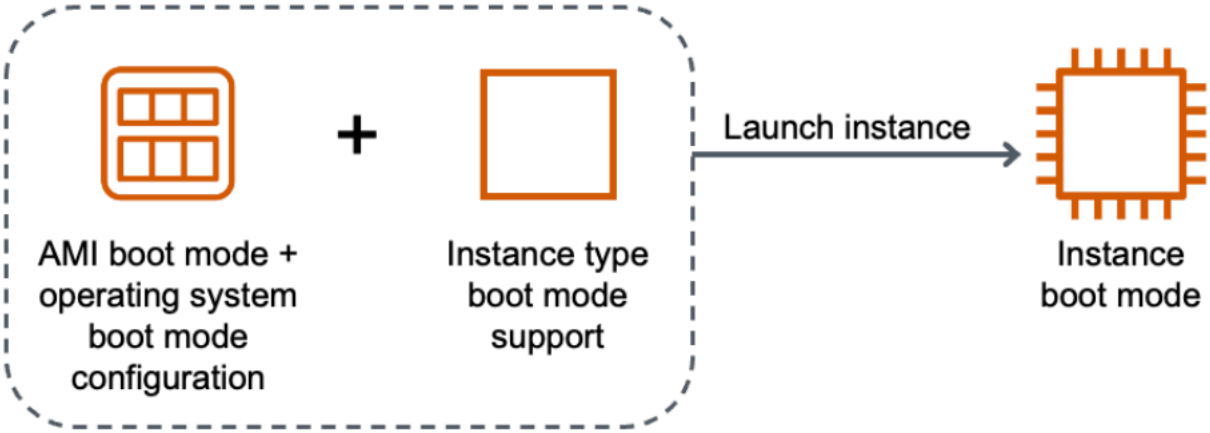
Limitações

A inicialização UEFI não tem compatibilidade em zonas locais, zonas do Wavelength ou com AWS Outposts.

Considerações

Considere o seguinte ao iniciar uma instância:

- O modo de inicialização da instância é determinado pela configuração da AMI, pelo sistema operacional contido nela e pelo tipo de instância, ilustrado pela imagem a seguir:



A tabela a seguir mostra que o modo de inicialização de uma instância (indicado pela coluna Modo de inicialização da instância resultante) é determinado por uma combinação do parâmetro do modo de inicialização da AMI (coluna 1), a configuração do modo de inicialização do sistema operacional contida na AMI (coluna 2) e o suporte ao modo de inicialização do tipo de instância (coluna 3).

Parâmetro do modo de inicialização da AMI	Configuração do modo de inicialização do sistema operacional	Suporte ao modo de inicialização do tipo de instância	Modo de inicialização da instância resultante
UEFI	UEFI	UEFI	UEFI
BIOS legado	BIOS legado	BIOS legado	BIOS legado
UEFI preferencial	UEFI	UEFI	UEFI
UEFI preferencial	UEFI	UEFI e BIOS legado	UEFI
UEFI preferencial	BIOS legado	BIOS legado	BIOS legado

Parâmetro do modo de inicialização da AMI	Configuração do modo de inicialização do sistema operacional	Suporte ao modo de inicialização do tipo de instância	Modo de inicialização da instância resultante
UEFI preferencial	BIOS legado	UEFI e BIOS legado	BIOS legado
Nenhum modo de inicialização especificado - ARM	UEFI	UEFI	UEFI
Nenhum modo de inicialização especificado - x86	BIOS legado	UEFI e BIOS legado	BIOS legado

- Modos de inicialização padrão:
  - Tipos de instância Graviton: UEFI
  - Tipos de instância Intel e AMD: BIOS legado
- Os tipos de instância Intel e AMD compatíveis com UEFI, além de BIOS herdado:
  - Todas as instâncias criadas com base no AWS Nitro System, exceto: instâncias bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 e VT1

Para ver os tipos de instância disponíveis com suporte a UEFI em uma região específica

Os tipos de instância disponíveis variam de acordo com a Região da AWS. Para ver os tipos de instâncias disponíveis com suporte a UEFI em uma região, use o comando describe-instance-types com o parâmetro `--region`. Se você omitir o parâmetro `--region`, sua região padrão será usada na solicitação. Inclua o parâmetro `--filters` para definir o escopo dos resultados para os tipos de instância com suporte a UEFI e o parâmetro `--query` para definir o escopo da saída para o valor de `InstanceType`.

Use o comando referente ao seu sistema operacional.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --
query "InstanceTypes[*].[InstanceType]" --output text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: False

InstanceType
------------
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
```

```
c5.9xlarge
...
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].
[InstanceType]" --output text | sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
c5.large
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {
     $_.SupportedBootModes -Contains "uefi" -and `
     $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
     } | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
...
```

Para ver os tipos de instância disponíveis com suporte a UEFI Secure Boot e variáveis persistentes não voláteis em uma região específica

Atualmente, as instâncias bare metal não oferecem suporte a UEFI Secure Boot e variáveis não voláteis. Use o comando describe-instance-types conforme descrito no exemplo anterior, mas filtre as instâncias bare metal, incluindo o filtro `Name=bare-metal,Values=false`. Para obter informações sobre o UEFI Secure Boot, consulte UEFI Secure Boot.

Use o comando referente ao seu sistema operacional.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
 text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType     SupportedBootModes  BareMetal SupportedArchitectures
------------     ------------------  --------- ----------------------
a1.2xlarge       {uefi}                  False arm64
a1.4xlarge       {uefi}                  False arm64
a1.large         {uefi}                  False arm64
```

```
a1.medium        {uefi}                 False arm64
a1.xlarge        {uefi}                 False arm64
c5.12xlarge      {legacy-bios, uefi}    False x86_64
c5.18xlarge      {legacy-bios, uefi}    False x86_64
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-
mode,Values=uefi Name=bare-metal,Values=false Name=processor-info.supported-
architecture,Values=x86_64 --query "InstanceTypes[*].[InstanceType]" --output text |
 sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False -and `
        $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType    SupportedBootModes  BareMetal SupportedArchitectures
------------    ------------------  --------- ----------------------
c5.12xlarge     {legacy-bios, uefi}     False x86_64
c5.18xlarge     {legacy-bios, uefi}     False x86_64
c5.24xlarge     {legacy-bios, uefi}     False x86_64
c5.2xlarge      {legacy-bios, uefi}     False x86_64
c5.4xlarge      {legacy-bios, uefi}     False x86_64
c5.9xlarge      {legacy-bios, uefi}     False x86_64
```

Requisitos para iniciar uma instância em UEFI

Para iniciar uma instância no modo de inicialização UEFI, é preciso selecionar um tipo de instância com suporte a UEFI e configurar a AMI e o sistema operacional para UEFI, da seguinte forma:

Tipo de instância

Ao iniciar uma instância, é preciso selecionar um tipo de instância com suporte a UEFI. Para ter mais informações, consulte Determinar os modos de inicialização compatíveis com um tipo de instância.

AMI

Ao iniciar uma instância, é preciso selecionar uma AMI configurada para UEFI. A AMI deve ser configurada da seguinte forma:

- Sistema operacional: o sistema operacional contido na AMI deve ser configurado para usar UEFI; caso contrário, a inicialização da instância falhará. Para ter mais informações, consulte Determina o modo de inicialização do sistema operacional.
- Parâmetro de modo de inicialização da AMI: o parâmetro de modo de inicialização da AMI deve ser definido como `uefi` ou `uefi-preferred`. Para ter mais informações, consulte Determinar o parâmetro de modo de inicialização de uma AMI.

Linux: a AWS fornece somente AMIs do Linux configuradas para oferecer suporte para a UEFI em relação aos tipos de instância baseados no Graviton. Para usar Linux em outros tipos de instância UEFI, é necessário configurar a AMI, importar a AMI por meio do VM Import/Export, ou importar a AMI por meio do CloudEndure.

Windows: as seguintes AMIs do Windows oferecem suporte para a UEFI:

- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Determinar o parâmetro de modo de inicialização de uma AMI

O parâmetro de modo de inicialização da AMI é opcional. Uma AMI pode ter um dos seguintes valores de parâmetro de modo de inicialização: `uefi`, `legacy-bios` ou `uefi-preferred`.

Algumas AMIs não têm um parâmetro de modo de inicialização. Quando uma AMI não tem parâmetro de modo de inicialização, as instâncias executadas a partir dela usam o valor padrão do tipo de instância, que é `uefi` no Graviton e `legacy-bios` nos tipos de instância Intel e AMD.

Console

Para determinar o parâmetro de modo de inicialização de uma AMI (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMIs e, em seguida, selecione a AMI.
3. Inspecione o campo Modo de inicialização.
   - Um valor de uefi indica que a AMI é compatível com a UEFI.
   - Um valor de uefi-preferred indica que a AMI é compatível tanto com a UEFI quanto a BIOS legada.
   - Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

Para determinar o parâmetro de modo de inicialização de uma AMI ao executar uma instância (console)

Ao executar uma instância usando o assistente de instância de execução, na etapa de selecionar uma AMI, verifique o campo Boot mode (Modo de inicialização). Para ter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).

AWS CLI

Para determinar o parâmetro de modo de inicialização de uma AMI (AWS CLI)

Use a operação describe-images para determinar o modo de inicialização de uma AMI.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890

{
```

```
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm",
            "BootMode":
 "uefi"
        }
    ]
}
```

No saída, o campo `BootMode` indica o modo de inicialização da AMI. Um valor de `uefi` indica que a AMI oferece suporte a UEFI. Um valor de `uefi-preferred` indica que a AMI oferece suporte tanto a UEFI quanto a BIOS legado. Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

PowerShell

Para determinar o parâmetro de modo de inicialização de uma AMI (Tools for PowerShell)

Use o Cmdlet Get-EC2Image para determinar o modo de inicialização de uma AMI.

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
 Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

No saída, o campo `BootMode` indica o modo de inicialização da AMI. Um valor de `uefi` indica que a AMI oferece suporte a UEFI. Um valor de `uefi-preferred` indica que a AMI oferece suporte tanto a UEFI quanto a BIOS legado. Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

Determinar os modos de inicialização compatíveis com um tipo de instância

É possível usar a AWS CLI ou oTools for PowerShell para determinar os modos de inicialização com suporte em um tipo de instância.

Para determinar os modos de inicialização com suporte por um tipo de instância

É possível usar os métodos abaixo para determinar os modos de inicialização com suporte em um tipo de instância.

AWS CLI

É possível usar o comando describe-instance-types para determinar os modos de inicialização com suporte em um tipo de instância. A incluir o parâmetro `--query`, é possível filtrar a saída. Neste exemplo, a saída é filtrada para retornar somente os modos de inicialização aceitos.

O exemplo a seguir mostra que `m5.2xlarge` suporta ambos os modos de inicialização UEFI e BIOS legado.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Saída esperada:

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

O exemplo a seguir mostra que `t2.xlarge` suporta apenas BIOS legado.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Saída esperada:

```
[
    [
        "legacy-bios"
```

```
    ]
]
```

PowerShell

É possível usar o Cmdlet da Get-EC2InstanceType (Tools for PowerShell) para determinar os modos de inicialização com suporte em um tipo de instância.

O exemplo a seguir mostra que `m5.2xlarge` suporta ambos os modos de inicialização UEFI e BIOS legado.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
 InstanceType, SupportedBootModes
```

Saída esperada:

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

O exemplo a seguir mostra que `t2.xlarge` suporta apenas BIOS legado.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
 InstanceType, SupportedBootModes
```

Saída esperada:

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Determinar o modo de inicialização de uma instância

O modo de inicialização de uma instância é exibido no campo Modo de inicialização no console do Amazon EC2 e pelo parâmetro `currentInstanceBootMode` na AWS CLI.

Quando uma instância é iniciada, o valor do parâmetro de modo de inicialização é determinado pelo valor do parâmetro de modo de inicialização da AMI usado para iniciá-la, da seguinte maneira:

- Uma AMI com um parâmetro de modo de inicialização `uefi` cria uma instância com um parâmetro `currentInstanceBootMode` de `uefi`.

- Uma AMI com um parâmetro de modo de inicialização `legacy-bios` cria uma instância com um parâmetro `currentInstanceBootMode` de `legacy-bios`.
- Uma AMI com um parâmetro de modo de inicialização `uefi-preferred` cria uma instância com um parâmetro `currentInstanceBootMode` de `uefi` se o tipo de instância oferecer suporte a UEFI, caso contrário, cria uma instância com um parâmetro `currentInstanceBootMode` de `legacy-bios`.
- Uma AMI sem valor de parâmetro no modo de inicialização cria uma instância com um valor de parâmetro `currentInstanceBootMode` que é dependente se a arquitetura da AMI é ARM ou x86, e do modo de inicialização com suporte pelo tipo de instância. O modo de inicialização padrão é `uefi` nos tipos de instância Graviton e `legacy-bios` nos tipos de instância Intel e AMD.

Console

Para determinar o modo de inicialização de uma instância (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Details (Detalhes), verifique o campo Boot mode (Modo de inicialização).

AWS CLI

Para determinar o modo de inicialização de uma instância (AWS CLI)

Use o comando describe-instances para determinar o modo de inicialização de uma instância. Você também pode determinar o modo de inicialização da AMI que foi usada para criar a instância.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
```

```
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                   "BootMode": "uefi",
                   "CurrentInstanceBootMode": "uefi"
                }
            ],
            "OwnerId": "1234567890",
            "ReservationId": "r-1234567890abcdef0"
        }
    ]
}
```

PowerShell

Para determinar o modo de inicialização de uma instância (Tools for PowerShell)

Use o CmdletGet-EC2Image para determinar o modo de inicialização de uma instância. Você também pode determinar o modo de inicialização da AMI que foi usada para criar a instância.

Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId

BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0265446f88eb4021b
```

Na saída, os parâmetros a seguir descrevem o modo de inicialização:

- `BootMode`: o modo de inicialização da AMI que foi usada para criar a instância.
- `CurrentInstanceBootMode`: o modo de inicialização usado para inicializar a instância na inicialização ou na execução.

Determina o modo de inicialização do sistema operacional

O modo de inicialização da AMI orienta o Amazon EC2 sobre o modo de inicialização que deve ser usado para inicializar uma instância. Para verificar se o sistema operacional da instância está

configurado para a UEFI, é necessário se conectar à instância usando SSH (instâncias do Linux) ou RDP (instâncias do Windows).

Use as instruções para o sistema operacional da sua instância.

Linux

Para determinar o modo de inicialização do sistema operacional da instância

1. Conecte-se à instância do Linux usando SSH.
2. Para exibir o modo de inicialização do sistema operacional, tente um dos seguintes procedimentos:

   - Execute o comando a seguir.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Saída esperada de uma instância inicializada no modo de inicialização UEFI

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

   - Execute o seguinte comando para verificar a existência do diretório `/sys/firmware/efi`. Esse diretório só existirá se a instância for inicializada usando UEFI. Se o diretório não existir, o comando retornará `Legacy BIOS Boot Detected`.

     ```
     [ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
      "Legacy BIOS Boot Detected"
     ```

     Saída esperada de uma instância inicializada no modo de inicialização UEFI

     ```
     UEFI Boot Detected
     ```

     Saída esperada de uma instância inicializada no modo de inicialização BIOS legado

     ```
     Legacy BIOS Boot Detected
     ```

- Execute o seguinte comando para verificar se EFI aparece na saída `dmesg`.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

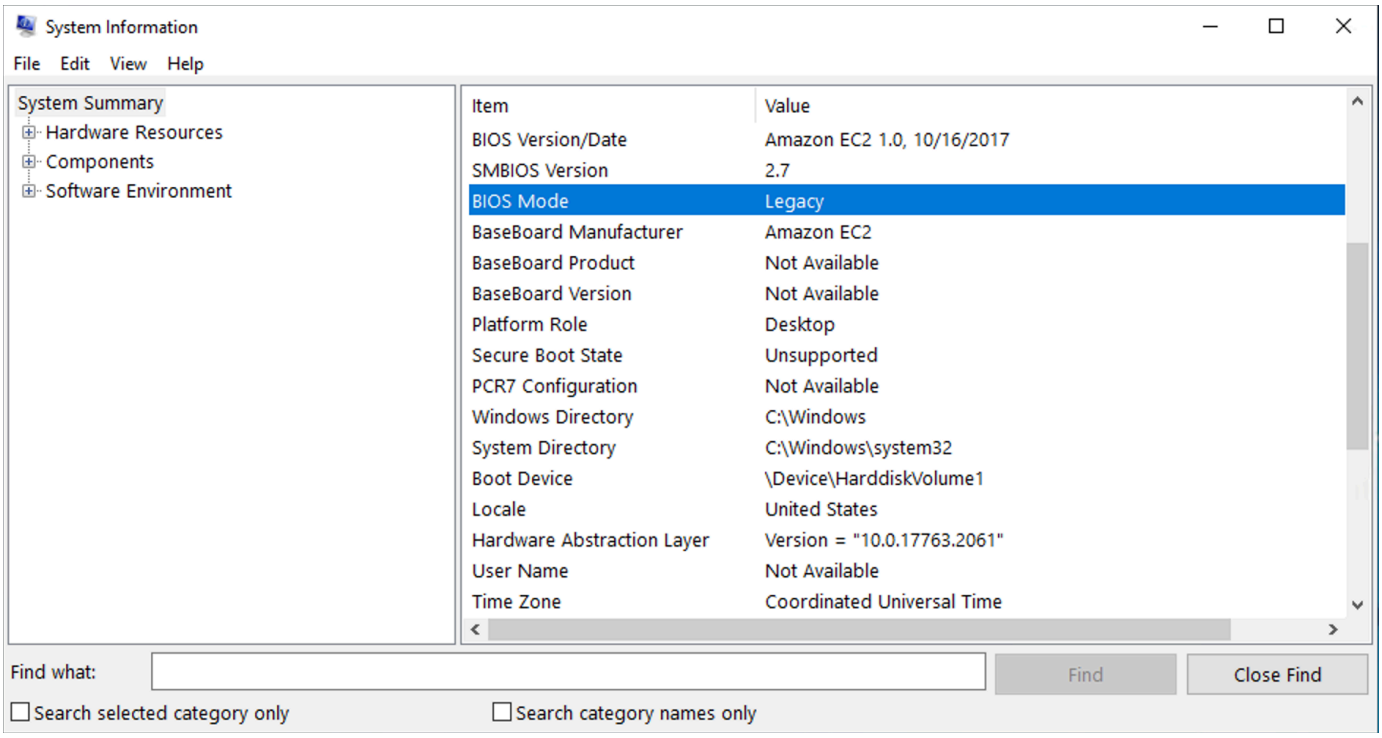
Saída esperada de uma instância inicializada no modo de inicialização UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Para determinar o modo de inicialização do sistema operacional da instância

1. Conecte-se à instância do Windows usando RDP.
2. Acesse System Information (Informações do sistema) e verifique a linha BIOS Mode (Modo BIOS).



Definir o modo de inicialização de uma AMI

Ao criar uma AMI usando o comando register-image, é possível definir o modo de inicialização da AMI como `uefi`, `legacy-bios` ou `uefi-preferred`.

Quando o modo de inicialização da AMI estiver definido como `uefi-preferred`, a instância será inicializada da seguinte forma:

- Para tipos de instância que ofereçam suporte a UEFI e BIOS legado (por exemplo, `m5.large`), a instância será inicializada usando UEFI.
- Para tipos de instância que ofereçam suporte somente a BIOS legado (por exemplo, `m4.large`), a instância será inicializada usando BIOS legado.

> **Note**
>
> Se você definir o modo de inicialização da AMI como `uefi-preferred`, o sistema operacional deverá oferecer suporte à capacidade de inicialização tanto com UEFI quanto com BIOS legado.
> Atualmente, você não pode usar o comando register-image para criar uma AMI que ofereça suporte a NitroTPM e UEFI preferencial.

> **Warning**
>
> Alguns recursos, como o UEFI Secure Boot, só estão disponíveis em instâncias que inicializadas em UEFI. Quando você usa o parâmetro do modo de inicialização `uefi-preferred` da AMI com um tipo de instância que não ofereça suporte a UEFI, a instância será iniciada como BIOS legado e o recurso dependente de UEFI será desativado. Se você confia na disponibilidade de um recurso dependente de UEFI, defina o parâmetro do modo de inicialização da AMI como `uefi`.

Para converter uma instância existente baseada em BIOS legado para UEFI, ou uma instância existente baseada em UEFI para BIOS legado, é preciso executar uma série de etapas: primeiro, modifique o volume e o sistema operacional da instância para oferecer suporte ao modo de inicialização selecionado. Em seguida, crie um snapshot do volume. Por fim, use register-image para criar a AMI usando o snapshot.

Não é possível definir o modo de inicialização de uma AMI usando o comando create-image. Com create-image, a AMI herda o modo de inicialização da instância do EC2 usada para criar a AMI. Por exemplo, se você criar uma AMI a partir de uma instância do EC2 executando em BIOS legado, o modo de inicialização da AMI será configurado como `legacy-bios`. Se você criar uma AMI a partir de uma instância do EC2 que tenha sido executada usando uma AMI com um modo de inicialização definido como `uefi-preferred`, a AMI criada também terá seu modo de inicialização definido como `uefi-preferred`.

> **Warning**
>
> Definir o parâmetro de modo de inicialização da AMI não configura automaticamente o sistema operacional para o modo de inicialização especificado. Antes de prosseguir com essas etapas, é preciso fazer modificações adequadas no volume e no sistema operacional da instância para oferecer suporte à inicialização usando o modo de inicialização selecionado, caso contrário, a AMI resultante não será utilizável. Por exemplo, caso esteja realizando a conversão de uma instância do Windows baseada em BIOS legado para a UEFI, você poderá usar a ferramenta MBR2GPT da Microsoft para converter o disco do sistema de MBR para GPT. As modificações necessárias são específicas do sistema operacional. Para obter mais informações, consulte o manual do sistema operacional.

Para definir o modo de inicialização de uma AMI (AWS CLI)

1. Faça as modificações adequadas no volume e no sistema operacional da instância para oferecer suporte à inicialização através do modo de inicialização selecionado. As modificações necessárias são específicas do sistema operacional. Para obter mais informações, consulte o manual do sistema operacional.

   > **Note**
   >
   > Se você não executar esta etapa, a AMI não será utilizável.

2. Para localizar o ID do volume da instância, use o comando describe-instances. Você criará um snapshot desse volume na próxima etapa.

   ```
   aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
   ```

   Saída esperada

```
...
            "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/sda1",
                            "Ebs": {
                                "AttachTime": "",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-1234567890abcdef0"
                            }
                        }
                        ...
```

3. Para criar um snapshot do volume, use o comando create-snapshot. Use o ID do volume da etapa anterior.

```
aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
description "add text"
```

Saída esperada

```
{
 "Description": "add text",
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. Guarde o ID do snapshot na saída da etapa anterior.
5. Aguarde até que a criação do snapshot seja `completed` antes de ir para a próxima etapa. Para consultar o estado do snapshot, use o comando describe-snapshots.

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Exemplo de saída

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. Para criar uma nova AMI, use o comando register-image. Use o ID de snapshot que você guardou na etapa anterior.

   - Para definir o modo de inicialização como UEFI, adicione o parâmetro `--boot-mode` ao comando e especifique `uefi` como o valor.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

   - Para definir o modo de inicialização como `uefi-preferred`, adicione o parâmetro `--boot-mode` ao comando e especifique `uefi-preferred` como o valor.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
```

```
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

Saída esperada

```
{
"ImageId": "ami-new_ami_123"
}
```

7. Para verificar se a AMI recém-criada tem o modo de inicialização especificado na etapa anterior, use o comando describe-images.

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Saída esperada

```
{
  "Images": [
   {
   "Architecture": "x86_64",
   "CreationDate": "2021-01-06T14:31:04.000Z",
   "ImageId": "ami-new_ami_123",
   "ImageLocation": "",
   ...
   "BootMode": "uefi"
   }
   ]
}
```

8. Execute uma nova instância usando a AMI recém-criada.

   Se o modo de inicialização da AMI for `uefi` ou `legacy-bios`, as instâncias criadas a partir dessa AMI terão o mesmo modo de inicialização da AMI. Se o modo de inicialização da AMI for `uefi-preferred`, a instância será inicializada usando UEFI se o tipo de instância oferecer

suporte a UEFI, caso contrário, a instância será inicializada usando o BIOS legado. Para ter mais informações, consulte Considerações.

9. Para verificar se a nova instância tem o modo de inicialização esperado, use o comando describe-instances.

Variáveis UEFI

Quando você inicia uma instância em que o modo de inicialização é definido como UEFI, um armazenamento de chave-valor para variáveis é criado. O armazenamento pode ser usado pela UEFI e pelo sistema operacional da instância para armazenar variáveis UEFI.

As variáveis UEFI são usadas pelo carregador de inicialização e pelo sistema operacional para configurar o startup antecipado do sistema. Eles permitem que o sistema operacional gerencie determinadas configurações do processo de inicialização, como a ordem de inicialização, ou gerencie as chaves para o UEFI Secure Boot.

> **Warning**
>
> Qualquer pessoa que possa se conectar à instância (e possivelmente a qualquer software em execução na instância) ou qualquer pessoa com permissão para usar a API GetInstanceUefiData na instância pode ler as variáveis. Você nunca deve armazenar dados sigilosos, como senhas ou informações de identificação pessoal, no armazenamento de variáveis UEFI.

Persistência de variáveis UEFI

- Para instâncias que foram iniciadas até 10 de maio de 2022, as variáveis UEFI são apagadas ao reinicializar ou parar.
- Para instâncias iniciadas a partir e 11 de maio de 2022, as variáveis UEFI marcadas como não voláteis persistem na reinicialização e na parada/início.
- As instâncias bare metal não preservam variáveis não voláteis da UEFI nas operações de parada/início da instância.

UEFI Secure Boot

O UEFI Secure Boot baseia-se no longo processo de inicialização segura do Amazon EC2, e fornece mais proteção abrangente que ajuda os clientes a proteger o software de ameaças que persistem durante as reinicializações. Ele garante que a instância inicialize apenas o software assinado com chaves criptográficas. As chaves são armazenadas no banco de dados de chaves do armazenamento de variáveis não voláteis UEFI. O UEFI Secure Boot impede a modificação não autorizada do fluxo de inicialização da instância.

Tópicos

- Como funciona o UEFI Secure Boot
- Iniciar uma instância com suporte a UEFI Secure Boot
- Verificar se uma instância está habilitada para o UEFI Secure Boot
- Criar uma AMI do Linux para oferecer suporte ao UEFI Secure Boot
- Como o blob binário AWS é criado

Como funciona o UEFI Secure Boot

O UEFI Secure Boot é um recurso especificado na UEFI que fornece verificação sobre o estado da cadeia de inicialização. Ele é projetado para garantir que apenas binários UEFI verificados criptograficamente sejam executados após a autoinicialização do firmware. Esses binários incluem drivers de UEFI e o carregador de inicialização principal, bem como componentes carregados em cadeia.

O UEFI Secure Boot especifica quatro bancos de dados principais que são usados em uma cadeia de confiança. Os bancos de dados são armazenados no armazenamento de variáveis UEFI.

A cadeia de confiança é a seguinte:

Banco de dados de chave de plataforma (PK)

O banco de dados de PK é a raiz de confiança. Ele contém uma única chave PK pública usada na cadeia de confiança para atualizar o banco de dados de chaves de troca de chave (KEK).

Para alterar o banco de dados de PK, você deve ter a chave PK privada para assinar uma solicitação de atualização. Isso inclui excluir o banco de dados de PK escrevendo uma chave PK vazia.

Banco de dados de chaves de troca de chave (KEK)

O banco de dados de KEK é uma lista de chaves KEK públicas que são usadas na cadeia de confiança para atualizar os bancos de dados de assinaturas (db) e de lista de negação (dbx).

Para alterar o banco de dados de KEK público, você deve ter a chave PK privada para assinar uma solicitação de atualização.

Banco de dados de assinaturas (db)

O banco de dados db é uma lista de chaves públicas e hashes que são usados na cadeia de confiança para validar todos os binários de inicialização UEFI.

Para alterar o banco de dados db, você deve ter a chave PK privada ou qualquer uma das chaves KEK privadas para assinar uma solicitação de atualização.

Banco de dados de lista de negação de assinatura (dbx)

O banco de dados dbx é uma lista de chaves públicas e hashes binários que não são confiáveis e são usados na cadeia de confiança como um arquivo de revogação.

O banco de dados dbx sempre tem precedência sobre todos os outros bancos de dados de chaves.

Para alterar o banco de dados dbx, você deve ter a chave PK privada ou qualquer uma das chaves KEK privadas para assinar uma solicitação de atualização.

O Fórum UEFI mantém um dbx disponível publicamente para muitos binários e certificados conhecidamente ruins em https://uefi.org/revocationlistfile.

Important

O UEFI Secure Boot impõe a validação da assinatura em qualquer binário UEFI. Para permitir a execução de um binário UEFI no UEFI Secure Boot, você o assina com qualquer uma das chaves db privadas descritas acima.

Por padrão, o UEFI Secure Boot é desabilitado e o sistema está no `SetupMode`. Quando o sistema estiver no `SetupMode`, todas as variáveis principais podem ser atualizadas sem uma assinatura criptográfica. Quando a PK está definida, o UEFI Secure Boot é habilitado e o SetupMode é encerrado.

Iniciar uma instância com suporte a UEFI Secure Boot

Quando você iniciar uma instância com os pré-requisitos a seguir, a instância validará automaticamente os binários de inicialização UEFI em relação ao banco de dados UEFI Secure Boot. Você também pode configurar o UEFI Secure Boot em uma instância após o início.

> **Note**
>
> O UEFI Secure Boot protege sua instância e seu sistema operacional contra modificações no fluxo de inicialização. Normalmente, o UEFI Secure Boot é configurado como parte da AMI. Se você criar uma nova AMI com parâmetros diferentes da AMI base, como alterar a `UefiData` dentro da AMI, é possível desabilitar o UEFI Secure Boot.

Pré-requisitos

AMIs Linux

Para iniciar uma instância Linux, a AMI Linux deve ter o UEFI Secure Boot habilitado.

O Amazon Linux oferece suporte ao UEFI Secure Boot a partir do AL2023 versão 2023.1. No entanto, o UEFI Secure Boot não está habilitado nas AMIs padrão. Para obter mais informações, consulte UEFI Secure Boot no Guia do usuário do AL2023. As versões mais antigas das AMIs do Amazon Linux não estão habilitadas para o UEFI Secure Boot. Para usar uma AMI compatível, é necessário executar várias etapas de configuração em sua própria AMI do Linux. Para ter mais informações, consulte Criar uma AMI do Linux para oferecer suporte ao UEFI Secure Boot.

AMIs Windows

Para iniciar uma instância Windows, a AMI Windows deve ter o UEFI Secure Boot habilitado.

As seguintes AMIs do Windows são pré-configuradas para habilitar o UEFI Secure Boot com chaves Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base

- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Atualmente, não oferecemos suporte à importação do Windows com o UEFI Secure Boot o comando import-image.

Tipo de instância

- Compatível: todos os tipos de instâncias virtualizadas que são compatíveis com UEFI também são compatíveis com UEFI Secure Boot. Para ver os tipos de instância compatíveis com o UEFI Secure Boot, consulte Considerações.
- Não compatível: os tipos de instância bare metal não são compatíveis com UEFI Secure Boot.

Verificar se uma instância está habilitada para o UEFI Secure Boot

Instâncias do Linux

É possível usar o utilitário `mokutil` para verificar se uma instância do Linux está habilitada para o UEFI Secure Boot. Se o `mokutil` não estiver instalado em sua instância, você precisará instalá-lo. Para obter instruções de instalação para o Amazon Linux 2, consulte https://docs.aws.amazon.com/linux/al2/ug/find-install-software.html. Para outras distribuições do Linux, consulte a documentação específica.

Verificar se uma instância do Linux está habilitada para o UEFI Secure Boot

Execute o comando a seguir como `root` na instância.

```
mokutil --sb-state
```

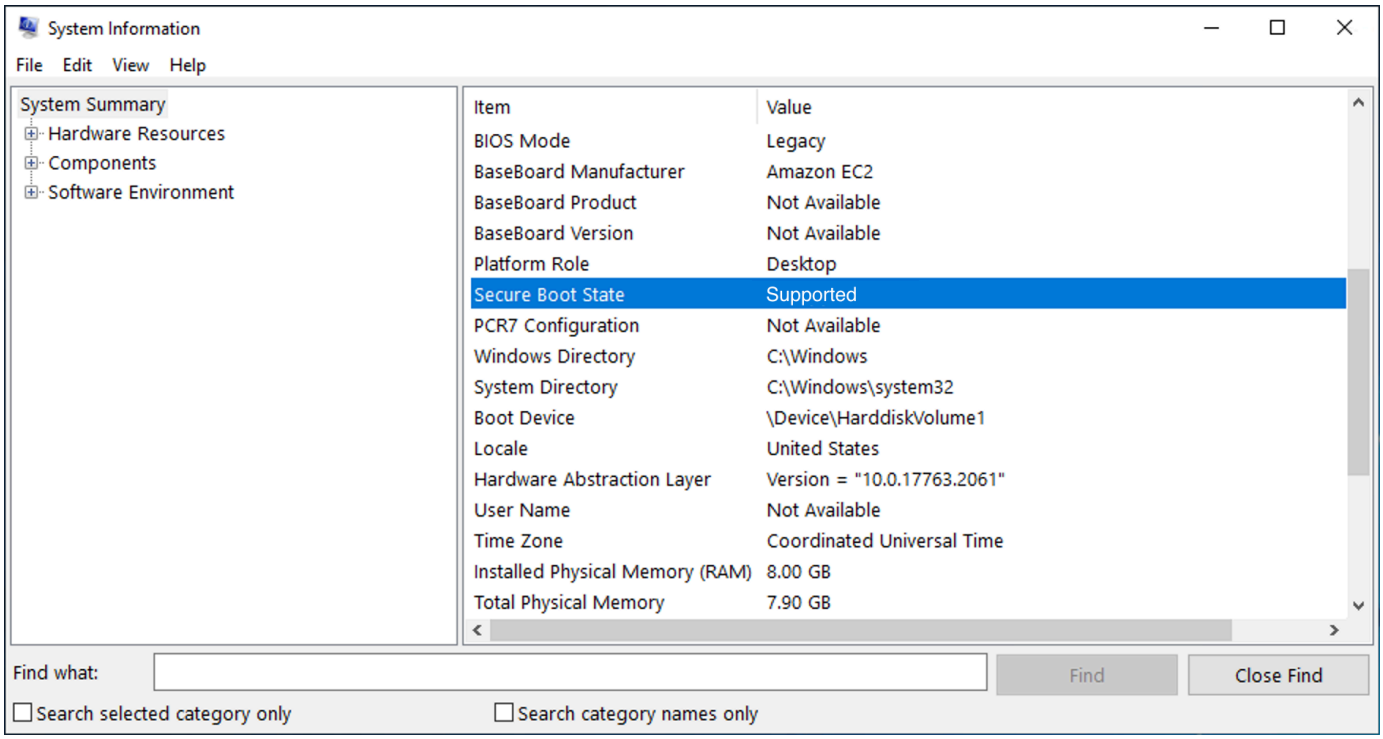
Saída esperada:

- Se o UEFI Secure Boot estiver habilitado, a saída conterá `SecureBoot enabled`.
- Se o UEFI Secure Boot não estiver habilitado, a saída conterá `SecureBoot disabled` ou `Failed to read SecureBoot`.

Instâncias do Windows

Para verificar se uma instância do Windows está habilitada para o UEFI Secure Boot

1. Abra a ferramenta msinfo32.
2. Verifique o campo Secure Boot State (Estado do Secure Boot). Supported (Com suporte) indica que o UEFI Secure Boot está habilitado.



Você também pode usar o cmdlet `Confirm-SecureBootUEFI` do Windows PowerShell para verificar o status do Secure Boot. Para obter mais informações sobre o cmdlet, consulte Confirm-SecureBootUEFI no site de documentação da Microsoft.

Criar uma AMI do Linux para oferecer suporte ao UEFI Secure Boot

Os procedimentos a seguir descrevem como criar seu próprio armazenamento de variáveis UEFI para inicialização segura com chaves privadas personalizadas. O Amazon Linux oferece suporte ao UEFI Secure Boot a partir do AL2023 versão 2023.1. Para obter mais informações, consulte UEFI Secure Boot no Guia do usuário do AL2023.

> **Important**
>
> Os procedimentos a seguir para criar uma AMI com suporte ao UEFI Secure Boot são destinados apenas a usuários avançados. Você deve ter conhecimento suficiente de SSL e do fluxo de inicialização da distribuição do Linux para usar esses procedimentos.

Pré-requisitos

- As seguintes ferramentas serão usadas:
  - OpenSSL: https://www.openssl.org/
  - efivar: https://github.com/rhboot/efivar
  - efitools: https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - Comando da AWS CLI get-instance-uefi-data
- Sua instância do Linux deve ter sido iniciada com uma AMI do Linux com suporte para o modo de inicialização UEFI e ter dados não voláteis presentes.

Instâncias recém-criadas sem chaves do UEFI Secure Boot são criadas em `SetupMode`, o que permite que você inscreva suas próprias chaves. Algumas AMIs vêm pré-configuradas com o UEFI Secure Boot, e você não pode alterar as chaves existentes. Se você desejar alterar as chaves, deve criar uma nova AMI com base na AMI original.

Você tem duas maneiras de propagar as chaves no armazenamento de variáveis, descritas na Opção A e na Opção B a seguir. A opção A descreve como fazer isso de dentro da instância, imitando o fluxo de hardware real. A opção B descreve como criar um blob binário, que será então passado como um arquivo codificado em base64 quando você criar a AMI. Para ambas as opções, você deve primeiro criar os três pares de chaves, que são usados para a cadeia de confiança.

Para criar uma AMI do Linux para oferecer suporte ao UEFI Secure Boot, primeiro crie os três pares de chaves e, em seguida, conclua a Opção A ou a Opção B:

- Para três pares de chaves
- Opção A: adicionar chaves ao armazenamento de variáveis de dentro da instância
- Opção B: criar um blob binário contendo um armazenamento de variáveis pré-preenchido

> **Note**
>
> Essas instruções só podem ser usadas para criar uma AMI do Linux. Se você precisar de uma AMI do Windows, use uma das AMIs com suporte para Windows. Para ter mais informações, consulte Iniciar uma instância com suporte a UEFI Secure Boot.

Para três pares de chaves

O UEFI Secure Boot é baseado nos três seguintes bancos de dados de chaves, que são usados em uma cadeia de confiança: a chave de plataforma (PK), a chave de troca de chaves (KEK) e o banco de dados de assinatura (db).[1]

Você cria cada chave na instância. Para preparar as chaves públicas em um formato válido para o padrão UEFI Secure Boot, você cria um certificado para cada chave. `DER` define o formato SSL (codificação binária de um formato). Em seguida, você converte cada certificado em uma lista de assinaturas UEFI, que é o formato binário entendido pelo UEFI Secure Boot. E, finalmente, você assina cada certificado com a chave relevante.

Tópicos

- Preparar para criar os pares de chaves
- Par de chaves 1: criar a chave da plataforma (PK)
- Par de chaves 2: criar a chave de troca de chaves (KEK)
- Par de chaves 3: criar o banco de dados de assinaturas (db)
- Assine a imagem de inicialização (kernel) com a chave privada

Preparar para criar os pares de chaves

Antes de criar os pares de chaves, crie um identificador exclusivo globalmente (GUID) para ser usado na geração de chaves.

1. Conecte-se à instância.
2. Execute o comando a seguir em um prompt de shell.

```
uuidgen --random > GUID.txt
```

Par de chaves 1: criar a chave da plataforma (PK)

A PK é a raiz da confiança para instâncias UEFI Secure Boot. A PK privada é usado para atualizar a KEK, que por sua vez pode ser usada para adicionar chaves autorizadas ao banco de dados de assinaturas (db).

O padrão X.509 é usado para criar o par de chaves. Para obter informações sobre o padrão, consulte X.509 na Wikipédia.

Para criar o PK

1. Crie a chave. Você deve nomear a variável PK.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Platform key/" -out PK.crt
   ```

   Os seguintes parâmetros são especificados:

   - `-keyout PK.key`: o arquivo da chave privada.
   - `-days 3650`: o número de dias em que o certificado é válido.
   - `-out PK.crt`: o certificado usado para criar a variável UEFI.
   - `CN=Platform key`: o nome comum (CN) para a chave. É possível inserir o nome da sua própria organização em vez de *Chave da plataforma*.
2. Crie o certificado.

   ```
   openssl x509 -outform DER -in PK.crt -out PK.cer
   ```
3. Converta o certificado em uma lista de assinaturas UEFI.

   ```
   cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
   ```
4. Assine a lista de assinaturas UEFI com a PK privada (autoassinada).

   ```
   sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
   ```

Par de chaves 2: criar a chave de troca de chaves (KEK)

A KEK privada é usada para adicionar chaves ao db, que é a lista de assinaturas autorizadas a inicializar no sistema.

Para criar a KEK

1. Crie a chave.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Crie o certificado.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Converta o certificado em uma lista de assinaturas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Assine a lista de assinaturas com a PK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Par de chaves 3: criar o banco de dados de assinaturas (db)

A lista db contém chaves autorizadas que estão autorizadas a ser inicializadas no sistema. Para modificar a lista, é necessária a KEK privada. As imagens de inicialização serão assinadas com a chave privada criada nesta etapa.

Para criar o db

1. Crie a chave.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Crie o certificado.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Converta o certificado em uma lista de assinaturas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Assine a lista de assinaturas com a KEK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Assine a imagem de inicialização (kernel) com a chave privada

Para o Ubuntu 22.04, as imagens a seguir exigem assinaturas.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Para assinar uma imagem

Utilize uma sintaxe semelhante à seguinte.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Você deve assinar todos os novos kernels. */boot/vmlinuz* geralmente será um link simbólico para o último kernel instalado.

Consulte a documentação da sua distribuição para saber sobre sua cadeia de inicialização e as imagens necessárias.

[1] Nossos agradecimentos à comunidade ArchWiki por todo o trabalho que eles fizeram. Os comandos para criar a PK, criar a KEK, criar o DB e assinar a imagem são de Criação de chaves, de autoria da Equipe de Manutenção do ArchWiki e/ou dos colaboradores do ArchWiki.

Opção A: adicionar chaves ao armazenamento de variáveis de dentro da instância

Depois de criar os três pares de chaves, é possível se conectar à sua instância e adicionar as chaves ao armazenamento de variáveis de dentro da instância, concluindo as etapas a seguir.

Etapas da Opção A:

- Etapa 1: iniciar uma instância que ofereça suporte ao UEFI Secure Boot
- Etapa 2: configurar uma instância para oferecer suporte ao UEFI Secure Boot

- Etapa 3: criar uma AMI da instância

Etapa 1: iniciar uma instância que ofereça suporte ao UEFI Secure Boot

Quando você iniciar uma instância com os pré-requisitos a seguir, a instância estará pronta para ser configurada para oferecer suporte ao UEFI Secure Boot. Você só pode habilitar o suporte ao UEFI Secure Boot em uma instância na inicialização; não será possível habilitá-lo mais tarde.

Pré-requisitos

- AMI: a AMI do Linux deve oferecer suporte ao modo de inicialização UEFI. Para verificar se a AMI oferece suporte ao modo de inicialização UEFI, o parâmetro do modo de inicialização da AMI deve ser UEFI. Para ter mais informações, consulte Determinar o parâmetro de modo de inicialização de uma AMI.

  Observe que fornece a AWS só fornece AMIs do Linux configuradas para compatibilidade com UEFI para tipos de instância baseados no Graviton. A AWS atualmente não fornece AMIs do Linux x86_64 que sejam compatíveis com o modo de inicialização UEFI. Você pode configurar a AMI para compatibilidade com o modo de inicialização UEFI para todas as arquiteturas. Para configurar sua própria AMI para compatibilidade com o modo de inicialização UEFI, é necessário realizar várias etapas de configuração em sua própria AMI. Para ter mais informações, consulte Definir o modo de inicialização de uma AMI.
- Tipo de instância: todos os tipos de instâncias virtualizadas com suporte a UEFI também oferecem suporte a UEFI Secure Boot. Os tipos de instância bare metal não oferecem suporte ao UEFI Secure Boot. Para ver os tipos de instância compatíveis com o UEFI Secure Boot, consulte Considerações.
- Inicie sua instância após o lançamento do UEFI Secure Boot. Somente instâncias iniciadas após 10 de maio de 2022 (quando o UEFI Secure Boot foi lançado) podem oferecer suporte ao UEFI Secure Boot.

Depois de iniciar sua instância, é possível verificar se ela está pronta para ser configurada para oferecer suporte à UEFI Secure Boot (em outras palavras, é possível prosseguir para a Etapa 2) verificando se os dados da UEFI estão presentes. A presença de dados de UEFI indica que dados não voláteis são persistidos.

Para verificar se sua instância está pronta para a Etapa 2

Use o comando get-instance-uefi-data e especifique o ID da instância.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

A instância estará pronta para a Etapa 2 se os dados da UEFI estiverem presentes na saída. Se a saída estiver vazia, a instância não poderá ser configurada para oferecer suporte ao UEFI Secure Boot. Isso pode acontecer se sua instância tiver sido iniciada antes que o suporte ao UEFI Secure Boot fique disponível. Inicie uma nova instância e tente novamente.

Etapa 2: configurar uma instância para oferecer suporte ao UEFI Secure Boot

Registre os pares de chaves no armazenamento de variáveis UEFI na instância

> **Warning**
>
> Você deve assinar suas imagens de inicialização depois de registrar as chaves, caso contrário, não poderá inicializar sua instância.

Depois que você criar as listas de assinaturas UEFI assinadas (`PK`, `KEK`, e `db`), elas devem ser registradas no firmware do UEFI.

A gravação na variável `PK` só será possível se:

- Ainda não houver PK registrada, o que será indicado se a variável `SetupMode` for `1`. Verifique isso usando o comando a seguir. A saída for `1` ou `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- A nova PK for assinada pela chave privada da PK existente.

Para registrar as chaves no seu armazenamento de variáveis UEFI

Os comandos a seguir devem ser executados na instância.

Se SetupMode estiver habilitado (o valor será 1), as chaves podem ser registradas executando os seguintes comandos na instância:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Para verificar se o UEFI Secure Boot está habilitado

Para verificar se o UEFI Secure Boot está habilitado, siga as etapas em Verificar se uma instância está habilitada para o UEFI Secure Boot.

Agora é possível exportar seu armazenamento de variáveis UEFI com o comando get-instance-uefi-data da CLI, ou prosseguir para a próxima etapa e assinar suas imagens de inicialização para reinicializar em uma instância habilitada para o UEFI Secure Boot.

Etapa 3: criar uma AMI da instância

Para criar uma AMI a partir da instância, é possível usar o console ou a API `CreateImage`, a CLI ou SDKs. Para obter instruções sobre o console, consulte Criação de uma AMI baseada no Amazon EBS. Para obter instruções sobre a API, consulte CreateImage.

> **Note**
>
> A API `CreateImage` copia automaticamente o armazenamento de variáveis UEFI da instância para a AMI. O console usa a API `CreateImage`. Depois de executar instâncias usando essa AMI, as instâncias terão o mesmo armazenamento de variáveis UEFI.

Opção B: criar um blob binário contendo um armazenamento de variáveis pré-preenchido

Depois de criar os três pares de chaves, é possível criar um blob binário contendo um armazenamento de variáveis pré-preenchido contendo as chaves do UEFI Secure Boot.

> **Warning**
>
> Você deverá assinar suas imagens de inicialização antes de registrar as chaves, caso contrário, não poderá inicializar sua instância.

Etapas da Opção B:

- Etapa 1: criar um novo armazenamento de variáveis ou atualizar um existente
- Etapa 2: carregar o blob binário na criação da AMI

Etapa 1: criar um novo armazenamento de variáveis ou atualizar um existente

É possível criar o armazenamento de variáveis offline, sem uma instância em execução, usando a ferramenta python-uefivars. A ferramenta pode criar um novo armazenamento de variáveis a partir de suas chaves. O script atualmente oferece suporte ao formato EDK2, ao formato AWS e a uma representação JSON que é mais fácil de editar com ferramentas de nível superior.

Para criar o armazenamento de variáveis offline sem uma instância em execução

1. Baixe a ferramenta no link a seguir.

```
https://github.com/awslabs/python-uefivars
```

2. Crie um novo armazenamento de variáveis a partir de suas chaves executando o comando a seguir. Isso criará um blob binário codificado em base64 em *your_binary_blob*.bin. A ferramenta também suporta a atualização de um blob binário através do parâmetro `-I`.

```
./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
 db.esl --dbx dbx.esl
```

Etapa 2: carregar o blob binário na criação da AMI

Use register-image para passar seus dados de armazenamento de variáveis UEFI. Para o parâmetro `--uefi-data`, especifique seu blob binário e para o parâmetro `--boot-mode`, especifique `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Como o blob binário AWS é criado

É possível usar as seguintes etapas para personalizar as variáveis do UEFI Secure Boot durante a criação da AMI. A KEK usado nessas etapas está atual desde de setembro de 2021. Se a Microsoft atualizar a KEK, você deverá usar a KEK mais recente.

Para criar o blob binário da AWS

1. Crie uma lista de assinaturas PK vazia.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Baixe os certificados de KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Empacote os certificados de KEK em uma lista de assinaturas UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Baixe os certificados de db da Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Gere a lista de assinaturas db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Baixe uma solicitação de alteração de dbx atualizada no link a seguir.

```
https://uefi.org/revocationlistfile
```

7. A solicitação de alteração de dbx que você baixou na etapa anterior já está assinada com a Microsoft KEK, então você precisa extraí-la ou descompactá-la. É possível usar os links a seguir.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Construa um armazenamento de variáveis UEFI usando o script `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/dbx-2021-April.bin
```

9. Verifique o blob binário e o armazenamento de variáveis UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. É possível atualizar o blob passando-o para a mesma ferramenta novamente.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/dbx-2021-April.bin
```

Saída esperada

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Encontrar uma AMI

Uma AMI inclui os componentes e as aplicações, como o sistema operacional e o tipo de volume raiz, necessários para iniciar uma instância. Para iniciar uma instância que atenda às suas necessidades, é necessário encontrar uma AMI adequada às suas exigências.

Ao selecionar uma AMI, considere os seguintes requisitos que você pode ter para as instâncias que deseja iniciar:

- A região: os IDs de AMI são exclusivos de cada região da AWS.
- O sistema operacional

- A arquitetura: 32 bits (`i386`), 64 bits (`x86_64`) ou ARM de 64 bits (`arm64`)
- O tipo de dispositivo raiz: Amazon EBS ou armazenamento de instâncias
- O provedor (por exemplo, Amazon Web Services)
- Software adicional (por exemplo, SQL Server)

Existem várias maneiras de encontrar uma AMI que atenda às suas necessidades. Este tópico descreve como encontrar uma AMI usando o console do Amazon EC2, a AWS CLI, o AWS Tools for Windows PowerShell e o AWS Systems Manager.

Tópicos

- Encontrar uma AMI usando o console do Amazon EC2
- Localizar uma AMI usando o AWS CLI
- Localizar uma AMI usando o AWS Tools for Windows PowerShell
- Encontrar uma AMI usando um parâmetro do Systems Manager
- Encontrar as AMIs mais recentes usando o Systems Manager
- Mais informações para encontrar AMIs

Encontrar uma AMI usando o console do Amazon EC2

É possível encontrar AMIs usando o console do Amazon EC2. É possível selecionar na lista de AMIs ao usar o assistente de inicialização de instância para iniciar a instância ou pesquisar todas as AMIs disponíveis usando a página Images (Imagens).

Encontrar uma AMI usando o assistente de inicialização de instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local. Os IDs da AMI são exclusivos de cada região da AWS.
3. No painel do console, selecione Launch instance (Executar instância).
4. (Novo console) Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e SO [imagem de máquina da Amazon]), escolha Quick Start (Início rápido), escolha o sistema operacional (SO) para sua instância e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon [AMI]), selecione uma das AMIs mais usadas na lista. Caso não veja a AMI

que deseja usar, escolha Browse more AMIs (Pesquisar mais AMIs) para navegar pelo catálogo completo de AMIs. Para ter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).

(Console antigo) Na guia Quick Start (Início rápido), selecione uma das AMIs mais usadas na lista. Se não encontrar a AMI necessária, escolha a guia My AMIs (Minhas AMIs), AWS Marketplace ou Community AMIs (AMIs da comunidade) para localizar outras AMIs. Para ter mais informações, consulte Etapa 1: Escolher uma imagem de máquina da Amazon (AMI).

Encontrar uma AMI usando a página de AMIs

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local. Os IDs da AMI são exclusivos de cada região da AWS.
3. No painel de navegação, selecione AMIs.
4. (Opcional) Use as opções de filtro e pesquisa para restringir o escopo da lista de AMIs exibidas e ver somente as AMIs correspondentes ao seu critério.

   Por exemplo, para listar todas as AMIs fornecidas pela AWS, escolha Imagens públicas. Em seguida, use as opções de pesquisa para aumentar o escopo da lista de AMIs exibidas. Escolha a barra de Pesquisa e, no menu, escolha Owner alias (Alias do proprietário), depois o operador = e, em seguida, o valor amazon. Para encontrar AMIs que correspondam a uma plataforma específica, por exemplo, Linux ou Windows, escolha novamente a barra Pesquisar para escolher Plataforma, depois o operador = e, em seguida, o sistema operacional na lista fornecida.
5. (Opcional) Escolha o ícone de Preferências para selecionar quais atributos de imagens serão exibidos, como o tipo de dispositivo raiz. Como alternativa, é possível selecionar uma AMI na lista e visualizar suas propriedades na guia Details (Detalhes).
6. Antes de selecionar uma AMI, é importante que você verifique se ela é baseada em um armazenamento de instâncias ou no Amazon EBS e se você está ciente dos efeitos dessa diferença. Para ter mais informações, consulte Armazenamento para o dispositivo raiz.
7. Para iniciar uma instância a partir dessa AMI, selecione-a e escolha Iniciar instância a partir da imagem. Para obter informações sobre como iniciar uma instância usando o console, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta. Se você não estiver pronto para executar a instância agora, anote o ID da AMI para consultar depois.

Localizar uma AMI usando o AWS CLI

É possível usar o comando describe-images da AWS CLI para listar somente as AMIs que atendem aos seus requisitos. Depois de localizar uma AMI que corresponda às suas necessidades, anote o ID de forma que você possa usá-lo para iniciar instâncias. Para obter mais informações, consulte Iniciar instância no Guia do usuário da AWS Command Line Interface.

O comando describe-images oferece suporte à filtragem de parâmetros. Por exemplo, use o parâmetro `--owners` para exibir AMIs públicas de propriedade da Amazon.

```
aws ec2 describe-images --owners amazon
```

É possível adicionar o seguinte filtro ao comando anterior para exibir somente AMIs do Windows.

```
--filters "Name=platform,Values=windows"
```

É possível adicionar o seguinte filtro ao comando anterior para exibir somente AMIs compatíveis com o Amazon EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

> **Important**
>
> Se você omitir o parâmetro `--owners` do comando `describe-images`, serão retornadas todas as imagens para as quais você tem permissões de inicialização, independentemente da propriedade.

Localizar uma AMI usando o AWS Tools for Windows PowerShell

É possível usar cmdlets do PowerShell para listar somente as AMIs do Windows que atendem aos seus requisitos. Para obter informações e exemplos, consulte Find an Amazon Machine Image Using Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

Depois de localizar uma AMI que corresponda às suas necessidades, anote o ID de forma que você possa usá-lo para iniciar instâncias. Para obter mais informações, consulte Launch an Amazon EC2 Instance Using Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

Encontrar uma AMI usando um parâmetro do Systems Manager

Ao iniciar uma instância usando o assistente de inicialização de instâncias do EC2 no console do Amazon EC2, é possível selecionar uma AMI na lista (descrita em Encontrar uma AMI usando o console do Amazon EC2) ou selecionar um parâmetro do AWS Systems Manager que aponte para um ID da AMI (descrito nesta seção). Se usar o código de automação para executar as instâncias, será possível especificar o parâmetro do Systems Manager em vez do ID de AMI.

Um parâmetro do Systems Manager é um par de chave-valor definido pelo cliente que pode ser criado no repositório de parâmetros do Systems Manager. O repositório de parâmetros fornece um armazenamento central para externalizar os valores de configuração da aplicação. Para obter mais informações, consulte o Parameter Store do AWS Systems Manager no Guia do usuário do AWS Systems Manager.

Ao criar um parâmetro que aponte para um ID de AMI, especifique o tipo de dado como `aws:ec2:image`. Especificar esse tipo de dado garante que, quando o parâmetro for criado, modificado ou validado, o valor dele será validado como um ID da AMI. Para obter mais informações, consulte Suporte a parâmetro nativo para IDs de imagem de máquina da Amazon no Guia do usuário do AWS Systems Manager.

Tópicos

- Casos de uso
- Permissões
- Limitações
- Executar uma instância usando um parâmetro de Systems Manager

Casos de uso

Ao usar os parâmetros do Systems Manager para apontar para IDs de AMI, é mais fácil para os usuários selecionar a AMI correta ao iniciar instâncias. Os parâmetros do Systems Manager também podem simplificar a manutenção do código de automação.

Mais fácil para os usuários

Se você precisar que as instâncias sejam iniciadas usando uma AMI específica, e se essa AMI for atualizada regularmente, recomendamos que você exija que os usuários selecionem um parâmetro do Systems Manager para localizar a AMI. Exigir que os usuários selecionem um parâmetro do Systems Manager garante que a AMI mais recente seja usada para iniciar instâncias.

Por exemplo, todo mês é possível criar em sua organização uma versão da AMI que tenha os patches mais recentes do sistema operacional e da aplicação. Além disso, exija que os usuários executem instâncias usando a versão mais recente da AMI. Para garantir que os usuários usem a versão mais recente, é possível criar um parâmetro do Systems Manager (por exemplo, `golden-ami`) que aponte para o ID da AMI correta. Toda vez que uma versão da AMI é criada, você atualiza o valor do ID de AMI no parâmetro para que ele sempre aponte para a AMI mais recente. Os usuários não precisam saber sobre as atualizações periódicas da AMI, porque eles continuarão selecionando sempre o mesmo parâmetro do Systems Manager todas as vezes. Usando um parâmetro do Systems Manager para a AMI, você facilita a seleção da AMI correta para uma inicialização da instância.

Simplificar a manutenção do código de automação

Se usar o código de automação para executar as instâncias, será possível especificar o parâmetro do Systems Manager em vez do ID de AMI. Se uma versão da AMI for criada, altere o valor do ID da AMI no parâmetro para que ele aponte para a AMI mais recente. O código de automação que faz referência ao parâmetro não precisa ser modificado toda vez que uma versão da AMI for criada. Isso simplifica a manutenção da automação e ajuda a reduzir os custos de implantação.

> **Note**
>
> As instâncias em execução não são afetadas quando você altera o ID da AMI para o qual o parâmetro do Systems Manager aponta.

Permissões

Se você usar parâmetros do Systems Manager que direcionem para IDs de AMI no assistente de inicialização de instâncias, deverá adicionar as seguintes permissões à política do IAM:

- `ssm:DescribeParameters`: concede permissão para visualizar e selecionar os parâmetros do Systems Manager.
- `ssm:GetParameters`: concede permissão para recuperar os valores dos parâmetros do Systems Manager.

Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações e exemplos de políticas do IAM, consulte Exemplo: uso do assistente de início de instância do EC2.

Limitações

As AMIs e os parâmetros do Systems Manager são específicos da região. Para usar o mesmo nome de parâmetro do Systems Manager entre regiões, crie um parâmetro do Systems Manager em cada região com o mesmo nome (por exemplo, `golden-ami`). Em cada região, aponte o parâmetro do Systems Manager para uma AMI nessa região.

Executar uma instância usando um parâmetro de Systems Manager

É possível executar uma instância usando o console ou a AWS CLI. Em vez de especificar um ID de AMI, é possível especificar um parâmetro do AWS Systems Manager que aponte para um ID de AMI.

New console

Encontrar uma AMI usando um parâmetro do Systems Manager (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel do console, selecione Launch instance (Executar instância).
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha Browse more AMIs (Procurar mais AMIs).
5. Escolha o botão de seta à direita da barra de pesquisa e escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager).
6. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido abaixo de Currently resolves to (Resolve atualmente para).
7. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.
8. Selecione a AMI na lista e escolha Select (Selecionar).

Para obter mais informações sobre como iniciar uma instância usando o assistente de inicialização de instância, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Old console

Encontrar uma AMI usando um parâmetro do Systems Manager (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel do console, selecione Launch instance (Executar instância).
4. Escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager) (no canto superior direito).
5. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido ao lado de Currently resolves to (Resolve atualmente para).
6. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.
7. Selecione a AMI na lista e escolha Select (Selecionar).

Para obter mais informações sobre como iniciar uma instância em uma AMI usando o assistente de inicialização de instância, consulte Etapa 1: Escolher uma imagem de máquina da Amazon (AMI).

Como executar uma instância usando um parâmetro do AWS Systems Manager em vez de um ID da AMI (AWS CLI)

O exemplo a seguir usa o parâmetro do Systems Manager `golden-ami` para executar uma instância `m5.xlarge`. O parâmetro aponta para um ID de AMI.

Para especificar o parâmetro no comando, use a seguinte sintaxe: `resolve:ssm:/`*`parameter-name`*, onde `resolve:ssm` é o prefixo padrão e `parameter-name` é o nome do parâmetro exclusivo. Observe que o nome do parâmetro faz distinção entre maiúsculas e minúsculas. As barras invertidas para o nome do parâmetro só são necessárias quando o parâmetro faz parte de uma hierarquia, por exemplo, `/amis/production/golden-ami`. Será possível omitir a barra invertida se o parâmetro não fizer parte de uma hierarquia.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances
```

```
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

Como executar uma instância usando uma versão específica de um parâmetro do AWS Systems Manager (AWS CLI)

Os parâmetros do Systems Manager são compatíveis com versão. Cada iteração de um parâmetro recebe um número de versão exclusivo. É possível referenciar a versão do parâmetro da seguinte forma `resolve:ssm:parameter-name:version`, onde `version` é o número de versão exclusivo. Por padrão, a versão mais recente do parâmetro é usada quando nenhuma versão é especificada.

O exemplo a seguir usa a versão 2 do parâmetro.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
    --instance-type m5.xlarge
    ...
```

Como executar uma instância usando um parâmetro público fornecido pela AWS

O Systems Manager fornece parâmetros públicos para as AMIs públicas fornecidas pela AWS. É possível usar os parâmetros públicos ao iniciar instâncias para garantir que está usando as AMIs mais recentes.

Para ter mais informações, consulte Encontrar as AMIs mais recentes usando o Systems Manager.

Encontrar as AMIs mais recentes usando o Systems Manager

O AWS Systems Manager fornece parâmetros públicos para as AMIs públicas mantidas pela AWS. É possível usar os parâmetros públicos ao iniciar instâncias para garantir que está usando as AMIs mais recentes. Por exemplo, o parâmetro público `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` está disponível em todas as regiões e sempre direciona para a versão mais recente da AMI do Amazon Linux 2023 para a arquitetura de arm64 em uma determinada região.

Os parâmetros públicos estão disponíveis ao usar os seguintes caminhos:

- Linux: `/aws/service/ami-amazon-linux-latest`
- Windows: `/aws/service/ami-windows-latest`

Para visualizar uma lista de todas as AMIs do Linux ou do Windows na região atual da AWS

Use o comando get-parameters-by-path da AWS CLI, apresentado a seguir para visualizar uma lista de todas as AMIs do Linux ou do Windows na região atual da AWS. O valor para o parâmetro `--path` é diferente para o Linux e para o Windows.

Para Linux:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

Para Windows:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

Como executar uma instância usando um parâmetro público

O exemplo apresentado a seguir especifica um parâmetro público do Systems Manager para o ID da imagem com a finalidade de iniciar uma instância usando a AMI do Amazon Linux 2023 mais recente.

Para especificar o parâmetro no comando, use a seguinte sintaxe: `resolve:ssm:`*`public-parameter`*, onde `resolve:ssm` é o prefixo padrão e *`public-parameter`* é o caminho e o nome do parâmetro público.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
    --instance-type m5.xlarge \
```

```
    --key-name MyKeyPair
```

Para obter mais informações, consulte Trabalhar com parâmetros públicos no Guia do usuário do AWS Systems Manager

Para obter exemplos que usam parâmetros do Systems Manager, consulte Query for the latest Amazon Linux AMI IDs Using AWS Systems Manager Parameter Store e Query for the Latest Windows AMI Using AWS Systems Manager Parameter Store.

Mais informações para encontrar AMIs

Para encontrar uma AMI do Amazon Linux 2023, consulte AL2023 on Amazon EC2 no Guia do usuário do Amazon Linux 2023.

Para encontrar uma AMI do Ubuntu, consulte Amazon EC2 AMI Locator no site Canonical Ubuntu.

Para encontrar uma AMI do RHEL, consulte Red Hat Enterprise Linux Images (AMI) Available on Amazon Web Services (AWS) no site da Red Hat.

AMIs compartilhadas

Uma AMI compartilhada é uma AMI que um desenvolvedor criou e disponibilizou para que outros desenvolvedores usem. Uma das maneiras mais fáceis de começar a usar o Amazon EC2 é usar AMIs compartilhadas com os componentes necessários e adicionar o conteúdo personalizado. Também é possível criar suas próprias AMIs e compartilhá-las com outros.

Use a AMI compartilhada sob seu próprio risco. A Amazon não pode responsabilizar-se pela integridade ou segurança das AMIs compartilhadas por outros usuários do Amazon EC2. Portanto, trate as AMIs compartilhadas como você faria com qualquer código estranho que considerasse implantar em seu próprio data center e execute a investigação aplicável. Recomendamos que você obtenha uma AMI de uma fonte confiável, como um provedor verificado.

Provedor verificado

No console do Amazon EC2, AMIs públicas de propriedade da Amazon ou de um parceiro verificado da Amazon são marcadas como Provedor verificado.

Você também pode usar o comando describe-images da AWS CLI para identificar as AMIs públicas provenientes de um provedor verificado. As imagens públicas de propriedade da Amazon ou de

um parceiro verificado têm um proprietário com alias, que é `amazon` ou `aws-marketplace`. Na saída da CLI, esses valores aparecem para `ImageOwnerAlias`. Outros usuários não podem dar um alias às AMIs deles. Isso permite que você encontre AMIs da Amazon ou de parceiros verificados facilmente.

Para se tornar um fornecedor verificado, você deve se registrar como vendedor no AWS Marketplace. Após o registro, você pode listar sua AMI no AWS Marketplace. Para obter mais informações, consulte Conceitos básicos como vendedor e Produtos baseados em AMIs no Guia do vendedor do AWS Marketplace.

Tópicos da AMI compartilhada

- Encontrar AMIs compartilhadas
- Tornar um AMI pública
- Compartilhe uma AMI com organizações ou unidades organizacionais específicas
- Compartilhar uma AMI com contas específicas da AWS
- Cancelar o compartilhamento de uma AMI com sua Conta da AWS
- Usar marcadores
- Diretrizes para AMIs em Linux compartilhadas

Se você estiver procurando informações sobre outros tópicos

- Para obter informações sobre como criar uma AMI, consulte the section called “Criar uma AMI em Linux com armazenamento de instâncias” ou the section called “Criação de uma AMI baseada no Amazon EBS”.
- Para obter informações sobre como criar, fornecer e manter suas aplicações no AWS Marketplace, consulte a Documentação do AWS Marketplace.

Encontrar AMIs compartilhadas

É possível usar o console do Amazon EC2 ou a linha de comando para encontrar AMIs compartilhadas.

As AMIs são um recurso regional. Ao pesquisar uma AMI compartilhada (pública ou privada), é necessário procurá-la na mesma região de onde ela é compartilhada. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para ter mais informações, consulte Copiar um AMI.

Tarefas

- Encontrar uma AMI compartilhada (console)
- Localizar uma AMI compartilhada (AWS CLI)
- Localizar uma AMI compartilhada (Tools for Windows PowerShell)
- Usar AMIs compartilhadas

Encontrar uma AMI compartilhada (console)

Para encontrar uma AMI privada usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens privadas. Estarão na lista todas as AMIs compartilhadas com você. Para refinar sua pesquisa, escolha a barra Search (Pesquisar) e use as opções de filtro fornecidas no menu.

Para encontrar uma AMI pública usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens públicas. Para refinar sua pesquisa, escolha o campo Search (Pesquisar) e use as opções de filtro fornecidas no menu.

Para encontrar AMIs públicas compartilhadas usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens públicas.
4. Selecione o campo Pesquisar e, nas opções de menu exibidas, escolha Owner alias (Alias do proprietário), = e depois amazon para exibir somente as imagens públicas da Amazon.

Para encontrar uma AMI pública de um provedor verificado usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha AMI Catalog (Catálogo de AMIs).
3. Escolha Community AMIs (AMIs da comunidade).
4. O rótulo de Provedor verificado indica as AMIs que são da Amazon ou de um parceiro verificado.

Localizar uma AMI compartilhada (AWS CLI)

Use o comando describe-images (AWS CLI) para listar as AMIs. É possível direcionar o escopo da lista para os tipos de AMI que lhe interessam, conforme exibido nos exemplos a seguir.

Exemplo: Listar todas as AMIs públicas

O comando a seguir lista todas as AMIs públicas, inclusive todas as AMIs públicas de sua propriedade.

```
aws ec2 describe-images --executable-users all
```

Exemplo: Listar AMIs permissões de execução explícita

O comando a seguir lista as AMIs para as quais você tenha permissões de execução explícita. Essa lista não inclui nenhuma AMI de sua propriedade.

```
aws ec2 describe-images --executable-users self
```

Exemplo: Listar AMIs pertencentes a fornecedores verificados

O comando a seguir lista as AMIs de propriedade de provedores verificados. As AMIs públicas de propriedade de fornecedores verificados (da Amazon ou de parceiros verificados) têm um proprietário com alias, que é exibido como `amazon` ou `aws-marketplace` no campo da conta. Isso ajuda você a encontrar facilmente AMIs de fornecedores verificados. Outros usuários não podem dar um alias às AMIs deles.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Exemplo: Listar AMIs de propriedade de uma conta

O comando a seguir lista as AMIs de propriedade da Conta da AWS especificada.

```
aws ec2 describe-images --owners 123456789012
```

Exemplo: Definir escopo das AMIs usando um filtro

Para reduzir o número de AMIs exibidas, use um filtro para listar somente os tipos de AMI que lhe interessam. Por exemplo, use o filtro a seguir para exibir somente AMIs com EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

Localizar uma AMI compartilhada (Tools for Windows PowerShell)

Use o comando Get-EC2Image (Tools for Windows PowerShell) para listar as AMIs. É possível direcionar o escopo da lista para os tipos de AMI que lhe interessam, conforme exibido nos exemplos a seguir.

Exemplo: Listar todas as AMIs públicas

O comando a seguir lista todas as AMIs públicas, inclusive todas as AMIs públicas de sua propriedade.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Exemplo: Listar AMIs permissões de execução explícita

O comando a seguir lista as AMIs para as quais você tenha permissões de execução explícita. Essa lista não inclui nenhuma AMI de sua propriedade.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Exemplo: Listar AMIs pertencentes a fornecedores verificados

O comando a seguir lista as AMIs de propriedade de provedores verificados. As AMIs públicas de propriedade de fornecedores verificados (da Amazon ou de parceiros verificados) têm um proprietário com alias, que é exibido como `amazon` ou `aws-marketplace` no campo da conta. Isso ajuda você a encontrar facilmente AMIs de fornecedores verificados. Outros usuários não podem dar um alias às AMIs deles.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Exemplo: Listar AMIs de propriedade de uma conta

O comando a seguir lista as AMIs de propriedade da Conta da AWS especificada.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Exemplo: Definir escopo das AMIs usando um filtro

Para reduzir o número de AMIs exibidas, use um filtro para listar somente os tipos de AMI que lhe interessam. Por exemplo, use o filtro a seguir para exibir somente AMIs com EBS.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Usar AMIs compartilhadas

Para que você use uma AMI compartilhada, execute as etapas a seguir para confirmar se não há credenciais pré-instaladas que permitam acesso indesejado à sua instância por terceiros e nenhum registro remoto pré-configurado que poderia transmitir dados confidenciais a terceiros. Verifique documentação da distribuição Linux usada pelas informações da AMI para obter informações sobre melhora da segurança do sistema.

Para garantir que você não perca acidentalmente acesso à sua instância, recomendamos que inicie duas sessões de SSH e mantenha a segunda sessão aberta até remover as credenciais que não reconhece e ter confirmado que ainda pode fazer login em sua instância usando SSH.

1. Identifique e desabilite todas as chaves SSH públicas não autorizadas. A única chave no arquivo deve ser aquela usada para executar as AMIs. O seguinte comando localiza os arquivos `authorized_keys`:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Desabilita a autenticação baseada em senha para o usuário raiz. Abra o arquivo `sshd_config` e edite a linha `PermitRootLogin` da seguinte forma:

   ```
   PermitRootLogin without-password
   ```

Como alternativa, é possível desativar a capacidade de fazer login na instância como usuário raiz:

```
PermitRootLogin No
```

Reinicie o serviço sshd.

3. Verifique se há outros usuários que possam fazer login na sua instância. Usuários com privilégios de superusuário são particularmente perigosos. Remova ou bloqueie senha de todas as contas desconhecidas.
4. Verifique se há portas abertas que você não está usando e escuta de serviços de rede em execução para as conexões de entrada.
5. Para evitar o registro em log remoto pré-configurado, exclua o arquivo de configuração existente e reinicie o serviço `rsyslog`. Por exemplo:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Verifique se todos os trabalhos cron são legítimos.

Se você descobrir uma AMI pública que sente que apresenta um risco de segurança, entre em contato com a equipe de segurança da AWS. Para obter informações, consulte o Centro de segurança da AWS.

Tornar um AMI pública

Você pode tornar sua AMI disponível publicamente compartilhando-a com todos os Contas da AWS.

Se você quiser impedir o compartilhamento público de suas AMIs, você pode habilitar o bloqueio de acesso público para AMIs. Isso bloqueia qualquer tentativa de tornar uma AMI pública, ajudando a evitar acesso não autorizado e possível uso indevido dos dados da AMI. Observe que habilitar o bloqueio de acesso público não afeta as AMIs que já estão publicamente disponíveis; elas permanecem publicamente acessíveis.

Para permitir que apenas contas específicas usem sua AMI para iniciar instâncias, consulte Compartilhar uma AMI com contas específicas da AWS.

Conteúdo

- Considerações
- Compartilhe uma AMI com todas as AWS contas (compartilhe publicamente)
- Bloqueie o acesso público às suas AMIs

Considerações

Considere as informações a seguir antes de tornar uma AMI pública.

- Propriedade: para tornar uma AMI pública, sua Conta da AWS deve ser proprietária da AMI.
- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível na região de onde foi compartilhada. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para ter mais informações, consulte Copiar um AMI.
- Bloquear o acesso público — Para compartilhar publicamente uma AMI, o bloqueio do acesso público para AMIs deve ser desativado em cada região na qual a AMI será compartilhada publicamente. Depois de compartilhar publicamente a AMI, você pode reativar o bloqueio do acesso público para AMIs para evitar mais compartilhamentos públicos de suas AMIs.
- Algumas AMIs não podem ser tornadas públicas: se sua AMI tiver um dos seguintes componentes, você não poderá torná-la pública (mas poderá compartilhar a AMI com Contas da AWS específicas):
  - Volumes criptografados
  - Snapshots de volumes criptografados
  - Códigos do produto
- Evite a exposição de dados confidenciais: para evitar expor dados confidenciais ao compartilhar uma AMI, leia as considerações de segurança em Diretrizes para AMIs em Linux compartilhadas e siga as ações recomendadas.
- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando sua AMI, poderão criar uma AMI com base na instância que iniciaram.
- Descontinuação automática: por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos após a data de criação da AMI. É possível definir a data de descontinuação para antes de dois anos. Para cancelar a data de descontinuação ou adiá-la para uma data posterior, você deve tornar a AMI privada compartilhando-a somente com Contas da AWS específicas.

- Remoção de AMIs obsoletas: depois que uma AMI pública atinge a data de descontinuação, se novas instâncias não forem iniciadas usando a AMI por seis meses ou mais, a AWS eventualmente remove a propriedade de compartilhamento público para que as AMIs obsoletas não apareçam nas listas de AMI públicas.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Compartilhe uma AMI com todas as AWS contas (compartilhe publicamente)

Depois de tornar uma AMI pública, ela fica disponível nas AMIs da comunidade no console, que você pode acessar no catálogo da AMI no navegador esquerdo do console do EC2 ou ao iniciar uma instância usando o console. Observe que pode demorar um pouco para a AMI aparecer em AMIs da comunidade depois de você torná-la pública.

Console

Para tornar um AMI pública

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI na lista e escolha Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em AMI availability (Disponibilidade da AMI), escolha Public (Pública).
5. Escolha Salvar alterações.

AWS CLI

Cada AMI tem uma propriedade `launchPermission` que controla quais Contas da AWS, além do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, é possível torná-la pública (o que concede permissões de execução a todas as Contas da AWS) ou compartilhá-la somente com as Contas da AWS que você especificar.

É possível adicionar ou remover os IDs da lista de contas que tiverem permissões de execução para uma AMI. Para tornar a AMI pública, especifique o grupo `all`. É possível especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

1. Use o comando modify-image-attribute da seguinte forma para adicionar o grupo `all` à lista `launchPermission` para a AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Para verificar as permissões de execução da AMI, use o comando describe-image-attribute.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Opcional) Para tornar a AMI privada novamente, remova o grupo `all` de suas permissões de execução. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Cada AMI tem uma propriedade `launchPermission` que controla quais Contas da AWS, além do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, é possível torná-la pública (o que concede permissões de execução a todas as Contas da AWS) ou compartilhá-la somente com as Contas da AWS que você especificar.

É possível adicionar ou remover os IDs da lista de contas que tiverem permissões de execução para uma AMI. Para tornar a AMI pública, especifique o grupo `all`. É possível especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

1. Use o comando Edit-EC2ImageAttribute da seguinte forma para adicionar o grupo `all` à lista `launchPermission` para a AMI especificada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserGroup all
```

2. Para verificar as permissões de execução da AMI, use o seguinte comando Get-EC2ImageAttribute.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

3. (Opcional) Para tornar a AMI privada novamente, remova o grupo `all` de suas permissões de execução. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserGroup all
```

Bloqueie o acesso público às suas AMIs

Para impedir o compartilhamento público de suas AMIs, você pode habilitar o bloqueio de acesso público para AMIs. Essa configuração é ativada no nível da conta, mas você precisa habilitá-la Região da AWS em cada uma das quais quiser impedir o compartilhamento público de suas AMIs.

Quando o bloqueio de acesso público está habilitado, qualquer tentativa de tornar uma AMI pública é automaticamente bloqueada. Entretanto, se você já tiver AMIs públicas, elas permanecerão disponíveis publicamente.

Para compartilhar AMIs publicamente, é necessário desabilitar o bloqueio de acesso público. Quando você terminar de compartilhar, é uma prática recomendada reabilitar o bloqueio de acesso público para evitar qualquer compartilhamento público não intencional das suas AMIs.

Você pode restringir as permissões do IAM a um usuário administrador para que apenas essa pessoa possa habilitar ou desabilitar o bloqueio de acesso público para AMIs.

Conteúdo

- Configurações padrão
- Permissões obrigatórias do IAM
- Habilite o bloqueio de acesso público para AMIs

- Desabilite o bloqueio de acesso público para AMIs
- Veja o estado do bloqueio de acesso público para AMIs

Configurações padrão

A configuração Bloquear acesso público para AMIs está habilitada ou desabilitada por padrão, dependendo se sua conta for nova ou existente e se você tem AMIs públicas. A tabela abaixo mostra as configurações padrão:

AWS account	Configuração padrão de bloquear acesso público para AMIs
Novas contas	Habilitado
Contas existentes sem AMIs públicas[1]	Habilitado
Contas existentes com um ou mais AMIs públicas	Desabilitado

[1] Se sua conta tinha uma ou mais AMIs públicas em ou após 15 de julho de 2023, a opção Bloquear acesso público para AMIs estará desabilitada por padrão, mesmo que você tenha posteriormente tornado todas as AMIs privadas.

Permissões obrigatórias do IAM

Para usar o bloqueio de acesso público para AMIs, você deve ter as seguintes permissões do IAM:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`
- `GetImageBlockPublicAccessState`

Habilite o bloqueio de acesso público para AMIs

Para evitar o compartilhamento público de suas AMIs, habilite o bloqueio de acesso público para AMIs no nível da conta. Você deve habilitar o bloqueio de acesso público para AMIs em cada Região

da AWS na qual deseja evitar o compartilhamento público das suas AMIs. Se você já tiver AMIs públicas, elas permanecerão disponíveis publicamente.

Console

Para habilitar o bloqueio de acesso público para AMIs na região especificada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação (na parte superior da tela), selecione a região na qual deseja executar o bloqueio de acesso público para as AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), escolha Manage (Gerenciar).
6. Selecione a caixa de seleção Block new public sharing (Bloquear novos compartilhamentos públicos) e, em seguida, escolha Update (Atualizar).

> **Note**
>
> A API pode levar até 10 minutos para definir essa configuração. Durante esse período, o valor será New public sharing allowed (Novo compartilhamento público permitido). Quando a API concluir a configuração, o valor mudará automaticamente para New public sharing blocked (Novo compartilhamento público bloqueado).

AWS CLI

Para habilitar o bloqueio de acesso público para AMIs na região especificada

Use o comando enable-image-block-public-access e especifique a região na qual habilitar o bloqueio de acesso público para AMIs. Para o parâmetro `--image-block-public-access-state`, especifique `block-new-sharing`:

```
aws ec2 enable-image-block-public-access \
    --region us-east-1 \
    --image-block-public-access-state block-new-sharing
```

Saída esperada

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

> **Note**
>
> A API pode levar até 10 minutos para definir essa configuração. Durante esse período, se você executar o comando get-image-block-public-access-state, a resposta será `unblocked`. Quando a API concluir a configuração, a resposta será `block-new-sharing`.

Desabilite o bloqueio de acesso público para AMIs

Para permitir que os usuários da sua conta compartilhem publicamente suas AMIs, desative o bloqueio do acesso público no nível da conta. Você deve desabilitar o bloqueio de acesso público para AMIs em cada Região da AWS na qual deseja permitir o compartilhamento público das suas AMIs.

Console

Para desabilitar o bloqueio de acesso público para AMIs na região especificada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação (na parte superior da tela), selecione a região na qual deseja desabilitar o bloqueio de acesso público para AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), escolha Manage (Gerenciar).
6. Limpe a caixa de seleção Block new public sharing (Bloquear novos compartilhamentos públicos) e, em seguida, escolha Update (Atualizar).
7. Insira **`confirm`** quando solicitado para confirmação e, em seguida, escolha Allow public sharing (Permitir compartilhamento público).

> **Note**
>
> A API pode levar até 10 minutos para definir essa configuração. Durante esse período, o valor será New public sharing blocked (Novo compartilhamento público bloqueado). Quando a API concluir a configuração, o valor mudará automaticamente para New public sharing allowed (Novo compartilhamento público permitido).

AWS CLI

Para desabilitar o bloqueio de acesso público para AMIs na região especificada

Use o comando disable-image-block-public-access e especifique a região na qual deseja desabilitar o bloqueio de acesso público para AMIs.

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Saída esperada

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

> **Note**
>
> A API pode levar até 10 minutos para definir essa configuração. Durante esse período, se você executar o comando get-image-block-public-access-state, a resposta será `block-new-sharing`. Quando a API concluir a configuração, a resposta será `unblocked`.

Veja o estado do bloqueio de acesso público para AMIs

Para ver se o compartilhamento público de suas AMIs está bloqueado em sua conta, você pode ver o estado do bloqueio de acesso público para AMIs. Você deve visualizar o estado em cada um Região da AWS no qual deseja ver se o compartilhamento público de suas AMIs está bloqueado.

Console

Para visualizar o estado do bloqueio de acesso público para AMIs na região especificada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação (na parte superior da tela), selecione a região na qual deseja visualizar o estado de bloqueio de acesso público para AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), marque o campo Public access (Acesso público). O valor é New public sharing blocked (Novo compartilhamento público bloqueado) ou New public sharing allowed (Novo compartilhamento público permitido).

AWS CLI

Para obter o estado do bloqueio de acesso público para AMIs na região especificada

Use o comando enable-image-block-public-access e especifique a região na qual obter o bloqueio de acesso público para AMIs.

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Saída esperada — O valor é `block-new-sharing` ou `unblocked`.

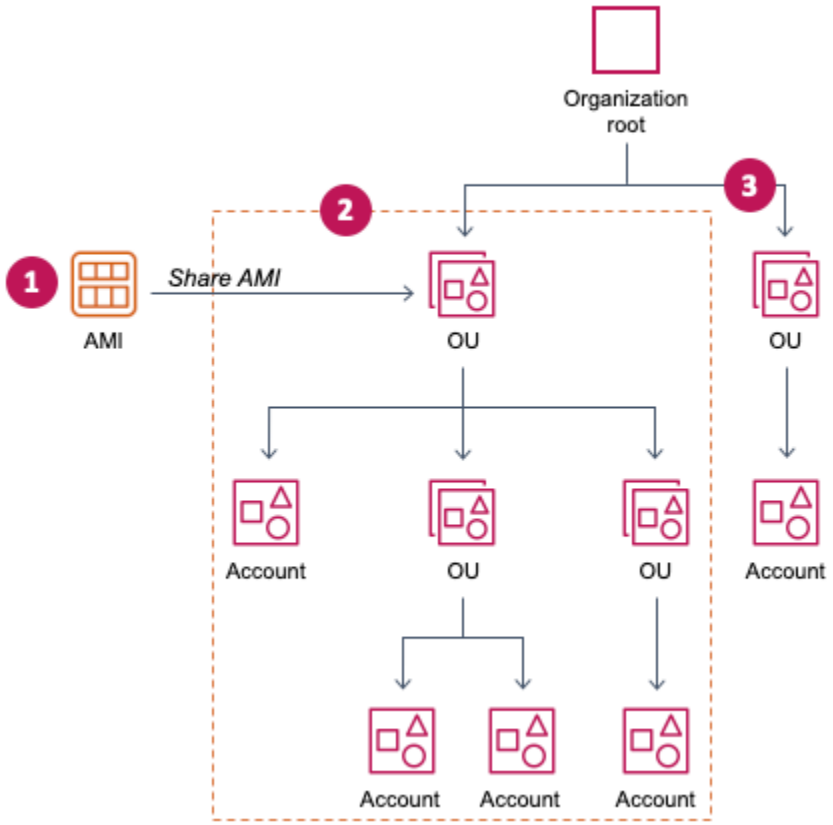
```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Compartilhe uma AMI com organizações ou unidades organizacionais específicas

O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma só organização, que você cria e gerencia centralmente. É possível compartilhar uma AMI com uma organização ou uma unidade organizacional (UO) que você criou, além de compartilhá-la com contas específicas.

Uma organização é uma entidade que você cria para consolidar e gerenciar suas Contas da AWS. É possível organizar as contas em uma estrutura em árvore hierárquica, com uma raiz no alto e unidades organizacionais aninhadas abaixo da raiz. Cada conta pode ser adicionada diretamente na raiz ou ser colocada em uma das UOs na hierarquia. Para obter mais informações, consulte Terminologia e conceitos das organizações da AWS no Guia do usuário do AWS Organizations.

Quando você compartilha uma AMI com uma organização ou uma UO, todas as contas subordinadas ganham acesso à AMI. Por exemplo, no diagrama a seguir, a AMI é compartilhada com uma UO de nível superior (indicada pela seta no número 1). Todas as UOs e contas aninhadas sob essa UO de nível superior (indicadas pela linha pontilhada no número 2) também têm acesso à AMI. As contas na organização e UO fora da linha pontilhada (indicadas pelo número 3) não têm acesso à AMI porque não são filhas da UO com a qual a AMI é compartilhada.



Considerações

Considere as informações a seguir ao compartilhar AMIs com organizações ou unidades organizacionais específicas.

- Propriedade: para compartilhar uma AMI, sua Conta da AWS deve ser proprietária da AMI.

- Limites de compartilhamento: o proprietário da AMI pode compartilhar uma AMI com qualquer organização ou UO, incluindo organizações e UOs às quais ele não pertence.

  Para saber o número máximo de entidades com as quais uma AMI pode ser compartilhada em uma região, consulte Service Quotas do Amazon EC2.

- Tags: você não pode compartilhar tags definidas pelo usuário (tags que você anexa a uma AMI). Quando você compartilha uma AMI, as tags definidas pelo usuário não estão disponíveis para nenhuma Conta da AWS em uma organização ou UO com a qual a AMI é compartilhada.

- Formato de ARN: ao especificar uma organização ou UO em um comando, verifique se usou o formato de ARN correto. Você receberá um erro se especificar apenas o ID, por exemplo, se você especificar apenas `o-123example` ou `ou-1234-5example`.

  Formatos corretos de ARN:

  - ARN de organização: `arn:aws:organizations::`*`account-id`*`:organization/`*`organization-id`*
  - ARN de UO: `arn:aws:organizations::`*`account-id`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Em que:

  - *`account-id`* é o número da conta de gerenciamento de 12 dígitos, por exemplo, `123456789012`. Se você não souber o número da conta de gerenciamento, poderá descrever a organização ou a unidade organizacional para obter o ARN, que inclui o número da conta de gerenciamento. Para ter mais informações, consulte Obter o ARN.
  - *`organization-id`* é o ID da organização, por exemplo, `o-123example`.
  - *`ou-id`* é o ID da unidade organizacional, por exemplo, `ou-1234-5example`.

  Para obter mais informações sobre o formato dos ARNs, consulte Nome do recurso da Amazon (ARN) no Guia do usuário do IAM.

- Criptografia e chaves: é possível compartilhar AMIs que tenham snapshots criptografados e não criptografados.
  - Os snapshots criptografados devem ser criptografados com uma chave gerenciada pelo cliente. Não é possível compartilhar AMIs que tenham snapshots que sejam criptografados com a chave gerenciada pela AWS padrão.
  - Se você compartilhar uma AMI que tenha snapshots criptografados, deverá permitir que as organizações ou UOs usem as chaves gerenciadas pelo cliente que foram usadas para criptografar os snapshots. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.

- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível na região de onde foi compartilhada. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para ter mais informações, consulte Copiar um AMI.
- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando sua AMI, poderão criar uma AMI com base na instância que iniciaram.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Permitir que organizações e UOs usem uma chave do KMS

Se você compartilhar uma AMI que tenha snapshots criptografados, também deverá permitir que as organizações ou UOs usem as AWS KMS keys que foram usadas para criptografar os snapshots.

Use as chaves `aws:PrincipalOrgID` e `aws:PrincipalOrgPaths` para comparar o caminho do AWS Organizations para a entidade principal que está fazendo a solicitação com o caminho na política. Essa entidade principal pode ser um usuário do IAM, um perfil do IAM, um usuário federado ou um usuário raiz da Conta da AWS. Em uma política, essa chave de condição garante que o solicitante seja um membro da conta na raiz da organização ou das UOs especificadas em AWS Organizations. Para obter mais exemplos de instruções de condição, consulte aws:PrincipalOrgID e aws:PrincipalOrgPaths no Guia do usuário do IAM.

Para obter mais informações sobre uma política de chaves, consulte Permitir que usuários de outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service.

Para conceder a uma organização ou UO permissão para usar uma chave do KMS, adicione a seguinte instrução à política de chaves.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
```

```
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Para compartilhar uma chave do KMS com várias UOs, é possível usar uma política semelhante ao exemplo a seguir.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Compartilhar uma AMI

É possível usar o console do Amazon EC2 ou a AWS CLI para compartilhar uma AMI com uma organização ou UO.

Compartilhar uma AMI (console)

Para compartilhar uma AMI com uma organização ou uma UO usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista e escolha Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em AMI availability (Disponibilidade da AMI), escolha Private (Privado).
5. Próximo a Shared organizations/OUs (Organizações/UOs compartilhadas), escolha Add organization/OU ARN (Adicionar ARN de organização/UO).
6. Em Organization/OU ARN (ARN de organização/UO), insira o ARN da organização ou o ARN da UO com o qual você deseja compartilhar a AMI e, em seguida, escolha Share AMI (Compartilhar AMI). Observe que especifique o ARN completo, e não apenas o ID.

   Para compartilhar essa AMI com várias organizações ou UOs, repita essa etapa até adicionar todas as organizações ou UOs necessárias.

   > **Note**
   >
   > Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Apenas a própria AMI precisa ser compartilhada, e o sistema fornece automaticamente acesso à instância aos snapshots do Amazon EBS referenciados para o início. No entanto, é necessário compartilhar todas as chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.

7. Após terminar, escolha Save changes (Salvar alterações).
8. (Opcional) Para visualizar as organizações ou UOs com as quais você compartilhou a AMI, selecione a AMI na lista, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs Organizações/UOs compartilhadas. Para localizar as AMIs que são compartilhadas com você, consulte Encontrar AMIs compartilhadas.

Compartilhar uma AMI (Tools for Windows PowerShell)

Use o comando Edit-EC2ImageAttribute (Tools for Windows PowerShell) para compartilhar uma AMI conforme exibido nos exemplos a seguir.

Para compartilhar uma AMI com uma organização ou uma UO

O comando a seguir concede permissões de execução para a AMI especificada à organização especificada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType add -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

> **Note**
>
> Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Apenas a própria AMI precisa ser compartilhada, e o sistema fornece automaticamente acesso à instância aos snapshots do Amazon EBS referenciados para o início. No entanto, é necessário compartilhar todas as chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.

Para interromper o compartilhamento de uma AMI com uma organização ou uma UO

O comando a seguir remove as permissões de execução para a AMI especificada da organização especificada:

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType remove -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

Para interromper o compartilhamento de uma AMI com todas as organizações, UOs e Contas da AWS

O comando a seguir remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Compartilhar uma AMI (AWS CLI)

Use o comando modify-image-attribute (AWS CLI) para compartilhar uma AMI.

Compartilhar uma AMI com uma organização usando a AWS CLI

O comando modify-image-attribute concede permissões de execução para a AMI especificada para a organização especificada. Observe que especifique o ARN completo, e não apenas o ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para compartilhar uma AMI com uma UO usando a AWS CLI

O comando modify-image-attribute concede permissões de execução para a AMI especificada à UO especificada. Observe que especifique o ARN completo, e não apenas o ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

> **Note**
>
> Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Apenas a própria AMI precisa ser compartilhada, e o sistema fornece automaticamente acesso à instância aos snapshots do Amazon EBS referenciados para o início. No entanto, é necessário compartilhar todas as chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.

Parar de compartilhar uma AMI

É possível usar o console do Amazon EC2 ou a AWS CLI para parar de compartilhar uma AMI com uma organização ou UO.

Interrupção de compartilhamento de uma AMI (console)

Para parar de compartilhar uma AMI com uma organização ou uma UO usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista e escolha Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em Shared organizations/OUs (Organizações/UOs compartilhadas), selecione as organizações ou UOs com as quais você deseja parar de compartilhar a AMI e, em seguida, escolha Remove selected (Remover selecionado).
5. Após terminar, escolha Save changes (Salvar alterações).
6. (Opcional) Para confirmar que você parou de compartilhar a AMI com as organizações ou UOs, selecione a AMI na lista, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs (Organizações/UOs compartilhadas).

Parar de compartilhar uma AMI (AWS CLI)

Use os comandos modify-image-attribute ou reset-image-attribute (AWS CLI) para interromper o compartilhamento de uma AMI.

Para interromper o compartilhamento uma AMI com uma organização ou uma UO usando a AWS CLI

O comando modify-image-attribute remove as permissões de execução para a AMI especificada da organização especificada. Observe que especifique o ARN.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para interromper o compartilhamento de uma AMI com todas as organizações, UOs e Contas da AWS usando a AWS CLI

O comando reset-image-attribute remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

> **Note**
>
> Você não pode interromper o compartilhamento de uma AMI com uma conta específica se ela estiver em uma organização ou UO com a qual uma AMI é compartilhada. Se você tentar parar de compartilhar a AMI removendo as permissões de execução da conta, o Amazon EC2 retornará uma mensagem de êxito. Porém, a AMI continua sendo compartilhada com a conta.

Veja as organizações e as UOs com as quais uma AMI é compartilhada

É possível usar o console do Amazon EC2 ou a AWS CLI para verificar com quais organizações e UOs você compartilhou sua AMI.

Veja as organizações e as UOs com as quais uma AMI é compartilhada (console)

Para verificar com quais organizações e UOs você compartilhou sua AMI usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs (Organizações/UOs compartilhadas).

   Para localizar as AMIs que são compartilhadas com você, consulte Encontrar AMIs compartilhadas.

Exibir as organizações e as UOs com as quais uma AMI é compartilhada (AWS CLI)

Usando o comando describe-image-attribute (AWS CLI) e o atributo `launchPermission`, é possível verificar com quais organizações e UOs você compartilhou sua AMI.

Para verificar com quais organizações e UOs você compartilhou sua AMI usando a AWS CLI

O comando describe-image-attribute descreve o atributo `launchPermission` para a AMI especificada e retorna as organizações e as UOs com as quais você compartilhou a AMI.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Exemplo de resposta

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

Obter o ARN

Os ARNs de organizações e de unidades organizacionais contêm o número da conta de gerenciamento de 12 dígitos. Se você não souber o número da conta de gerenciamento, poderá descrever a organização e a unidade organizacional para obter o ARN para cada uma delas. Nos exemplos a seguir, `123456789012` é o número da conta de gerenciamento.

Antes de obter os ARNs, é necessário ter permissão para descrever organizações e unidades organizacionais. O modelo de política a seguir fornece as permissões necessárias.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter o ARN de uma organização

Use o comando describe-organization e o parâmetro `--query` definido como `'Organization.Arn'` para retornar apenas o ARN da organização.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Exemplo de resposta

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

Para obter o ARN de uma unidade organizacional

Use o comando describe-organizational-unit, especifique o ID da UO e defina o parâmetro `--query` como `'OrganizationalUnit.Arn'` para retornar apenas o ARN da unidade organizacional.

```
aws organizations describe-organizational-unit --organizational-unit-
id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Exemplo de resposta

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Compartilhar uma AMI com contas específicas da AWS

É possível compartilhar uma AMI com Contas da AWS específicas sem torná-la pública. Basta ter os IDs de Conta da AWS.

Um ID de Conta da AWS é um número de 12 dígitos, como `012345678901`, que identifica de forma exclusiva uma Conta da AWS. Para obter mais informações, consulte Visualizar identificadores de Conta da AWS no Guia de referência da AWS Account Management.

Considerações

Considere as informações a seguir ao compartilhar AMIs com Contas da AWS específicas.

- Propriedade: para compartilhar uma AMI, sua Conta da AWS deve ser proprietária da AMI.
- Limites de compartilhamento: para saber o número máximo de entidades com as quais uma AMI pode ser compartilhada em uma região, consulte Service Quotas do Amazon EC2.
- Tags: você não pode compartilhar tags definidas pelo usuário (tags que você anexa a uma AMI). Quando você compartilha uma AMI, suas tags definidas pelo usuário não estão disponíveis para nenhuma Conta da AWS com a qual a AMI é compartilhada.
- Criptografia e chaves: é possível compartilhar AMIs que tenham snapshots criptografados e não criptografados.
  - Os snapshots criptografados devem ser criptografados com uma chave do KMS. Não é possível compartilhar AMIs que tenham snapshots que sejam criptografados com a chave gerenciada pela AWS padrão.
  - Se você compartilhar uma AMI que tenha snapshots criptografados, permita que as Contas da AWS usem as chaves do KMS que foram usadas para criptografar os snapshots. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS. Para configurar a política de chave de que você precisa para executar instâncias do Auto Scaling ao usar uma chave gerenciada pelo cliente para criptografia, consulte Política necessária de AWS KMS key para uso com volumes criptografados no Guia do usuário do Amazon EC2 Auto Scaling.
- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível naquela região. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para ter mais informações, consulte Copiar um AMI.
- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando a sua AMI, eles podem criar uma AMI a partir da instância deles.
- Cópias de AMIs compartilhadas: se os usuários em outra conta quiserem copiar uma AMI compartilhada, você deverá conceder a eles permissões de leitura para o armazenamento que oferece suporte à AMI. Para ter mais informações, consulte Cópia entre contas.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Compartilhar uma AMI (console)

Para conceder permissões de execução explícita usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista e escolha Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Selecione Private (Privado).
5. Em Shared accounts (Contas compartilhadas), escolha Add account ID (Adicionar ID de conta).
6. Em Conta da AWS ID (ID da), insira o ID da Conta da AWS com a qual você deseja compartilhar a AMI e, em seguida, escolha Share AMI (Compartilhar AMI).

   Para compartilhar essa AMI com várias contas, repita as Etapas 5 e 6 até adicionar todos os ID de conta necessários.

   > **Note**
   >
   > Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS.

7. Escolha Save changes (Salvar alterações) quando terminar.
8. (Opcional) Para visualizar os IDs de Conta da AWS com a qual você compartilhou a AMI, selecione a AMI na lista e escolha a guia Permissions (Permissões). Para localizar as AMIs que são compartilhadas com você, consulte Encontrar AMIs compartilhadas.

Compartilhar uma AMI (Tools for Windows PowerShell)

Use o comando Edit-EC2ImageAttribute (Tools for Windows PowerShell) para compartilhar uma AMI conforme exibido nos exemplos a seguir.

Para conceder permissões de execução explícitas

O comando a seguir concede permissões de execução da AMI especificada para a Conta da AWS especificada. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida e substitua *account-id* pela ID da Conta da AWS com 12 dígitos.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserId "account-id"
```

> **Note**
>
> Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS.

Para remover as permissões de execução de uma conta

O comando a seguir remove permissões de execução para a AMI especificada da Conta da AWS especificada. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida e substitua *account-id* pela ID da Conta da AWS com 12 dígitos.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserId "account-id"
```

Para remover todas as permissões de execução

O comando a seguir remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Compartilhar uma AMI (AWS CLI)

Use o comando modify-image-attribute (AWS CLI) para compartilhar uma AMI conforme exibido nos exemplos a seguir.

Para conceder permissões de execução explícitas

O comando a seguir concede permissões de execução da AMI especificada para a Conta da AWS especificada. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida e substitua *account-id* pela ID da Conta da AWS com 12 dígitos.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=account-id}]"
```

> **Note**
>
> Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS.

Para remover as permissões de execução de uma conta

O comando a seguir remove permissões de execução para a AMI especificada da Conta da AWS especificada. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida e substitua *account-id* pela ID da Conta da AWS com 12 dígitos.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=account-id}]"
```

Para remover todas as permissões de execução

O comando a seguir remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto,

não é afetado por este comando. No exemplo a seguir, substitua a ID da AMI de exemplo por uma ID de AMI válida.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Cancelar o compartilhamento de uma AMI com sua Conta da AWS

Uma imagem de máquina da Amazon (AMI) pode ser compartilhada com Contas da AWS específicas adicionando as contas às permissões de execução da AMI. Se uma AMI tiver sido compartilhada com sua Conta da AWS e você não quiser mais compartilhá-la com sua conta, poderá remover sua conta das permissões de execução da AMI. Você pode fazer isso executando o comando `cancel-image-launch-permission` da AWS CLI. Ao executar esse comando, sua Conta da AWS é removida das permissões de execução para a AMI especificada.

Você pode cancelar o compartilhamento de uma AMI com sua conta, p. ex., para reduzir a probabilidade de executar uma instância com uma AMI não utilizada ou obsoleta que tenha sido compartilhada com você. Quando você cancela o compartilhamento de uma AMI com sua conta, ela não aparece mais em nenhuma lista de AMI no console do EC2 ou na saída do comando describe-images.

Tópicos

- Limitações
- Cancelar o compartilhamento de uma AMI com sua conta
- Localizar AMIs que são compartilhadas com sua conta

Limitações

- Você pode remover sua conta das permissões de inicialização de uma AMI que seja compartilhada apenas com sua Conta da AWS. Você não pode usar `cancel-image-launch-permission` para remover sua conta das permissões de inicialização de uma AMI compartilhada com uma organização ou unidade organizacional (UO) ou para remover o acesso a AMIs públicas.
- Você não pode remover permanentemente sua conta das permissões de execução de uma AMI. O proprietário de uma AMI pode compartilhar uma AMI com sua conta novamente.

- As AMIs são um recurso regional. Ao executar `cancel-image-launch-permission`, você deve especificar a região na qual a AMI está localizada. Especifique uma região no comando ou use a variável de ambiente AWS_DEFAULT_REGION.
- Somente a AWS CLI e os SDKs são compatíveis com a remoção de sua conta das permissões de execução de uma AMI. No momento, o console do EC2 não é compatível com essa ação.

Cancelar o compartilhamento de uma AMI com sua conta

> **Note**
>
> Após cancelar o compartilhamento de uma AMI com sua conta, você não poderá desfazer essa ação. Para recuperar o acesso à AMI, o proprietário da AMI deverá compartilhá-la com sua conta.

AWS CLI

Para cancelar o compartilhamento de uma AMI com sua Conta da AWS

Use o comando cancel-image-launch-permission e especifique o ID da AMI.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Saída esperada

```
{
    "Return": true
}
```

PowerShell

Para cancelar o compartilhamento de uma AMI com sua Conta da AWS usando o AWS Tools for PowerShell

Use o comando Stop-EC2ImageLaunchPermission e especifique o ID da AMI.

```
Stop-EC2ImageLaunchPermission `
```

```
    -ImageId ami-0123456789example `
    -Region us-east-1
```

Saída esperada

```
True
```

Localizar AMIs que são compartilhadas com sua conta

Para localizar as AMIs que são compartilhadas com sua Conta da AWS, consulte Encontrar AMIs compartilhadas.

Usar marcadores

Se você tiver criado uma AMI pública ou compartilhado uma AMI com outra Conta da AWS, você poderá criar um favorito que permita a um usuário acessar sua AMI e executar imediatamente uma instância na conta dele. Essa é uma maneira fácil de compartilhar referências de AMI, de forma que os usuários não tenham de gastar tempo para encontrar sua AMI para utilizá-la.

Observe que sua AMI deve ser pública; caso contrário, é necessário tê-la compartilhado com o usuário a quem deseja enviar o favorito.

Para criar um favorito para sua AMI

1. Digite um URL com as informações a seguir, onde região é a região na qual sua AMI reside:

   ```
   https://console.aws.amazon.com/ec2/v2/home?
   region=region#LaunchInstanceWizard:ami=ami_id
   ```

   Por exemplo, esse URL executa uma instância com base na AMI ami-0abcdef1234567890 na região `us-east-1` (Leste dos EUA [N. da Virgínia]):

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=us-
   east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
   ```

2. Distribua o link para os usuários que desejam usar sua AMI.
3. Para usar um favorito, escolha o link ou copie-o e cole-o no navegador. O assistente de execução se abre com as AMIs já selecionadas.

Diretrizes para AMIs em Linux compartilhadas

Use as diretrizes a seguir para reduzir a superfície de ataque e melhorar a confiabilidade das AMIs criadas.

> **Important**
>
> Nenhuma lista de diretrizes de segurança consegue ser exaustiva. Crie suas AMIs compartilhadas cuidadosamente e tire um tempo para considerar onde é possível expor dados confidenciais.

Tópicos

- Atualização das ferramentas de AMI antes do uso
- Desabilitar logins remotos com senha para o usuário raiz
- Desabilitar o acesso à raiz local
- Remover pares de chave do host SSH
- Instalação de credenciais de chave pública
- Desabilitação de verificações de DNS para SSHD (opcional)
- Proteja-se

Se você estiver criando AMIs para o AWS Marketplace, consulte Práticas recomendadas para a criação de AMIs no Guia do vendedor do AWS Marketplace para obter diretrizes, políticas e práticas recomendadas.

Para obter informações adicionais sobre compartilhamento de AMIs com segurança, consulte os seguintes artigos:

- Como compartilhar e usar AMIs públicas de forma segura
- Public AMI Publishing: Hardening and Clean-up Requirements

Atualização das ferramentas de AMI antes do uso

Para AMIs com armazenamento de instâncias, recomendamos que suas AMIs façam download e atualizem as ferramentas de criação de AMI do Amazon EC2 antes de usá-las. Isso garante que as novas AMIs baseadas nas suas AMIs compartilhadas tenham as ferramentas de AMI mais recentes.

No Amazon Linux 2, instale o pacote `aws-amitools-ec2` e adicione as ferramentas de AMI no seu caminho com o comando a seguir. No Amazon Linux AMI, o pacote `aws-amitools-ec2` já vem instalado por padrão.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin
 > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Atualize as ferramentas de AMI com o comando a seguir:

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Para outras distribuições, tenha as ferramentas de AMI mais recentes.

Desabilitar logins remotos com senha para o usuário raiz

Usar uma senha de raiz fixa com uma AMI pública é um risco de segurança que pode rapidamente ficar conhecido. Até mesmo depender dos usuários para alterar a senha depois do primeiro login abre uma pequena janela de oportunidade para potencial abuso.

Para resolver esse problema, desabilite logins remotos com senha para o usuário raiz.

Para desabilitar logins remotos com senha para o usuário raiz

1. Abra o arquivo `/etc/ssh/sshd_config` com um editor de texto e localize a seguinte linha:

   ```
   #PermitRootLogin yes
   ```

2. Altere a linha para:

   ```
   PermitRootLogin without-password
   ```

   O local desse arquivo de configuração pode diferir para sua distribuição ou se você não estiver executando OpenSSH. Se esse for o caso, consulte a documentação apropriada.

Desabilitar o acesso à raiz local

Quando você trabalha com AMIs compartilhadas, a prática recomendada é desabilitar logins diretos na raiz. Para isso, faça login na sua instância em execução e emita o seguinte comando:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Esse comando não afeta o uso de `sudo`.

Remover pares de chave do host SSH

Se você pretende compartilhar uma AMI derivada de uma AMI pública, remova os pares de chaves do host SSH existentes localizadas em `/etc/ssh`. Isso força o SSH a gerar novos pares de chaves SSH exclusivos quando alguém executar uma instância usando sua AMI, melhorando a segurança e reduzindo a probabilidade de ataques "man-in-the-middle".

Elimine todos os arquivos de chave a seguir presentes no seu sistema.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

É possível remover com segurança todos esses arquivos com o comando a seguir.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Utilitários de exclusão segura, como **`shred`**, podem não remover todas as cópias de um arquivo da sua mídia de armazenamento. Podem ser criadas cópias ocultas de arquivos ao criar registros dos sistemas de arquivos (incluindo Amazon Linux padrão ext4), snapshots,

backups, RAID e cache temporário. Para obter mais informações, consulte a documentação do **shred**.

Important

Se você se esquecer de remover o par de chaves existente do host SSH da AMI pública, nosso processo de auditoria de rotina notificará você e todos os clientes que executam instâncias da sua AMI sobre o risco potencial à segurança. Após um breve período de carência, marcamos a AMI como privada.

Instalação de credenciais de chave pública

Depois de configurar a AMI para impedir o login usando uma senha, é necessário garantir que os usuários possam fazer login usando outro mecanismo.

O Amazon EC2 permite que os usuários especifiquem um nome de par de chaves público-privado ao executarem uma instância. Quando um nome válido de par de chaves for fornecido para a chamada de API `RunInstances` (ou pelas ferramentas de API da linha de comando), a chave pública (a parte do par de chaves que o Amazon EC2 retém no servidor depois de uma chamada para `CreateKeyPair` ou `ImportKeyPair`) será disponibilizada para a instância por meio de uma consulta HTTP contra os metadados de instância.

Para fazer login com SSH, sua AMI deve recuperar o valor da chave na inicialização e anexá-la a `/root/.ssh/authorized_keys` (ou o equivalente para qualquer outra conta de usuário na AMI). Os usuários podem executar instâncias da sua AMI com um par de chaves e fazer login sem exigir uma senha raiz.

Muitas distribuições, inclusive Amazon Linux e Ubuntu, usam o pacote `cloud-init` para injetar credenciais de chave pública a um usuário configurado. Se sua distribuição não oferecer suporte a `cloud-init`, é possível adicionar o código a seguir a um script de inicialização do sistema (como `/etc/rc.local`) para puxar a chave pública especificada na execução para o usuário raiz.

Note

No exemplo a seguir, o endereço IP do http://169.254.169.254/ é um endereço local de link e é válido apenas a partir da instância.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Isso pode se aplicar a qualquer usuário; não precisa ficar restrito ao `root`.

> **Note**
>
> Reempacotar uma instância baseada nessa AMI inclui a chave com a qual ela foi executada. Para evitar a inclusão de chaves, é necessário desmarcar (ou excluir) o arquivo `authorized_keys` ou excluir esse arquivo do reempacotamento.

Desabilitação de verificações de DNS para SSHD (opcional)

Desabilitar as verificações de DNS sshd enfraquece levemente a segurança de sshd. Contudo, se uma solução de DNS falhar, o login de SSH continuará funcionando. Se você não desabilitar verificações de sshd, falhas de resolução de DNS impedirão todos os logins.

Para desabilitar as verificações de DNS sshd

1. Abra o arquivo `/etc/ssh/sshd_config` com um editor de texto e localize a seguinte linha:

```
#UseDNS yes
```

2. Altere a linha para:

```
UseDNS no
```

> **Note**
>
> O local desse arquivo de configuração pode diferir para sua distribuição ou se você não estiver executando OpenSSH. Se esse for o caso, consulte a documentação apropriada.

Proteja-se

Não recomendamos armazenar dados confidenciais ou software em nenhuma AMI compartilhada. Os usuários que executarem uma AMI compartilhada podem ser capazes de reempacotá-la e registrá-la como própria. Siga estas diretrizes para ajudá-lo a evitar alguns riscos de segurança facilmente negligenciados:

- Recomendamos usar a opção `--exclude` *`directory`* em `ec2-bundle-vol` para ignorar todos os diretórios e subdiretórios que contêm informações secretas que você não gostaria de incluir no seu pacote. Mais especificamente, exclua todos os arquivos `authorized_keys` de pares de chaves públicas/privadas e SSH de propriedade do usuário ao empacotar a imagem. As AMIs públicas da Amazon os armazenam na `/root/.ssh` do usuário raiz e `/home/`*`user_name`*`/.ssh/` para os usuário regulares. Para ter mais informações, consulte ec2-bundle-vol.

- Sempre exclua o histórico do shell antes de empacotar. Se você tentar fazer mais de um upload de bundle na mesma AMI, o histórico do shell conterá sua chave de acesso. O exemplo a seguir deve ser o último comando executado antes de empacotar na instância.

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> As limitações de **`shred`** descritas no alerta acima aplicam-se aqui também.
> Esteja ciente de que, ao sair, o bash grava o histórico da sessão atual no disco. Se você fizer logout da sua instância após a exclusão de `~/.bash_history`, e depois fizer login de volta, descobrirá que `~/.bash_history` foi recriado e contém todos os comandos executados durante a sessão anterior.
> Outros programas além do bash também gravam históricos no disco. Use com cuidado e remova ou exclua arquivos-ponto ou diretórios-ponto desnecessários.

- O empacotamento de uma instância em execução requer sua chave privada e o certificado X.509. Coloque essas e outras credenciais em um local que não seja empacotado (como armazenamento de instâncias).

AMIs pagas

Uma AMI paga é uma AMI que está listada para venda no AWS Marketplace. O AWS Marketplace é uma loja online na qual é possível adquirir o software executado na AWS, incluindo as AMIs usadas na execução da instância do EC2. As AMIs do AWS Marketplace são organizadas em categorias, como Ferramentas para desenvolvedores, o que permite que você encontre produtos para atender às suas necessidades. Para obter mais informações sobre o AWS Marketplace, consulte o site do AWS Marketplace.

É possível comprar AMIs no AWS Marketplace de terceiros, incluindo AMIs equipadas com contratos de serviço de organizações como a Red Hat. Além disso, é possível criar uma AMI e vendê-la no AWS Marketplace para outros usuários do Amazon EC2. A criação de uma AMI segura, protegida e utilizável para consumo público é um processo bastante direto, quando você segue algumas diretrizes simples. Para obter informações sobre como criar e usar AMIs compartilhadas, consulte AMIs compartilhadas.

Executar uma instância de uma AMI paga é o mesmo que executar uma instância de qualquer outra AMI. Nenhum parâmetro adicional é necessário. A instância é cobrada de acordo com as taxas definidas pelo proprietário da AMI, bem como de acordo com as taxas de uso padrão dos serviços Web relacionados, por exemplo, a taxa por hora para a execução de um tipo de instância m5.small no Amazon EC2. Taxas adicionais também podem ser cobradas. O proprietário da AMI paga pode confirmar se uma determinada instância foi executada usando essa AMI paga.

> **Important**
>
> O Amazon DevPay não está mais aceitando novos vendedores ou produtos. O AWS Marketplace agora é a única plataforma unificada de comércio eletrônico para vender software e serviços por meio da AWS. Para obter informações sobre como implantar e vender software do AWS Marketplace, consulte Como vender no AWS Marketplace. O AWS Marketplace oferece suporte para AMIs com o Amazon EBS.

Tópicos

- Vender sua AMI
- Localizar uma AMI paga
- Comprar uma AMI paga
- Obter o código do produto para sua instância
- Usar suporte pago
- Faturas para AMI pagas e compatíveis
- Gerenciar suas assinaturas do AWS Marketplace

Vender sua AMI

É possível vender a AMI usando o AWS Marketplace. O AWS Marketplace oferece uma experiência de compras organizada. Além disso, o AWS Marketplace também oferece suporte a recursos da AWS, como AMIs baseadas no Amazon EBS, instâncias reservadas e instâncias spot.

Para obter informações sobre como vender a AMI no AWS Marketplace, consulte Como vender no AWS Marketplace.

Localizar uma AMI paga

Há algumas formas de encontrar AMIs que estão disponíveis para compra. Por exemplo, é possível usar o AWS Marketplace, o console do Amazon EC2 ou a linha de comando. De forma alternativa, um desenvolvedor pode, por conta própria, informar você sobre uma AMI paga.

Para localizar uma AMI paga usando o console

Para localizar uma AMI paga usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens públicas.
4. Na barra Search (Pesquisar), escolha Owner alias (Alias do proprietário), = e depois aws-marketplace.
5. Se você souber o código do produto, escolha Product Code (Código do produto), = e depois insira o código do produto.

Localizar uma AMI paga usando o AWS Marketplace

Para encontrar uma AMI paga usando o AWS Marketplace

1. Aberto AWS Marketplace.
2. Insira o nome do sistema operacional no campo de pesquisa e escolha o botão de pesquisa (lupa).
3. Para definir ainda mais o escopo dos resultados, use uma das categorias ou filtros.
4. Cada produto é identificado com o tipo: `AMI` ou `Software as a Service`.

Localizar uma AMI paga usando o AWS CLI

É possível encontrar uma AMI paga usando o seguinte comando describe-images (AWS CLI).

```
aws ec2 describe-images
    --owners aws-marketplace
```

Esse comando retorna detalhes numerosos que descrevem cada AMI, incluindo o código do produto para uma AMI paga. A saída de `describe-images` inclui uma entrada para o código do produto como o seguinte:

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

Se você souber o código do produto, poderá filtrar os resultados por código do produto. Esse exemplo retorna a AMI mais recente com o código do produto especificado.

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Localizar uma AMI paga usando o Tools for Windows PowerShell

É possível encontrar uma AMI paga usando o seguinte comando Get-EC2Image.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

A saída de uma AMI paga inclui o código do produto.

```
ProductCodeId           ProductCodeType
-------------           ---------------
product_code            marketplace
```

Se você souber o código do produto, poderá filtrar os resultados por código do produto. Esse exemplo retorna a AMI mais recente com o código do produto especificado.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First
 1).ImageId
```

Comprar uma AMI paga

É necessário cadastrar-se (para comprar) uma AMI paga para poder executar uma instância usando a AMI.

Normalmente, um vendedor de uma AMI paga apresenta informações sobre as AMIs, incluindo o preço e um link no qual é possível comprá-las. Quando você clicar no link, será solicitado que você faça login na AWS e, em seguida, será possível comprar a AMI.

Comprar uma AMI paga usando o console

É possível comprar uma AMI paga usando o assistente de execução do Amazon EC2. Para obter mais informações, consulte Executar uma instância AWS Marketplace.

Assinar um produto usando o AWS Marketplace

Para usar o AWS Marketplace, é necessário ter uma conta da AWS. Para executar instâncias de produtos do AWS Marketplace, é necessário estar cadastrado para usar o serviço Amazon EC2 e ter assinado o produto do qual iniciar a instância. Há duas maneiras de assinar produtos no AWS Marketplace:

- Site do AWS Marketplace: é possível executar o software pré-configurado rapidamente com o recurso de implantação de um clique.
- Assistente de execução do Amazon EC2: é possível procurar uma AMI e executar uma instância diretamente do assistente. Para obter mais informações, consulte Executar uma instância AWS Marketplace.

Obter o código do produto para sua instância

Recupere o código do produto do AWS Marketplace para sua instância usando os metadados da instância. Se a instância tiver um código de produto, o Amazon EC2 o retornará. Para obter mais informações sobre como recuperar os metadados, consulte Recuperar metadados da instância.

Para recuperar um código de produto, use o comando do sistema operacional da sua instância.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Usar suporte pago

O Amazon EC2 também permite que desenvolvedores ofereçam suporte para o software (ou AMI derivadas). Os desenvolvedores podem criar produtos de suporte nos quais é possível se cadastrar para usar. Durante o cadastro no produto de suporte, o desenvolvedor oferece a você um código de produto, que é necessário associar à sua própria AMI. Isso permite ao desenvolvedor confirmar que sua instância está qualificada para suporte. Também garante que quando você executar instâncias do produto, você será cobrado de acordo com os termos do produto especificado pelo desenvolvedor.

> **Important**
>
> Você não pode usar um produto de suporte com Instâncias reservadas. Você sempre paga o preço que está especificado pelo vendedor do produto de suporte.

Para associar um código de produto com sua AMI, use um dos seguintes comandos, em que ami_id é o ID da AMI e product_code é o código do produto:

- modify-image-attribute (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Depois de definir o atributo de código de produto, ele não pode ser alterado nem removido.

Faturas para AMI pagas e compatíveis

No final de cada mês, você recebe um e-mail com o valor que foi cobrado de seu cartão de crédito pelo uso de todas as AMIs pagas ou compatíveis durante o mês. Essa conta é separada de sua conta normal do Amazon EC2. Para obter mais informações, consulte Pagamento de produtos no Guia do comprador do AWS Marketplace.

Gerenciar suas assinaturas do AWS Marketplace

No site do AWS Marketplace, é possível verificar os detalhes de sua assinatura, visualizar as instruções de uso do fornecedor, gerenciar as assinaturas, etc.

Para verificar os detalhes de sua assinatura

1. Faça login no AWS Marketplace.
2. Escolha Your Marketplace Account.
3. Escolha Manage your software subscriptions.
4. Todas as assinaturas atuais estão listadas. Escolha Usage Instructions para visualizar instruções específicas sobre o uso do produto; por exemplo, um nome de usuário para se conectar à instância em execução.

Para cancelar a assinatura do AWS Marketplace

1. Certifique-se de que você tenha encerrado todas as instâncias em execução da assinatura.
   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. No painel de navegação, escolha Instances (Instâncias).
   c. Selecione a instância e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

d. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

2. Inicie a sessão no AWS Marketplace, escolha Your Marketplace Account (Sua conta do Marketplace) e, depois, Manage your software subscriptions (Gerenciar suas assinaturas de software).
3. Escolha Cancel subscription. Será solicitada a confirmação do cancelamento.

> **Note**
>
> Depois de cancelar sua assinatura, você não poderá mais executar nenhuma instância dessa AMI. Para usar essa AMI novamente, você precisará assiná-la novamente, no site do AWS Marketplace ou por meio do assistente de inicialização no console do Amazon EC2.

Ciclo de vida da AMI

É possível criar suas próprias AMIs, copiá-las, fazer backup e mantê-las até que esteja pronto para descontinuar ou cancelá-las.

Conteúdo

- Criar uma AMI
- Modificar uma AMI do
- Copiar um AMI
- Armazenar e restaurar uma AMI usando o S3
- Descontinuar uma AMI
- Desabilitar uma AMI
- Arquivar snapshots da AMI
- Cancelar o registro de uma AMI (excluir a AMI)
- Automatizar o ciclo de vida da AMI com suporte do EBS

Criar uma AMI

É possível criar AMIs do Linux ou do Windows baseadas em volumes do Amazon EBS. Você também pode criar AMIs do Linux baseadas em volumes de armazenamento de instância (as AMIs

do Windows não são compatíveis com o armazenamento de instância para o dispositivo raiz). Além disso, é possível usar a ferramenta Sysprep do Windows para criar AMIs do Windows.

Tópicos

- Criação de uma AMI baseada no Amazon EBS
- Criar uma AMI em Linux com armazenamento de instâncias
- Criação de uma AMI com a ferramenta Sysprep do Windows

Criação de uma AMI baseada no Amazon EBS

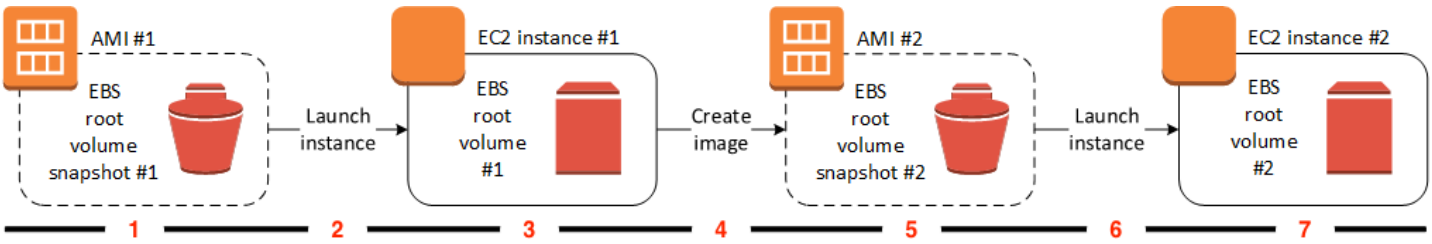
Para criar uma AMI baseada no Amazon EBS, comece com uma instância iniciada usando uma AMI baseada no Amazon EBS existente. Pode ser uma AMI que você obteve do AWS Marketplace, uma AMI que você criou usando o AWS Server Migration Service ou o VM Import/Export, ou qualquer outra AMI à qual você tenha acesso. Depois de personalizar a instância para atender a suas necessidades, crie e registre uma nova AMI, que poderá ser usada para executar novas instâncias com essas personalizações.

Os procedimentos descritos abaixo funcionam para instâncias do Amazon EC2 baseada em volumes do Amazon Elastic Block Store (Amazon EBS) criptografados (incluindo o volume raiz), bem como para volumes descriptografados.

O processo de criação da AMI é diferente para as AMIs com armazenamento de instâncias. Para obter informações sobre as diferenças entre instâncias com Amazon EBS e instâncias com armazenamento de instâncias, e como determinar o tipo de dispositivo raiz para sua instância, consulte Armazenamento para o dispositivo raiz. Para obter informações sobre como criar uma AMI baseada no armazenamento de instância, consulte Criar uma AMI em Linux com armazenamento de instâncias.

Visão geral da criação de AMIs baseadas no Amazon EBS

O diagrama a seguir resume o processo de criação de uma AMI baseada no Amazon EBS a partir de uma instância do EC2 em execução: comece com uma AMI existente, inicie uma instância, personalize-a, crie uma nova AMI a partir dela e, por fim, inicie uma instância de sua nova AMI. Os números no diagrama correspondem aos números na descrição a seguir.



1: AMI #1: comece com uma AMI existente

Encontre uma AMI existente semelhante à AMI que você deseja criar. Pode ser uma AMI que você obteve do AWS Marketplace, uma AMI que você criou usando o AWS Server Migration Service ou o VM Import/Export, ou qualquer outra AMI à qual você tenha acesso. Você personalizará essa AMI para suas necessidades.

No diagrama, EBS root volume snapshot #1 (Snapshot do volume raiz do EBS #1) indica que a AMI é uma AMI baseada no Amazon EBS e que as informações sobre o volume raiz são armazenadas neste snapshot.

2: iniciar instância a partir da AMI existente

A maneira de configurar uma AMI é iniciar uma instância a partir da AMI na qual você gostaria de basear sua nova AMI e, em seguida, personalizar a instância (indicado em 3 no diagrama). Em seguida, você vai criar uma nova AMI que inclua as personalizações (indicado em 4 no diagrama).

3: instância do EC2 #1: personalize a instância

Conecte-se à sua instância e personalize-a para suas necessidades. Sua nova AMI incluirá essas personalizações.

É possível executar qualquer uma destas ações em sua instância para personalizá-la:

- Instalar o software e aplicações
- Copiar dados
- Reduzir o tempo de inicialização excluindo arquivos temporários e desfragmentando o disco rígido
- Anexar volumes adicionais do EBS

4: Crie a imagem

Quando você cria uma AMI a partir de uma instância, o Amazon EC2 desativa a instância antes de criar a AMI para garantir que tudo na instância seja interrompido e esteja em um estado

consistente durante o processo de criação. Se você estiver seguro de que sua instância está em um estado consistente e apropriado para a criação da AMI, poderá informar ao Amazon EC2 para não desativar e reiniciar a instância. Alguns sistemas de arquivos, como o XFS, podem congelar e descongelar atividades, tornando seguro criar a imagem sem reinicializar a instância.

Durante o processo de criação da AMI, o Amazon EC2 cria snapshots do volume raiz de sua instância e de todos os outros volumes do EBS anexados à sua instância. Você é cobrado pelos snapshots até que você cancele o registro da AMI e exclua os snapshots. Se qualquer volume anexado à instância estiver criptografado, a nova AMI só será iniciada com êxito em instâncias com suporte para a criptografia do Amazon EBS.

Dependendo do tamanho dos volumes, pode levar vários minutos para que o processo de criação da AMI se complete (às vezes até 24 horas). É possível achar mais eficiente criar snapshots de seus volumes antes de criar sua AMI. Dessa forma, apenas snapshots pequenos e incrementais precisam ser criados quando a AMI é criada, e o processo é concluído mais rapidamente (o tempo total para a criação de snapshot permanece o mesmo.)

5: AMI #2: nova AMI

Após a conclusão do processo, você terá novos AMI e snapshot (snapshot #2) criados a partir do volume raiz da instância. Se você adicionou volumes de armazenamento de instâncias ou volumes do EBS à instância, além do volume raiz, o mapeamento de dispositivos de blocos para a nova AMI conterá informações sobre esses volumes.

O Amazon EC2 registra automaticamente a AMI para você.

6: inicie uma instância a partir da nova AMI

É possível usar a nova AMI para iniciar uma instância.

7: instância do EC2 #2: nova instância

Quando você inicia uma instância usando a nova AMI, o Amazon EC2 cria um novo volume do EBS para o volume raiz da instância usando o snapshot. Se você adicionou volumes de armazenamento de instâncias ou volumes do EBS quando personalizou a instância, o mapeamento de dispositivos de blocos para a nova AMI conterá informações sobre esses volumes, e os mapeamentos de dispositivos de blocos para as instâncias que você iniciar da nova AMI conterão automaticamente informações sobre esses volumes. Os volumes de armazenamento de instâncias especificados no mapeamento de dispositivos de bloco para a nova instância são novos e não contêm dados dos volumes de armazenamento de instâncias da instância usada para criar a AMI. Os dados nos volumes do EBS persistem. Para obter mais informações, consulte Mapeamentos de dispositivos de blocos.

Ao criar uma nova instância de uma AMI com suporte do EBS, é necessário inicializar o volume raiz todo o armazenamento adicional EBS antes de colocá-lo em produção. Para obter mais informações, consulte Inicializar volumes do Amazon EBS no Guia do usuário do Amazon EBS.

Criação de uma AMI usando uma instância

É possível criar uma AMI usando o AWS Management Console ou a linha de comando.

Console

Criar uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância da qual a AMI será criada e escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).

   > **Tip**
   >
   > Se essa opção está desabilitada, sua instância não é uma instância baseada no Amazon EBS.

4. Na página Create image (Criar imagem), especifique as seguintes informações:

   a. Em Image name (Nome da imagem), insira um nome exclusivo para a imagem com até 127 caracteres.

   b. Em Image description (Descrição da imagem), insira uma descrição opcional da imagem, com até 255 caracteres.

   c. Em No reboot (Sem reinicialização), mantenha a caixa de seleção Enable (Habilitar) desmarcada (o padrão) ou marque-a.

   - Se a caixa de seleção Habilitar em Não reinicializar estiver desmarcada, quando o Amazon EC2 criar a nova AMI, ele reinicializará a instância para que possa obter snapshots dos volumes anexados enquanto os dados estiverem em repouso, a fim de garantir um estado consistente.
   - Se a caixa de seleção Habilitar em Não reinicializar estiver marcada, quando o Amazon EC2 criar a nova AMI, ele não desligará e reinicializará a instância.

> **Warning**
>
> Se optar por habilitar No reboot (Sem reinicialização), não poderemos garantir a integridade do sistema de arquivos da imagem criada.

d. Volumes da instância: você pode modificar o volume raiz e adicionar volumes do Amazon EBS e volumes com armazenamento de instância, como mostrado a seguir:

   i. O volume raiz é definido na primeira linha.

      - Para alterar o tamanho do volume raiz, em Size (Tamanho), insira o valor necessário.
      - Se você selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância criada a partir desta AMI, o volume do EBS será excluído. Se você não selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância, o volume do EBS não será excluído. Para obter mais informações, consulte Preservação de dados quando uma instância for encerrada.

   ii. Para adicionar o volume do EBS; escolha Add volume (Adicionar volume) (que acrescenta uma nova linha). Em Tipo de armazenamento, escolha EBS e preencha os campos da linha. Quando você executa uma instância da nova AMI, os volumes adicionais são anexados automaticamente à instância. Os volumes vazios devem ser formatados e montados. Os volumes baseados em um snapshot devem ser montados.

   iii. Para adicionar um volume de armazenamento de instância, consulte Adicionar volumes de armazenamento de instâncias a uma AMI. Quando você executa uma instância da nova AMI, os volumes adicionais são automaticamente inicializados e montados. Esses volumes não contêm dados de volumes de armazenamento de instâncias da instância em execução na qual a AMI foi baseada.

e. Tags: é possível marcar a AMI e os snapshots com as mesmas tags ou pode marcá-los com tags diferentes.

   - Para marcar a AMI e os snapshots com as mesmas tags, escolha Tag image and snapshots together (Marcar Imagem e snapshots juntos). As mesmas tags são aplicadas à AMI e a cada snapshot criado.

- Para marcar a AMI e os snapshots com tags diferentes, escolha Tag image and snapshots separately (Marcar imagem e snapshots separadamente). Diferentes tags são aplicadas à AMI e aos snapshots criados. No entanto, todos os snapshots obtêm as mesmas tags; não é possível marcar cada snapshot com uma tag diferente.

(Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

f. Quando você estiver pronto para criar a AMI, escolha Create image (Criar imagem).

5. Para visualizar o status da AMI enquanto ela estiver sendo criada:

   a. No painel de navegação, selecione AMIs.

   b. Defina o filtro como Owned by me (De minha propriedade) e encontre a AMI na lista.

      Inicialmente, o status será `pending`, mas deverá mudar para `available` após alguns minutos.

6. (Opcional) Para visualizar o snapshot que foi criado para a nova AMI:

   a. Anote o ID da AMI que você localizou na etapa anterior.

   b. No painel de navegação, escolha Snapshots.

   c. Defina o filtro como Owned by me (De minha propriedade) e, em seguida, localize o snapshot da novo ID da AMI na coluna Description (Descrição).

      Quando você inicia uma instância dessa AMI, o Amazon EC2 usa esse snapshot para criar seu volume do dispositivo raiz.

AWS CLI

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- create-image (AWS CLI)
- New-EC2Image (AWS Tools for Windows PowerShell)

Criar uma AMI do Linux a partir de um snapshot

Caso tenha um snapshot do volume do dispositivo raiz de uma instância, você poderá criar uma AMI do Linux com esse snapshot usando o AWS Management Console ou a linha de comando. Atualmente, este recurso não está disponível para instâncias do Windows.

Console

Criar uma AMI de um snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot do qual a AMI será criada e escolha Actions, (Ações), Create image from snapshot (Criar imagem do snapshot).
4. Na página Criar imagem de um snapshot, especifique as seguintes informações:
   a. Em Image name (Nome da imagem), insira um nome descritivo para a imagem.
   b. Em Description (Descrição), insira uma breve descrição da imagem.
   c. Em Architecture (Arquitetura), escolha a arquitetura da imagem. Escolha i386 para 32 bits, x86_64 para 64 bits, arm64 para ARM de 64 bits ou x86_64 para macOS de 64 bits.
   d. Em Root device name (Nome do dispositivo raiz), insira o nome do volume raiz. Para ter mais informações, consulte Nomes de dispositivos em instâncias do Amazon EC2.
   e. Em Virtualization type (Tipo de virtualização), escolha o tipo de virtualização a ser usado por instâncias iniciadas partir dessa AMI. Para ter mais informações, consulte Tipos de virtualização de AMI.
   f. (Somente para virtualização paravirtual) Em Kernel ID (ID do kernel), selecione o kernel do sistema operacional para a imagem. Se você estiver usando um snapshot do volume raiz de uma instância, selecione o mesmo ID do kernel da instância original. Se não tiver certeza, use o kernel padrão.
   g. (Somente para virtualização paravirtual) Ema RAM disk ID (ID do disco de RAM), selecione o disco de RAM para a imagem. Se você selecionar um kernel específico, pode precisar selecionar um disco de RAM específico com os drivers que ofereçam suporte a ele.
   h. Em Modo de inicialização, escolha o modo de inicialização para a imagem ou escolha Usar padrão para que, quando uma instância for iniciada com essa AMI, ela seja

inicializada com o modo de inicialização com suporte para o tipo de instância. Para ter mais informações, consulte Definir o modo de inicialização de uma AMI.

i. (Opcional) Em Mapeamentos de dispositivos de blocos, personalize o volume raiz e adicione os demais volumes de dados.

   Para cada volume, é possível especificar o tamanho, o tipo, as características de performance, o comportamento de exclusão ao término e o status da criptografia. Para o volume da raiz, o tamanho não pode ser menor do que o tamanho do snapshot. Para o tipo de volume, o SSD de uso geral gp3 é a seleção padrão.

j. (Opcional) Em Tags, você pode adicionar uma ou mais tags à nova AMI. (Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

k. Quando você estiver pronto para criar a AMI, escolha Create image (Criar imagem).

AWS CLI

Para criar uma AMI de um snapshot usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- register-image (AWS CLI)
- Register-EC2Image (AWS Tools for Windows PowerShell)

Inicialização de uma instância usando uma AMI que você criou

É possível iniciar uma instância a partir de uma AMI criada a partir de uma instância ou snapshot.

Como iniciar uma instância a partir da AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Defina o filtro como Owned by me (De minha propriedade) e selecione sua AMI.
4. Escolha Iniciar instância a partir da AMI.
5. Aceite os valores padrão ou especifique valores personalizados no assistente de inicialização da instância. Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Criar uma AMI em Linux com armazenamento de instâncias

A AMI que você especifica ao executar a instância determina o tipo de volume do dispositivo raiz

Para criar uma AMI em Linux com armazenamento de instâncias, inicie a instância que você executou a partir de uma AMI em Linux com o armazenamento de instâncias existente. Depois de personalizar a instância para atender às suas necessidades, empacote o volume e registre uma nova AMI, que é possível usar para executar novas instâncias com essas personalizações.

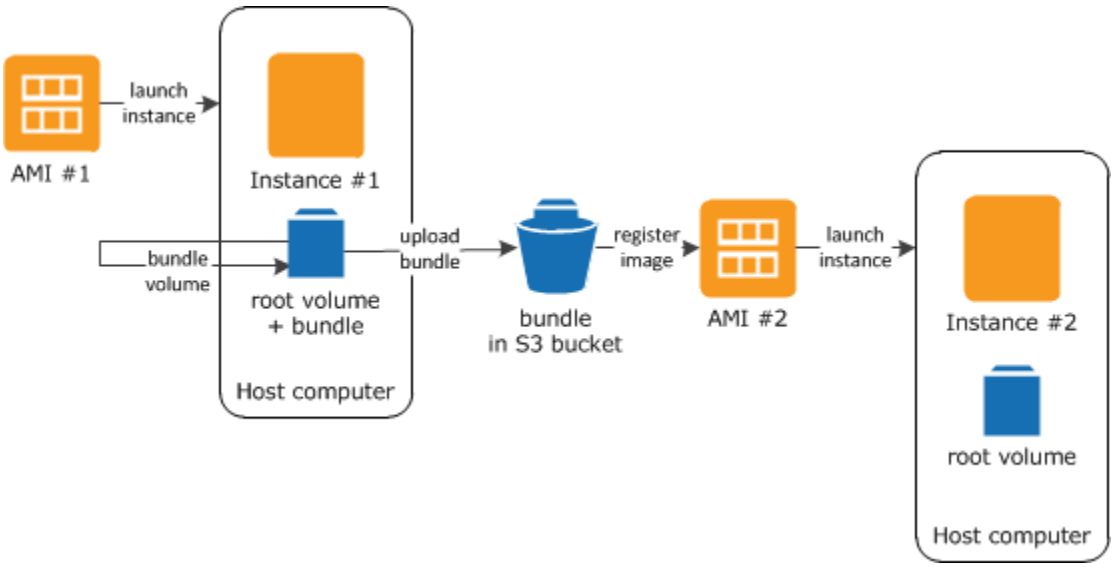
Não é possível criar uma AMI do Windows baseada no armazenamento de instância porque as AMIs do Windows não são compatíveis com o armazenamento de instância para o dispositivo raiz.

> **Important**
>
> Somente os seguintes tipos de instância oferecem suporte a um volume de armazenamento de instância como o dispositivo raiz: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

O processo de criação da AMI é diferente para AMIs baseadas no Amazon EBS. Para obter mais informações sobre as diferenças entre instâncias com Amazon EBS e instâncias com armazenamento de instâncias, e como determinar o tipo de dispositivo raiz para sua instância, consulte Armazenamento para o dispositivo raiz. Se você precisar criar uma AMI baseada no Amazon EBS, consulte Criação de uma AMI baseada no Amazon EBS.

Visão geral do processo de criação para AMIs baseadas no armazenamento de instâncias

O diagrama a seguir resume o processo de criação de uma AMI a partir de uma instância com armazenamento de instâncias.



Primeiro, execute uma instância de uma AMI semelhante à AMI que você deseja criar. É possível conectá-la à sua instância e personalizá-la. Quando a instância estiver configurada da forma como você deseja, é possível empacotá-la. Demora vários minutos para o processo de empacotamento ser concluído. Depois de o processo ser concluído, você terá um pacote, que consiste em um manifesto de imagem (`image.manifest.xml`) e nos arquivos (`image.part.xx`) que contêm um modelo para o volume raiz. Em seguida, você carrega o pacote para seu bucket Amazon S3 e registra sua AMI.

> **Note**
>
> Para carregar objetos para um bucket do S3 para sua AMI de Linux baseada em armazenamento de instâncias, as ACLs devem estar habilitadas para o bucket. Caso contrário, o Amazon EC2 não poderá definir ACLs nos objetos a serem carregados. Se o bucket de destino usar a configuração imposta pelo proprietário do bucket para propriedade de objeto do S3, isso não funcionará, porque as ACLs estarão desabilitadas. Para obter mais informações, consulte Controle da propriedade de objetos carregados usando a propriedade de objeto do S3.

Quando você executa uma instância usando a nova AMI, criamos o volume do dispositivo raiz da instância usando o pacote que você carregou para o Amazon S3. O espaço de armazenamento usado pelo pacote no Amazon S3 gera cobranças na sua conta até que você o exclua. Para obter mais informações, consulte Cancelar o registro de uma AMI (excluir a AMI).

Se você adicionar volumes de armazenamento de instâncias à sua instância além do volume do dispositivo raiz, o mapeamento de dispositivos de blocos para a nova AMI conterá informações para esses volumes, e os mapeamentos de dispositivos de blocos para as instâncias que você executar pela nova AMI conterão automaticamente informações para esses volumes. Para ter mais informações, consulte Mapeamentos de dispositivos de blocos.

Pré-requisitos

Antes que você crie uma AMI, é preciso concluir as tarefas seguir:

- Instale as ferramentas da AMI. Para obter mais informações, consulte Configurar as ferramentas da AMI.
- Instale o AWS CLI. Para obter mais informações, consulte Configuração da AWS Command Line Interface.
- Verifique se você tem um bucket do S3 para o pacote e se o bucket tem ACLs habilitadas. Para obter mais informações sobre a configuração de ACLs, consulte Configuração de ACLs.
  - Para criar um bucket do S3 usando o AWS Management Console, abra o console do Amazon S3 em https://console.aws.amazon.com/s3/ e escolha Criar bucket.
  - Para criar um bucket do S3 com a AWS CLI, é possível usar o comando mb. Se a versão instalada das ferramentas da AMI for 1.5.18 ou posterior, também será possível usar o comando `ec2-upload-bundle` para criar o bucket do S3. Para ter mais informações, consulte ec2-upload-bundle.
- Verifique se você tem seu ID de conta da AWS. Para obter mais informações, consulte Visualizar identificadores de Conta da AWS no Guia de referência de gerenciamento de contas da AWS.
- Certifique-se de ter credenciais para usar o AWS CLI. Para obter mais informações, consulte Best Practices for AWS accounts (Práticas recomendadas para contas da) no Guia de referência do AWS Account Management.
- Verifique se você tem um certificado x.509 e a chave privada correspondente.
  - Se você precisar criar um certificado X.509, consulte Gerenciar certificados de assinatura. O certificado X.509 e a chave privada são usados para criptografar e descriptografar sua AMI.
  - [China (Pequim)] Use o certificado `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (US-West)] Use o certificado `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem`.

- Conecte-se à sua instância e personalize-a. Por exemplo, é possível instalar softwares e aplicações, copiar dados, excluir arquivos temporários e modificar a configuração do Linux.

Tarefas

- Configurar as ferramentas da AMI
- Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias
- Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias
- Converter de uma AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS

Configurar as ferramentas da AMI

É possível usar os comandos das ferramentas de AMI para criar e gerenciar AMIs do Linux com armazenamento de instâncias. Para usar as ferramentas, é necessário instalá-las na sua instância do Linux. As ferramentas das AMIs estão disponíveis como RPM e arquivo .zip para distribuições Linux incompatíveis com RPM.

Para definir as ferramentas da AMI usando RPM

1. Instale o Ruby usando o gerenciador de pacotes para sua distribuição do Linux, como yum. Por exemplo:

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Baixe o arquivo RPM usando uma ferramenta como wget ou curl. Por exemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Verifique se a assinatura do arquivo RPM está usando o seguinte comando:

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

   O comando acima deve indicar que os hashes SHA1 e MD5 do arquivo estão `OK`. Se o comando indicar que os hashes estão `NOT OK`, use o seguinte comando para ver os hashes SHA1 e MD5 do cabeçalho do arquivo:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

Em seguida, compare os hashes SHA1 e MD5 do cabeçalho do arquivo com os seguintes hashes das ferramentas de AMIs verificadas para confirmar a autenticidade do arquivo:

- SHA1 do cabeçalho: a1f662d6f25f69871104e6a62187fa4df508f880
- MD5: 9faff05258064e2f7909b66142de6782

Se os hashes SHA1 e MD5 do cabeçalho do arquivo corresponder aos hashes das ferramentas de AMI verificadas, vá para a próxima etapa.

4. Instale o RPM usando o comando a seguir:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Verifique a instalação das suas ferramentas da AMI usando o comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Se você receber um erro de carregamento, como "não é possível carregar esse arquivo -- ec2/amitools/version (LoadError)", realize a próxima etapa para adicionar o local de instalação das suas ferramentas da AMI para seu `RUBYLIB` caminho.

6. (Opcional) Se você tiver recebido um erro na etapa anterior, adicione a localização das suas ferramentas da AMI para seu caminho `RUBYLIB`.

   a. Execute o comando a seguir para determinar os caminhos a adicionar.

   ```
   [ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
   /usr/lib/ruby/site_ruby/ec2/amitools/version.rb
   /usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
   ```

   No exemplo acima, o arquivo ausente no erro de carga anterior está localizado em `/usr/lib/ruby/site_ruby` e `/usr/lib64/ruby/site_ruby`.

   b. Adicione os locais da etapa anterior ao seu caminho de `RUBYLIB`.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
```

c. Verifique a instalação das suas ferramentas da AMI usando o comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Para configurar as ferramentas da AMI usando o arquivo .zip

1. Instale o Ruby e descompacte usando o gerenciador de pacotes para sua distribuição do Linux, como apt-get. Por exemplo:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Baixe o arquivo .zip usando uma ferramenta como wget ou curl. Por exemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Descompacte os arquivos em um diretório de instalação apropriado, como `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Observe que o arquivo .zip contém uma pasta ec2-ami-tools-*x.x.x*, em que *x.x.x* é o número da versão das ferramentas (por exemplo, `ec2-ami-tools-1.5.7`).

4. Ajuste a variável de ambiente `EC2_AMITOOL_HOME` para o diretório de instalação para as ferramentas. Por exemplo:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Adicione as ferramentas à sua variável de ambiente `PATH`. Por exemplo:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. É possível verificar a instalação das suas ferramentas da AMI usando o comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gerenciar certificados de assinatura

Determinados comandos nas ferramentas da AMI exigem a assinatura de um certificado (também conhecido como certificado X.509). É necessário criar o certificado e, então, carregá-lo para a AWS. Por exemplo, é possível usar uma ferramenta de terceiros, como OpenSSL, para criar o certificado.

Para criar um certificado de assinatura

1. Instale e configure o OpenSSL.
2. Crie uma chave privada usando o comando `openssl genrsa` e salve a saída em um arquivo `.pem`. Recomendamos que você crie uma chave RSA de 2048 ou 4096 bits.

   ```
   openssl genrsa 2048 > private-key.pem
   ```
3. Gere um certificado usando o comando `openssl req`.

   ```
   openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
   out certificate.pem
   ```

Para carregar o certificado para a AWS, use o comando upload-signing-certificate.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Para listar os certificados para um usuário, use o comando list-signing-certificates:

```
aws iam list-signing-certificates --user-name user-name
```

Para desabilitar ou reabilitar um certificado de assinatura para um usuário, use o comando update-signing-certificate. O comando a seguir desabilita o certificado:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Para excluir um certificado, use o comando delete-signing-certificate:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Criar uma AMI a partir de uma instância com armazenamento de instâncias

Os procedimentos a seguir são para criar uma AMI com armazenamento de instâncias com base na instância com armazenamento de instâncias. Antes de começar, certifique-se de que você leu os Pré-requisitos.

Tópicos

- Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias
- Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias

Esta seção descreve a criação da AMI a partir de uma instância do Amazon Linux. Os procedimentos a seguir podem não funcionar para instâncias que executam outras distribuições do Linux. Para procedimentos específicos do Ubuntu, consulte Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias.

Para se preparar para usar as ferramentas da AMI (somente instâncias do HVM)

1. As ferramentas de AMI exigem GRUB Legacy para inicializarem corretamente. Use o comando a seguir para instalar o GRUB:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Instale os pacotes de gerenciamento de partição com o seguinte comando:

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

Para criar uma AMI a partir de uma instância de Amazon Linux com armazenamento de instâncias

Este procedimento pressupõe que você atendeu aos pré-requisitos de Pré-requisitos.

Nos comandos a seguir, substitua cada *espaço reservado para entrada do usuário* por suas próprias informações.

1. Carregue suas credenciais para sua instância. Usamos essas credenciais para garantir que só você e o Amazon EC2 possam acessar sua AMI.

   a. Crie um diretório temporário na sua instância para suas credenciais, da seguinte forma:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   Isso permite que você exclua suas credenciais da imagem criada.

   b. Copie o certificado X.509 e a chave privada correspondente do seu computador para o diretório `/tmp/cert` na sua instância usando uma ferramenta de cópia segura, como scp. A opção `-i` *`my-private-key`*`.pem` no comando scp é a chave privada que você usa para se conectar à sua instância com o SSH, não a chave privada X.509. Por exemplo:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   Como alternativa, por serem arquivos de texto simples, é possível abrir o certificado e a chave em um editor de texto e copiar o conteúdo para novos arquivos em `/tmp/cert`.

2. Prepare o pacote para carregar para o Amazon S3 executando o comando ec2-bundle-vol em sua instância. Não se esqueça de especificar a opção `-e` para de excluir o diretório onde suas credenciais estão armazenadas. Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Para incluir todos os arquivos, use a opção `--no-filter`. Para incluir alguns dos arquivos, use a opção `--include`.

   > **Important**
   >
   > Por padrão, o processo de empacotamento da AMI cria um conjunto de arquivos compactados e criptografados no diretório `/tmp` que representa o volume raiz. Se você não tem o espaço em disco suficiente em `/tmp` para armazenar o pacote, precisa especificar um local diferente para o pacote ser armazenado com a opção `-d` *`/path/to/bundle/storage`*. Algumas instâncias têm armazenamento temporário montado

em `/mnt` ou `/media/ephemeral0` que você pode usar, ou você pode também criar, associar e montar um novo volume do Amazon EBS para armazenar o pacote. Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2.

a. Execute o comando ec2-bundle-vol como raiz. Na maioria dos comandos, é possível usar sudo para ganhar permissões elevadas, mas neste caso, é necessário executar sudo -E su para manter as variáveis do ambiente.

```
[ec2-user ~]$ sudo -E su
```

Observe que prompt bash agora identifica você como usuário raiz, e o cifrão foi substituído por uma hashtag, sinalizando que você está em um shell raiz:

```
[root ec2-user]#
```

b. Para criar o pacote de AMIs, execute o comando ec2-bundle-vol da seguinte forma:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Para as regiões China (Pequim) e AWS GovCloud (US-West), use o parâmetro `--ec2cert` e especifique os certificados de acordo com os pré-requisitos.

Pode demorar alguns minutos para criar a imagem. Quando esse comando for concluído, o diretório `/tmp` (ou não padrão) conterá o pacote (`image.manifest.xml`, além de vários arquivos `image.part.xx`).

c. Saída do shell raiz.

```
[root ec2-user]# exit
```

3. (Opcional) Para adicionar mais volumes de armazenamento de instâncias, edite os mapeamentos de dispositivos de blocos no arquivo `image.manifest.xml` para sua AMI. Para obter mais informações, consulte Mapeamentos de dispositivos de blocos.

   a. Crie um backup do seu arquivo `image.manifest.xml`.

   ```
   [ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Reformate o arquivo `image.manifest.xml` para que seja mais fácil ler e editar.

   ```
   [ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Edite os mapeamentos de dispositivos de blocos em `image.manifest.xml` com um editor de texto. O exemplo abaixo mostra uma nova entrada para o volume do armazenamento de instâncias `ephemeral1`.

   > **Note**
   >
   > Para obter uma lista dos arquivos excluídos, consulte ec2-bundle-vol.

   ```
   <block_device_mapping>
     <mapping>
       <virtual>ami</virtual>
       <device>sda</device>
     </mapping>
     <mapping>
       <virtual>ephemeral0</virtual>
       <device>sdb</device>
     </mapping>
     <mapping>
       <virtual>ephemeral1</virtual>
       <device>sdc</device>
     </mapping>
     <mapping>
       <virtual>root</virtual>
       <device>/dev/sda1</device>
     </mapping>
   </block_device_mapping>
   ```

d. Salve o arquivo `image.manifest.xml` e saia do seu editor de texto.

4. Para fazer upload do pacote para o Amazon S3, execute o comando ec2-upload-bundle da seguinte forma.

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Para registrar a AMI em uma região diferente de US East (N. Virginia), é preciso especificar tanto a região de destino com a opção `--region` quanto um caminho do bucket que já exista na região de destino, ou um caminho de bucket exclusivo que possa ser criado na região de destino.

5. (Opcional) Depois de o pacote ser carregado para o Amazon S3, é possível removê-lo do diretório `/tmp` na instância usando o comando rm a seguir:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Se você tiver especificado um caminho com a opção `-d` */path/to/bundle/storage* em Step 2, use esse caminho em vez de `/tmp`.

6. Para registrar a AMI, execute o comando register-image da seguinte maneira.

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Se você tiver especificado previamente uma região para o comando ec2-upload-bundle, especifique essa região novamente para esse comando.

Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Esta seção descreve a criação de uma AMI a partir de uma instância Ubuntu Linux com um volume de armazenamento de instâncias como o volume raiz. Os procedimentos a seguir podem não funcionar para instâncias que executam outras distribuições do Linux. Para obter procedimentos específicos para o Amazon Linux, consulte Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias.

Para se preparar para usar as ferramentas da AMI (somente instâncias do HVM)

As ferramentas de AMI exigem GRUB Legacy para inicializarem corretamente. Contudo, o Ubuntu está configurado para usar GRUB 2. É necessário verificar se sua instância usa GRUB Legacy e, caso negativo, é preciso instalá-lo e configurá-lo.

As instâncias de HVM também exigem a instalação de ferramentas de particionamento para as ferramentas de AMI funcionarem corretamente.

1. O GRUB Legacy (versão 0.9*x* ou anterior) deve estar instalado na sua instância. Verifique se o GRUB Legacy está presente e instale-o, se necessário.

   a. Verifique a versão da sua instalação do GRUB.

   ```
   ubuntu:~$ grub-install --version
   grub-install (GRUB) 1.99-21ubuntu3.10
   ```

   Neste exemplo, a versão do GRUB é posterior à 0.9*x*, de modo que é necessário instalar o GRUB Legacy. Vá para Step 1.b. Se o GRUB Legacy já estiver presente, vá direto para Step 2.

   b. Instale o pacote `grub` usando o comando a seguir.

   ```
   ubuntu:~$ sudo apt-get install -y grub
   ```

2. Instale os pacotes de gerenciamento de partição a seguir usando o gerenciador de pacotes para sua distribuição.

   - `gdisk` (algumas distribuições podem acessar o pacote `gptfdisk` em seu lugar)
   - `kpartx`
   - `parted`

Use o seguinte comando.

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. Verifique os parâmetros do kernel para sua instância.

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

Observe as opções após o kernel e os parâmetros do dispositivo raiz: `ro`, `console=ttyS0` e `xen_emul_unplug=unnecessary`. Suas opções podem diferir.

4. Verifique as entradas do kernel em `/boot/grub/menu.lst`.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel  /boot/memtest86+.bin
```

Observe se o parâmetro `console` está apontando para `hvc0` em vez de `ttyS0` e se o parâmetro `xen_emul_unplug=unnecessary` está ausente. Mais uma vez, suas opções podem diferir.

5. Edite o arquivo `/boot/grub/menu.lst` com seu editor de texto favorito (como o vim ou o nano) para alterar o console e adicionar os parâmetros identificados anteriormente às entradas de inicialização.

```
title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
 ro console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
 single console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual
```

```
title           Ubuntu 12.04.3 LTS, memtest86+
root            (hd0)
kernel          /boot/memtest86+.bin
```

6. Verifique se suas entradas de kernel agora contêm os parâmetros corretos.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
 xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
 console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7. [Somente para Ubuntu 14.04 e mais recentes] Começando pelo Ubuntu 14.04, AMIs do Ubuntu compatíveis com o armazenamento de instâncias usam uma tabela de partição de GPT e uma partição de EFI separado montados em `/boot/efi`. O comando ec2-bundle-vol não empacotará essa partição de inicialização, portanto você precisa comentar a entrada `/etc/fstab` para a partição EFI, conforme exibido no exemplo a seguir.

```
LABEL=cloudimg-rootfs   /        ext4   defaults        0 0
#LABEL=UEFI     /boot/efi       vfat    defaults        0 0
/dev/xvdb       /mnt    auto    defaults,nobootwait,comment=cloudconfig 0       2
```

Para criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Este procedimento pressupõe que você atendeu aos pré-requisitos de Pré-requisitos.

Nos comandos a seguir, substitua cada *espaço reservado para entrada do usuário* por suas próprias informações.

1. Carregue suas credenciais para sua instância. Usamos essas credenciais para garantir que só você e o Amazon EC2 possam acessar sua AMI.

   a. Crie um diretório temporário na sua instância para suas credenciais, da seguinte forma:

   ```
   ubuntu:~$ mkdir /tmp/cert
   ```

   Isso permite que você exclua suas credenciais da imagem criada.

   b. Copie a chave privada e o certificado X.509 do seu computador para o diretório `/tmp/cert` na sua instância usando uma ferramenta de cópia segura, como a scp. A opção `-i` *my-*

private-key.pem no comando scp é a chave privada que você usa para se conectar à sua instância com o SSH, não a chave privada X.509. Por exemplo:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

Como alternativa, por serem arquivos de texto simples, é possível abrir o certificado e a chave em um editor de texto e copiar o conteúdo para novos arquivos em /tmp/cert.

2. Prepare o pacote para fazer upload para o Amazon S3 executando o comando ec2-bundle-vol a partir de sua instância. Não se esqueça de especificar a opção -e para de excluir o diretório onde suas credenciais estão armazenadas. Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem *.sw, *.swo, *.swp, *.pem, *.priv, *id_rsa*, *id_dsa* *.gpg, *.jks, */.ssh/authorized_keys e */.bash_history. Para incluir todos os arquivos, use a opção --no-filter. Para incluir alguns dos arquivos, use a opção --include.

> **Important**
>
> Por padrão, o processo de empacotamento da AMI cria um conjunto de arquivos compactados e criptografados no diretório /tmp que representa o volume raiz. Se você não tem o espaço em disco suficiente em /tmp para armazenar o pacote, precisa especificar um local diferente para o pacote ser armazenado com a opção -d */path/to/bundle/storage*. Algumas instâncias têm armazenamento temporário montado em /mnt ou /media/ephemeral0 que você pode usar, ou você pode também criar, associar e montar um novo volume do Amazon EBS para armazenar o pacote. Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2.

   a. Execute o comando ec2-bundle-vol como raiz. Na maioria dos comandos, é possível usar sudo para ganhar permissões elevadas, mas neste caso, é necessário executar sudo -E su para manter as variáveis do ambiente.

```
ubuntu:~$ sudo -E su
```

Observe que prompt bash agora identifica você como usuário raiz, e o cifrão foi substituído por uma hashtag, sinalizando que você está em um shell raiz:

```
root@ubuntu:#
```

b. Para criar o pacote de AMIs, execute o comando ec2-bundle-vol da seguinte forma.

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/
cert --partition gpt
```

> **Important**
>
> Para Ubuntu 14.04 e as instâncias HVM posteriores, adicione o marcador `--partition mbr` para empacotar as instruções de inicialização corretamente; caso contrário, sua AMI recém-criada não inicializará.

Pode demorar alguns minutos para criar a imagem. Quando esse comando for concluído, o diretório `tmp` conterá o pacote (`image.manifest.xml`, além de vários arquivos `image.part.xx`).

c. Saída do shell raiz.

```
root@ubuntu:# exit
```

3. (Opcional) Para adicionar mais volumes de armazenamento de instâncias, edite os mapeamentos de dispositivos de blocos no arquivo `image.manifest.xml` para sua AMI. Para obter mais informações, consulte Mapeamentos de dispositivos de blocos.

   a. Crie um backup do seu arquivo `image.manifest.xml`.

   ```
   ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Reformate o arquivo `image.manifest.xml` para que seja mais fácil ler e editar.

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Edite os mapeamentos de dispositivos de blocos em `image.manifest.xml` com um editor de texto. O exemplo abaixo mostra uma nova entrada para o volume do armazenamento de instâncias *ephemeral1*.

```
    <block_device_mapping>
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
      </mapping>
      <mapping>
        <virtual>ephemeral0</virtual>
        <device>sdb</device>
      </mapping>
      <mapping>
        <virtual>ephemeral1</virtual>
        <device>sdc</device>
      </mapping>
      <mapping>
        <virtual>root</virtual>
        <device>/dev/sda1</device>
      </mapping>
    </block_device_mapping>
```

d. Salve o arquivo `image.manifest.xml` e saia do seu editor de texto.

4. Para fazer upload do pacote para o Amazon S3, execute o comando ec2-upload-bundle da seguinte forma.

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Se você pretende registrar a AMI em uma região diferente de US East (N. Virginia), é preciso especificar tanto a região de destino com a opção `--region` quanto um caminho do bucket que já exista na região de destino, ou um caminho de bucket exclusivo que possa ser criado na região de destino.

5. (Opcional) Depois de o pacote ser carregado para o Amazon S3, é possível removê-lo do diretório `/tmp` na instância usando o comando rm a seguir:

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Se você tiver especificado um caminho com a opção `-d` *`/path/to/bundle/storage`* em Step 2, use o mesmo caminho abaixo, em vez de `/tmp`.

6. Para registrar a AMI, execute o comando register-image da AWS CLI da seguinte maneira.

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Se você tiver especificado previamente uma região para o comando ec2-upload-bundle, especifique essa região novamente para esse comando.

7. [Ubuntu 14.04 e posterior] Retire a entrada EFI em `/etc/fstab`; caso contrário, sua instância em execução não conseguirá reinicializar.

Converter de uma AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS

É possível converter uma AMI do Linux com armazenamento de instâncias em uma AMI do Linux baseada no Amazon EBS.

> **Important**
>
> Não é possível converter uma AMI que não lhe pertença.

Para converter uma AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS

1. Execute uma instância do Amazon Linux a partir de uma AMI baseada no Amazon EBS. Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de

instância, versão beta. As instâncias do Amazon Linux têm a AWS CLI e as ferramentas da AMI pré-instaladas.

2. Carregue a chave privada X.509 usada para empacotar sua AMI com armazenamento de instâncias para sua instância. Usamos essa chave para garantir que só você e o Amazon EC2 possam acessar sua AMI.

   a. Crie um diretório temporário na sua instância para a chave privada X.509 da seguinte forma:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   b. Copie a chave privada X.509 do seu computador para o diretório `/tmp/cert` na sua instância usando uma ferramenta de cópia segura, como a scp. O parâmetro *my-private-key* no comando a seguir é a chave privada que você usa para se conectar à sua instância com o SSH. Por exemplo:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   ```

3. Configure as variáveis de ambiente para usar o AWS CLI. Para obter mais informações, consulte Criar um par de chaves.

   a. (Recomendado) Defina as variáveis de ambiente para sua chave de acesso, chave secreta e token de sessão da AWS.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Defina as variáveis de ambiente para sua chave de acesso da AWS e uma chave secreta.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Prepare um volume do Amazon Elastic Block Store (Amazon EBS) para sua nova AMI.

   a. Crie um o volume do EBS vazio na mesma zona de disponibilidade que sua instância usando o comando create-volume. Observe o ID do volume na saída do comando.

> **Important**
>
> Esse volume do EBS deve ter tamanho igual ou superior ao volume do dispositivo raiz do armazenamento de instâncias original.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

b. Associe o volume à sua instância com Amazon EBS usando o comando attach-volume.

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Crie uma pasta para o seu pacote.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Baixe o pacote para sua AMI com armazenamento de instâncias para `/tmp/bundle` usando o comando ec2-download-bundle.

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m
 image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Reconstitua o arquivo de imagem do pacote usando o comando ec2-unbundle.

a. Altere os diretórios para a pasta de pacotes.

```
[ec2-user ~]$ cd /tmp/bundle/
```

b. Execute o comando ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copie os arquivos da imagem não empacotada para o novo volume do EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Teste o volume quanto a quaisquer novas partições não empacotadas.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Liste os dispositivos de blocos para encontrar o nome do dispositivo para montar.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

Neste exemplo, a partição a montar é `/dev/sdb1`, mas o nome do seu dispositivo provavelmente será diferente. Se seu volume não estiver particionado, o dispositivo para montar será semelhante a `/dev/sdb` (sem um dígito final de partição do dispositivo).

11. Crie um ponto de montagem para o novo volume do EBS e monte o volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Abra o arquivo `/etc/fstab` no volume do EBS com seu editor de texto favorito (como o vim ou o nano) e remova todas as entradas dos volumes de armazenamento de instâncias (temporários). Como o volume do EBS é montado em `/mnt/ebs`, o arquivo `fstab` é localizado em `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

Neste exemplo, a última linha deve ser removida.

13. Desmonte o volume e separe-o da instância.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
```

```
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Crie uma AMI a partir do novo volume do EBS, da seguinte forma.

    a. Crie um snapshot do novo volume do EBS.

    ```
    [ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
     "your_snapshot_description" --volume-id volume_id
    ```

    b. Verifique se seu snapshot está concluído.

    ```
    [ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
    id snapshot_id
    ```

    c. Identifique a arquitetura do processador, o tipo de virtualização e a imagem do kernel (`aki`) usados na AMI original com o comando describe-images. Para esta etapa, você precisa do ID da AMI com armazenamento de instâncias original.

    ```
    [ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id
     --output text
    IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
     available public machine aki-fc8f11cc instance-store paravirtual xen
    ```

    Neste exemplo, arquitetura é `x86_64` e o ID da imagem do kernel é `aki-fc8f11cc`. Use os valores a seguir na próxima etapa. Se a saída do comando acima também listar um ID `ari`, anote isso também.

    d. Registre sua nova AMI com o ID do snapshot do seu novo volume do EBS e os valores da etapa anterior. Se a saída do comando anterior listou um ID `ari`, inclua-o no comando seguinte com `--ramdisk-id` *`ari_id`*.

    ```
    [ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
    name your_new_ami_name --block-device-mappings DeviceName=device-
    name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
    architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
    ```

15. (Opcional) Depois de ter testado que pode executar uma instância a partir da nova AMI, é possível excluir o volume do EBS criado para esse procedimento.

    ```
    aws ec2 delete-volume --volume-id volume_id
    ```

Referência de ferramentas da AMI

É possível usar os comandos das ferramentas da AMI para criar e gerenciar AMIs em Linux com armazenamento de instâncias. Para configurar as ferramentas, consulte Configurar as ferramentas da AMI.

Para obter mais informações, consulte Práticas recomendadas para contas da AWS no Guia de referência do AWS Account Management.

Comandos

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opções comuns de ferramentas da AMI

ec2-ami-tools-version

Descrição

Descreve a versão das ferramentas da AMI.

Sintaxe

```
ec2-ami-tools-version
```

Saída

As informações da versão.

Exemplo

Este comando de exemplo exibe as informações da versão das ferramentas de AMI que você está usando.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Descrição

Crie uma AMI em Linux com armazenamento de instâncias a partir de uma imagem de sistema operacional criada em um arquivo de loopback.

Sintaxe

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Opções

`-c, --cert` path

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

`-k, --privatekey` path

O caminho para um arquivo de chave RSA codificado por PEM. Será necessário especificar essa chave para desfazer esse pacote e, assim, mantê-lo em um lugar seguro. Observe que a chave não precisa estar registrada na conta da AWS.

Obrigatório: sim

`-u, --user` account

O ID da conta da AWS do usuário, sem traços.

Obrigatório: sim

`-i, --image` path

O caminho até imagem para fazer o pacote.

Obrigatório: sim

`-d, --destination` path

O diretório no qual o pacote deve ser criado.

Padrão: `/tmp`

Exigido: Não

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em Configurar as ferramentas da AMI, os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

Arquitetura da imagem. Se você não tiver fornecido a arquitetura na linha de comando, ela será solicitada quando o empacotamento for iniciado.

Valores válidos: `i386` | `x86_64`

Exigido: Não

`--productcodes` code1,code2,...

Os códigos de produto para associar à imagem no momento do registro, separado por vírgulas.

Exigido: Não

`-B, --block-device-mapping` mapping

Define como dispositivos de blocos são expostos a uma instância dessa AMI, caso esse tipo de instância seja compatível com o dispositivo especificado.

Especifique uma lista separada por vírgulas de pares de valor-chave, nos quais cada chave é um nome virtual e cada valor é o nome do dispositivo correspondente. Os nomes virtuais incluem o seguinte:

- `ami` — o dispositivo do sistema de arquivos raiz, como visto pela instância
- `root` — o dispositivo do sistema de arquivos raiz, como visto pelo kernel
- `swap` — o dispositivo de troca, como visto pela instância
- `ephemeralN` — o enésimo volume de armazenamento de instâncias

Exigido: Não

`-p, --prefix` prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: O nome de arquivo de imagem. Por exemplo: se o caminho da imagem for `/var/spool/my-image/version-2/debian.img`, o prefixo padrão será `debian.img`.

Exigido: Não

`--kernel` kernel_id

Suspenso. Use register-image para configurar o kernel.

Exigido: Não

`--ramdisk` ramdisk_id

Suspenso. Use register-image para configurar o disco RAM, se necessário.

Obrigatório: Não

Saída

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

Exemplo

Este exemplo cria uma AMI empacotada a partir de uma imagem de sistema operacional criada em um arquivo de loopback.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
```

```
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Descrição

Cria uma AMI em Linux com armazenamento de instâncias ao compactar, criptografar e assinar uma cópia do volume do dispositivo raiz da instância.

O Amazon EC2 tenta herdar códigos de produto, configurações de kernel, configurações do disco RAM e mapeamentos de dispositivos de blocos a partir da instância.

Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Para incluir todos os arquivos, use a opção `--no-filter`. Para incluir alguns dos arquivos, use a opção `--include`.

Para ter mais informações, consulte Criar uma AMI em Linux com armazenamento de instâncias.

Sintaxe

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-
r architecture] [--productcodes code1,code2,...] [-B mapping] [--all] [-e
directory1,directory2,...] [-i file1,file2,...] [--no-filter] [-p prefix]
```

[-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Opções

`-c, --cert` path

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

`-k, --privatekey` path

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Obrigatório: sim

`-u, --user` account

O ID da conta da AWS do usuário, sem traços.

Obrigatório: sim

`-d, --destination` destination

O diretório no qual o pacote deve ser criado.

Padrão: `/tmp`

Exigido: Não

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em Configurar as ferramentas da AMI, os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

A arquitetura da imagem. Se você não tiver fornecido isso na linha de comando, ela será solicitada a fornecer quando o empacotamento for iniciado.

Valores válidos: `i386` | `x86_64`

Exigido: Não

`--productcodes` code1,code2,...

Os códigos de produto para associar à imagem no momento do registro, separado por vírgulas.

Exigido: Não

`-B, --block-device-mapping` mapping

Define como dispositivos de blocos são expostos a uma instância dessa AMI, caso esse tipo de instância seja compatível com o dispositivo especificado.

Especifique uma lista separada por vírgulas de pares de valor-chave, nos quais cada chave é um nome virtual e cada valor é o nome do dispositivo correspondente. Os nomes virtuais incluem o seguinte:

- `ami` — o dispositivo do sistema de arquivos raiz, como visto pela instância
- `root` — o dispositivo do sistema de arquivos raiz, como visto pelo kernel
- `swap` — o dispositivo de troca, como visto pela instância
- `ephemeralN` — o enésimo volume de armazenamento de instâncias

Exigido: Não

`-a, --all`

Inclua todos os diretórios, incluindo aqueles em sistemas de arquivos montados remotamente.

Exigido: Não

`-e, --exclude` directory1,directory2,...

Uma lista de caminhos absolutos e arquivos no diretório para excluir a operação de pacotes. Esse parâmetro substitui a opção `--all`. Quando a exclusão for especificada, os diretórios subdiretórios listados com esse parâmetro não serão reunidos com o volume.

Exigido: Não

`-i, --include` file1,file2,...

Uma lista de arquivos a serem incluídos na operação de pacotes. Os arquivos especificados seriam excluídos da AMI, pois poderiam conter informações sigilosas.

Exigido: Não

`--no-filter`

Se especificado, não excluiremos os arquivos da AMI, pois eles podem conter informações sigilosas.

Exigido: Não

`-p, --prefix` prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: `image`

Exigido: Não

`-s, --size` size

O tamanho, em MB (1024 x 1024 bytes), do arquivo de imagem a ser criado. O tamanho máximo é de 10240 MB.

Padrão: 10240

Exigido: Não

`--[no-]inherit`

Indica se a imagem deve herdar metadados da instância (o padrão é herdar). O empacotamento falhará se você habilitar `--inherit`, mas os metadados de instância não estiverem acessíveis.

Exigido: Não

`-v, --volume` volume

O caminho absoluto até o volume montado, a partir do qual o pacote deve ser criado.

Padrão: O diretório de raiz (/)

Exigido: Não

`-P, --partition` type

Indica se a imagem do disco deve usar uma tabela de partição. Se você não especificar um tipo de tabela de partição, o padrão será o tipo usado no dispositivo de blocos do volume, se aplicável; caso contrário, o padrão é `gpt`.

Valores válidos: `mbr` | `gpt` | `none`

Exigido: Não

`-S, --script` script

Um script de personalização a ser sido executado logo antes do empacotamento. O script deve esperar um único argumento, o ponto de montagem do volume.

Exigido: Não

`--fstab` path

O caminho até fstab para empacotar na imagem. Se isso não estiver especificado, o Amazon EC2 empacotará /etc/fstab.

Exigido: Não

`--generate-fstab`

Empacote o volume usando um fstab fornecido pelo Amazon EC2.

Exigido: Não

`--grub-config`

O caminho para um arquivo alternativo de configuração do GRUB para empacotar na imagem. Por padrão, `ec2-bundle-vol` espera que `/boot/grub/menu.lst` ou `/boot/grub/grub.conf` exista na imagem clonada. Essa opção permite que você especifique um caminho para um arquivo alternativo de configuração do GRUB, que será então copiado para os padrões (se presente).

Exigido: Não

`--kernel` kernel_id

Suspenso. Use register-image para configurar o kernel.

Exigido: Não

`--ramdiskramdisk_id`

Suspenso. Use register-image para configurar o disco RAM, se necessário.

Obrigatório: Não

Saída

Mensagens de status que descrevem os estágios e o status do empacotamento.

Exemplo

Esse exemplo criar uma AMI empacotada ao comprimir, criptografar e assinar um snapshot do sistema de arquivos raiz da máquina local.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
```

```
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

Descrição

Exclui o pacote especificado do armazenamento Amazon S3. Após excluir um pacote, você não pode executar instâncias a partir da AMI correspondente.

Sintaxe

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Opções

`-b, --bucket` bucket

O nome do bucket do Amazon S3 que contém a AMI empacotada, seguido por um prefixo de caminho opcional delimitado por '/'

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: sim

`-t, --delegation-token` token

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte Usar credenciais de segurança temporárias.

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

`--region`*region*

A região a ser usada na assinatura da solicitação.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

`--sigv`*versão*

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`-m, --manifest`*path*

O caminho até o arquivo manifesto.

Obrigatório: Especifique `--prefix` ou `--manifest`.

`-p, --prefix` *prefix*

O prefixo do nome de arquivo da AMI empacotada. Forneça o prefixo inteiro. Por exemplo, se o prefixo for image.img, use `-p image.img`, não. `-p image`

Obrigatório: Especifique `--prefix` ou `--manifest`.

`--clear`

Exclui o bucket Amazon S3 se estiver vazio depois do pacote especificado.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

`-y, --yes`

Pressupõe automaticamente que a resposta a todos os avisos é sim.

Obrigatório: Não

Saída

O Amazon EC2 exibe mensagens de status indicando os estágios e o status do processo de exclusão.

Exemplo

Este exemplo exclui um pacote do Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -
s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET1/image.manifest.xml
DOC-EXAMPLE-BUCKET1/image.part.00
DOC-EXAMPLE-BUCKET1/image.part.01
DOC-EXAMPLE-BUCKET1/image.part.02
DOC-EXAMPLE-BUCKET1/image.part.03
DOC-EXAMPLE-BUCKET1/image.part.04
DOC-EXAMPLE-BUCKET1/image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Descrição

Faz download das AMIs do Linux com armazenamento de instâncias especificadas a partir do armazenamento do Amazon S3.

Sintaxe

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Opções

`-b, --bucket` bucket

O nome do bucket Amazon S3 no qual o pacote está localizado, seguido por um prefixo de caminho opcional delimitado por '/'.

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: sim

`-k, --privatekey` path

A chave privada usada para descriptografar o manifesto.

Obrigatório: sim

`--url` url

O URL do serviço Amazon S3.

Padrão: `https://s3.amazonaws.com/`

Exigido: Não

`--region` region

A região a ser usada na assinatura da solicitação.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

`--sigv` version

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`-m, --manifest` file

O nome do arquivo manifesto (sem o caminho). Recomendamos que você especifique o manifesto (`-m`) ou um prefixo (`-p`).

Exigido: Não

`-p, --prefix` prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: `image`

Exigido: Não

`-d, --directory` directory

O diretório no qual o pacote baixado é salvo. O diretório deve existir.

Padrão: O diretório de trabalho atual.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Obrigatório: Não

Saída

São exibidas as mensagens de status que indicam os vários estágios do processo de download.

Exemplo

Este exemplo cria o diretório `bundled` (usando o comando Linux mkdir) e faz download do pacote do bucket `DOC-EXAMPLE-BUCKET1` do Amazon S3.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

ec2-migrate-manifest

Descrição

Modifica uma AMI em Linux com armazenamento de instâncias (por exemplo, seu certificado, kernel e disco RAM), de forma que suporte uma região diferente.

Sintaxe

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -
s secret_access_key --region region) | (--no-mapping)} [--ec2cert
ec2_cert_path] [--kernel kernel-id] [--ramdisk ramdisk_id]
```

Opções

`-c, --cert` path

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

`-k, --privatekey` path

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Obrigatório: sim

`--manifest` path

O caminho até o arquivo manifesto.

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`--region` region

A região a pesquisar no arquivo de mapeamento.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`--no-mapping`

Desabilita o mapeamento automático de kernels e discos RAM.

Durante a migração, o Amazon EC2 substitui o kernel e o disco RAM no arquivo manifesto por um kernel e disco RAM projetados para a região de destino. A menos que o parâmetro `--no-mapping` seja fornecido, `ec2-migrate-bundle` poderá usar as operações `DescribeRegions` e `DescribeImages` para executar mapeamentos automatizados.

Obrigatório: Obrigatório se não fornecer as opções `-a`, `-s` e `--region` usadas para mapeamento automático.

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo ZIP em Configurar as ferramentas da AMI, os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

`--kernel` kernel_id

O ID do kernel para selecionar.

> **Important**
>
> Recomendamos que você use PV-GRUB em vez de kernels e discos RAM. Para obter mais informações, consulte User provided kernels no Amazon Linux 2 User Guide.

Obrigatório: Não

`--ramdisk` ramdisk_id

O ID do disco RAM para selecionar.

> **Important**
>
> Recomendamos que você use PV-GRUB em vez de kernels e discos RAM. Para obter mais informações, consulte User provided kernels no Amazon Linux 2 User Guide.

Obrigatório: Não

Saída

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

Exemplo

Este exemplo copia a AMI especificada no manifesto `my-ami.manifest.xml` dos EUA para a União Europeia.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Descrição

Recria o pacote a partir de uma AMI em Linux com armazenamento de instâncias.

Sintaxe

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Opções

`-k, --privatekey` path

O caminho para seu arquivo de chave RSA codificado por PEM.

Obrigatório: sim

`-m, --manifest` path

O caminho até o arquivo manifesto.

Obrigatório: sim

`-s, --source` source_directory

O diretório que contém o pacote.

Padrão: O diretório atual.

Exigido: Não

`-d, --destination` destination_directory

O diretório no qual o pacote da AMI deve ser desfeito. O diretório de destino deve existir.

Padrão: O diretório atual.

Obrigatório: Não

Exemplo

Este exemplo de Linux e UNIX desfaz o pacote da AMI especificado no arquivo `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Saída

São exibidas mensagens de status indicando os vários estágios do processo de desempacotamento.

ec2-upload-bundle

Descrição

Carrega o pacote de uma AMI do Linuxbaseada em armazenamento de instâncias para o Amazon S3 e define as lista de controle de acesso (ACLs) apropriadas nos objetos carregados. Para ter mais informações, consulte Criar uma AMI em Linux com armazenamento de instâncias.

> **Note**
>
> Para carregar objetos para um bucket do S3 para sua AMI de Linux baseada em armazenamento de instâncias, as ACLs devem estar habilitadas para o bucket. Caso contrário, o Amazon EC2 não poderá definir ACLs nos objetos a serem carregados. Se o bucket de destino usar a configuração imposta pelo proprietário do bucket para propriedade de objeto do S3, isso não funcionará, porque as ACLs estarão desabilitadas. Para obter mais informações, consulte Controle da propriedade de objetos carregados usando a propriedade de objeto do S3.

Sintaxe

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Opções

`-b, --bucket` bucket

O nome do bucket Amazon S3 no qual armazenar o pacote, seguido por um prefixo de caminho opcional delimitado por '/'. Se o bucket não existir, ele será criado se o nome do bucket estiver disponível. Além disso, se o bucket não existir e a versão das ferramentas da AMI for 1.5.18 ou posterior, esse comando definirá as ACLs para o bucket.

Obrigatório: Sim

`-a, --access-key` access_key_id

Seu ID de chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

Sua chave de acesso secreta da AWS.

Obrigatório: sim

`-t, --delegation-token` token

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte Usar credenciais de segurança temporárias.

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

`-m, --manifest` path

O caminho até o arquivo manifesto. O arquivo manifesto é criado durante o processo de empacotamento e pode ser localizado no diretório que contém o pacote.

Obrigatório: sim

`--url` url

Suspenso. Use a opção `--region` a menos que seu bucket esteja restrito ao local `EU` (e não `eu-west-1`). A marca `--location` é uma única forma de destinar essa restrição específica de local.

O URL do serviço de endpoint do Amazon S3.

Padrão: `https://s3.amazonaws.com/`

Exigido: Não

`--region` region

A região a ser usada na assinatura da solicitação para o bucket do S3 de destino.

- Se o bucket não existir e você não especificar uma região, a ferramenta criará o bucket sem uma restrição de local (em `us-east-1`).
- Se o bucket não existir e você especificar uma região, a ferramenta criará o bucket na região especificada.
- Se o bucket existir e você não especificar uma região, a ferramenta usará o local do bucket.
- Se o bucket existir e você especificar `us-east-1` como região, a ferramenta usará o local real do bucket sem nenhuma mensagem de erro e todos os arquivos correspondentes serão substituídos.
- Se o bucket existir e você especificar uma região (além de `us-east-1`) que não corresponde ao local real do bucket, a ferramenta sairá com um erro.

Se seu bucket estiver restrito ao local `EU` (e não `eu-west-1`), use a marca `--location`. A marca `--location` é uma única forma de destinar essa restrição específica de local.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

`--sigv` version

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`--acl` acl

A política de lista de controle de acesso da imagem empacotada.

Valores válidos: `public-read` | `aws-exec-read`

Padrão: `aws-exec-read`

Exigido: Não

`-d, --directory` directory

O diretório que contém as partes da AMI empacotadas.

Padrão: O diretório que contém o arquivo manifesto (veja a opção `-m`).

Exigido: Não

`--part` part

Inicia a transferência da parte especificada e de todas as partes subsequentes. Por exemplo, `--part 04`.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

`--skipmanifest`

Não faz upload do manifesto.

Exigido: Não

`--location` location

Suspenso. Use a opção `--region`, a menos que seu bucket esteja restrito ao local `EU` (e não `eu-west-1`). A marca `--location` é uma única forma de destinar essa restrição específica de local.

A restrição do local do bucket Amazon S3 de destino. Se o bucket existir e você especificar um local que não corresponde ao local real do bucket, a ferramenta sairá com um erro. Se o bucket existir e você não especificar um local, a ferramenta usará o local do bucket. Se o bucket não existir e você especificar um local, a ferramenta criará o bucket no local especificado. Se o bucket não existir e você não especificar um local, a ferramenta criará o bucket sem uma restrição de local (em `us-east-1`).

Padrão: se `--region` for especificado, o local será definido para essa região especificada. Se `--region` não for especificado, o local padrão será `us-east-1`.

Obrigatório: Não

Saída

O Amazon EC2 exibe mensagens de status que indicam os estágios e o status do processo de upload.

Exemplo

Esse exemplo faz uploads do pacote especificado pelo manifesto `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
```

```
Uploaded manifest.
Bundle upload completed.
```

Opções comuns de ferramentas da AMI

A maioria das ferramentas da AMI aceita os parâmetros opcionais a seguir.

`--help, -h`

Exibe a mensagem de ajuda.

`--version`

Exibe a notificação de versão e direitos autorais.

`--manual`

Exibe a entrada manual.

`--batch`

Executa no modo em lote, suprimindo prompts interativos.

`--debug`

Exibe informações que podem ser úteis ao resolver problemas.

Criação de uma AMI com a ferramenta Sysprep do Windows

A ferramenta Microsoft System Preparation (Sysprep) simplifica o processo de duplicar uma instalação personalizada do Windows. É possível usar o Sysprep para criar uma imagem de máquina da Amazon (AMI) padronizada. É possível criar novas instâncias do Amazon EC2 para o Windows a partir desta imagem padronizada.

Recomendamos que você use o EC2 Image Builder para automatizar a criação, o gerenciamento e a implantação de imagens de servidor “douradas” personalizadas, seguras e atualizadas que são pré-instaladas e pré-configuradas com software e configurações.

Se você usar a ferramenta Sysprep do Windows para criar uma AMI padronizada, recomendamos executá-la com EC2Launch v2. Se você ainda estiver usando os agentes EC2Config (Windows Server 2012 R2 e anterior) ou EC2Launch (Windows Server 2016 e 2019), consulte a documentação para usar o Sysprep com o EC2Config e o EC2Launch a seguir.

> **Important**
>
> Não use o Sysprep para criar um backup da instância. O Sysprep remove informações específicas do sistema; remover essas informações pode ter consequências não intencionais para um backup da instância.

Para solucionar problemas do Sysprep, consulte Solução de problemas de Sysprep com instâncias do Windows.

Tópicos

- Antes de começar
- Usar o Sysprep com o EC2Launch v2
- Usar o Sysprep com o EC2Launch
- Usar o Sysprep com o EC2Config

Antes de começar

- Antes de executar o Sysprep, recomendamos que você remova todas as contas de usuário locais e todos os perfis de conta, exceto a única conta de administrador em que o Sysprep será executado. Se você executar Sysprep com contas e perfis adicionais, um comportamento inesperado poderá acontecer, incluindo perda de dados de perfil ou falha de conclusão do Sysprep.
- Saiba mais sobre o Sysprep no Microsoft TechNet.
- Saiba quais funções do servidor são compatíveis com Sysprep.

Usar o Sysprep com o EC2Launch v2

Esta seção contém detalhes sobre as diferentes fases de execução do Sysprep e as tarefas executadas pelo serviço EC2Launch v2 à medida que a imagem é preparada. Ele também inclui as etapas para criar uma AMI padronizada usando o Sysprep com o serviço EC2Launch v2.

Sysprep com tópicos do EC2Launch v2

- Fases do Sysprep
- Ações do Sysprep
- Após Sysprep

- Executar o Sysprep com o EC2Launch v2

Fases do Sysprep

O Sysprep é executado nas seguintes fases:

- Generalizar: a ferramenta elimina informações e configurações específicas da imagem. Por exemplo, o Sysprep remove o identificador de segurança (SID), o nome do computador, os logs de evento e os drivers específicos, entre outros. Após essa fase ser encerrada, o sistema operacional (SO) estará pronto para criar a AMI.

  > **Note**
  >
  > Ao executar o Sysprep com o serviço EC2Launch v2, o sistema impede que os drivers sejam removidos porque, por padrão, a configuração `PersistAllDeviceInstalls` é definida como true.

- Especializar: o plug and play examina o computador e instala drivers para todos os dispositivos detectados. A ferramenta gera requisitos do sistema operacional, como o nome de computador e o SID. Opcionalmente, é possível executar comandos nessa fase.
- Experiência Out-of-Box (OOBE): o sistema executa uma versão abreviada da configuração do Windows e pede para o usuário inserir informações como o idioma do sistema, o fuso horário e a organização registrada. Quando você executa o Sysprep com o EC2Launch v2, o arquivo de resposta automatiza essa fase.

Ações do Sysprep

O Sysprep e o EC2Launch v2 executam as seguintes ações ao preparar uma imagem.

1. Quando você escolhe Shutdown with Sysprep (Desligar com Sysprep) na caixa de diálogo EC2Launch settings (Configurações do EC2Launch), o sistema executa o comando `ec2launch sysprep`.
2. O EC2Launch v2 edita o conteúdo do arquivo `unattend.xml` lendo o valor do registro em `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. O arquivo está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

A chave de registro desabilita as conexões RDP até serem re-habilitadas. Desabilitar as conexões RDP é uma medida de segurança necessária, pois, na primeira sessão de inicialização após o Sysprep ser executado, há um breve período no qual a RDP permite conexões e senha do Administrador fica em branco.

4. O serviço EC2Launch v2 chama o Sysprep executando o seguinte comando:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml"

Generalizar a fase

- O EC2Launch v2 remove informações e configurações específicas da imagem, como o nome do computador e o SID. Se a instância pertencer a um domínio, ela será removida do domínio. O arquivo de resposta `unattend.xml` inclui as seguintes configurações que afetam a fase:
  - PersistAllDeviceInstalls: essa configuração impede que a Configuração do Windows remova e reconfigure dispositivos, o que acelera o processo de preparação de imagem, pois as AMIs da Amazon exigem a execução de determinados drivers e a nova detecção desses drivers tomaria o tempo.
  - DoNotCleanUpNonPresentDevices: essa configuração retém informações de plug and play para dispositivos que não estão presentes no momento.
- O Sysprep fecha o SO à medida que se prepara para criar a AMI. O sistema executa uma nova instância ou inicia a instância original.

Fase especializada

O sistema gera requisitos específicos do sistema operacional, como um nome de computador e um SID. O sistema também executa as ações a seguir com base nas configurações que você especifica no arquivo de resposta `unattend.xml`.

- CopyProfile: o Sysprep pode ser configurado para excluir todos os perfis de usuário, incluindo o perfil incorporado do Administrador. Essa configuração retém a conta incorporada do administrador, de forma que todas as personalizações que você fizer nessa conta serão transferidas para a nova imagem. O valor padrão é `True`.

CopyProfile substitui o perfil padrão pelo perfil de administrador local existente. Todas as contas em que você faz login depois da execução do Sysprep recebem uma cópia desse perfil e de seu conteúdo no primeiro login.

Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para `False`. O Sysprep removerá todos os perfis de usuário (isso economiza tempo e espaço em disco).

- TimeZone: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha:

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
PASSWORDREQ:YES
```

- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança foi projetada para impedir que a instância seja acessível após a conclusão do Sysprep, caso você não tenha configurado a tarefa `setAdminAccount`.

  O sistema executa o seguinte comando no diretório local do agente de inicialização (`C:\Program Files\Amazon\EC2Launch\`).

```
EC2Launch.exe internal randomize-password --username Administrator
```

- Para habilitar conexões de área de trabalho remota, o sistema define a chave de registro `fDenyTSConnections` do Terminal Server como false.

Fase OOBE

1. O sistema especifica as seguintes configurações usando o arquivo de resposta do EC2Launch v2:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`

- `<ProtectYourPC>3</ProtectYourPC>`
- `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
- `<TimeZone>UTC</TimeZone>`
- `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
- `<RegisteredOwner>EC2</RegisteredOwner>`

> **Note**
>
> Durante as fases de generalização e de especialização, o EC2Launch v2 monitora o status do sistema operacional. Se o EC2Launch v2 detectar que o sistema operacional está na fase Sysprep, ele publicará a seguinte mensagem no log do sistema:
> O Windows está sendo configurado. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. O sistema executa o EC2Launch v2.

Após Sysprep

Após a conclusão do Sysprep, o EC2Launch v2 envia a seguinte mensagem para a saída do console:

```
Windows sysprep configuration complete.
```

Depois, o EC2Launch v2 executa as ações a seguir:

1. Lê o conteúdo do arquivo `agent-config.yml` e executa as tarefas configuradas.
2. Executa todas as tarefas no estágio `preReady`.
3. Após a conclusão, envia uma mensagem `Windows is ready` para os logs do sistema de instância.
4. Executa todas as tarefas no estágio `PostReady`.

Para obter mais informações sobre o EC2Launch v2, consulte Configurar uma instância do Windows usando o EC2Launch v2.

Executar o Sysprep com o EC2Launch v2

Use o procedimento a seguir para criar uma AMI padronizada usando o Sysprep com o EC2Launch v2.

1. No console do Amazon EC2, localize uma AMI que você deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize-a.
4. No menu Start (Iniciar) do Windows, procure e escolha Amazon EC2Launch settings (Configurações do Amazon EC2Launch). Para obter mais informações sobre as opções e configurações na caixa de diálogo Amazon EC2Launch settings (Configurações do Amazon EC2Launch), consulte Configurações do EC2Launch v2.
5. Selecione Shutdown with Sysprep (Desligar com Sysprep) ou Shutdown without Sysprep (Desligar sem Sysprep).

Quando houver uma solicitação para confirmar que você deseja executar o Sysprep e desativar a instância, clique em Yes (Sim). EC2Launch v2 executa o Sysprep. Você é desconectado da instância, e a instância é desligada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância será alterado de `Running` para `Stopping` e para `Stopped`. Nesse momento, é seguro criar uma AMI com base nessa instância.

É possível invocar manualmente a ferramenta Sysprep pela linha de comando usando o seguinte comando:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Usar o Sysprep com o EC2Launch

O EC2Launch oferece um arquivo de resposta padrão e arquivos em lote para o Sysprep que automatizam e protegem o processo de preparação de imagem na AMI. A modificação desses arquivos é opcional. Esses arquivos estão localizados no seguinte diretório por padrão: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Não use o Sysprep para criar um backup da instância. O Sysprep remove as informações específicas ao sistema. Se você remover essas informações, poderá haver consequências não intencionais em um backup da instância.

Sysprep com tópicos do EC2Launch

- Arquivos de resposta e em lotes do EC2Launch para o Sysprep
- Executar o Sysprep com o EC2Launch
- Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada

Arquivos de resposta e em lotes do EC2Launch para o Sysprep

O arquivo de resposta e os arquivos em lote do EC2Launch para o Sysprep incluem o seguinte:

`Unattend.xml`

Esse é o arquivo de resposta padrão. Se você executar o `SysprepInstance.ps1` ou escolher ShutdownWithSysprep na interface do usuário, o sistema lerá a configuração nesse arquivo.

`BeforeSysprep.cmd`

Personalize esse arquivo em lote para executar comandos antes que o EC2Launch execute o Sysprep.

`SysprepSpecialize.cmd`

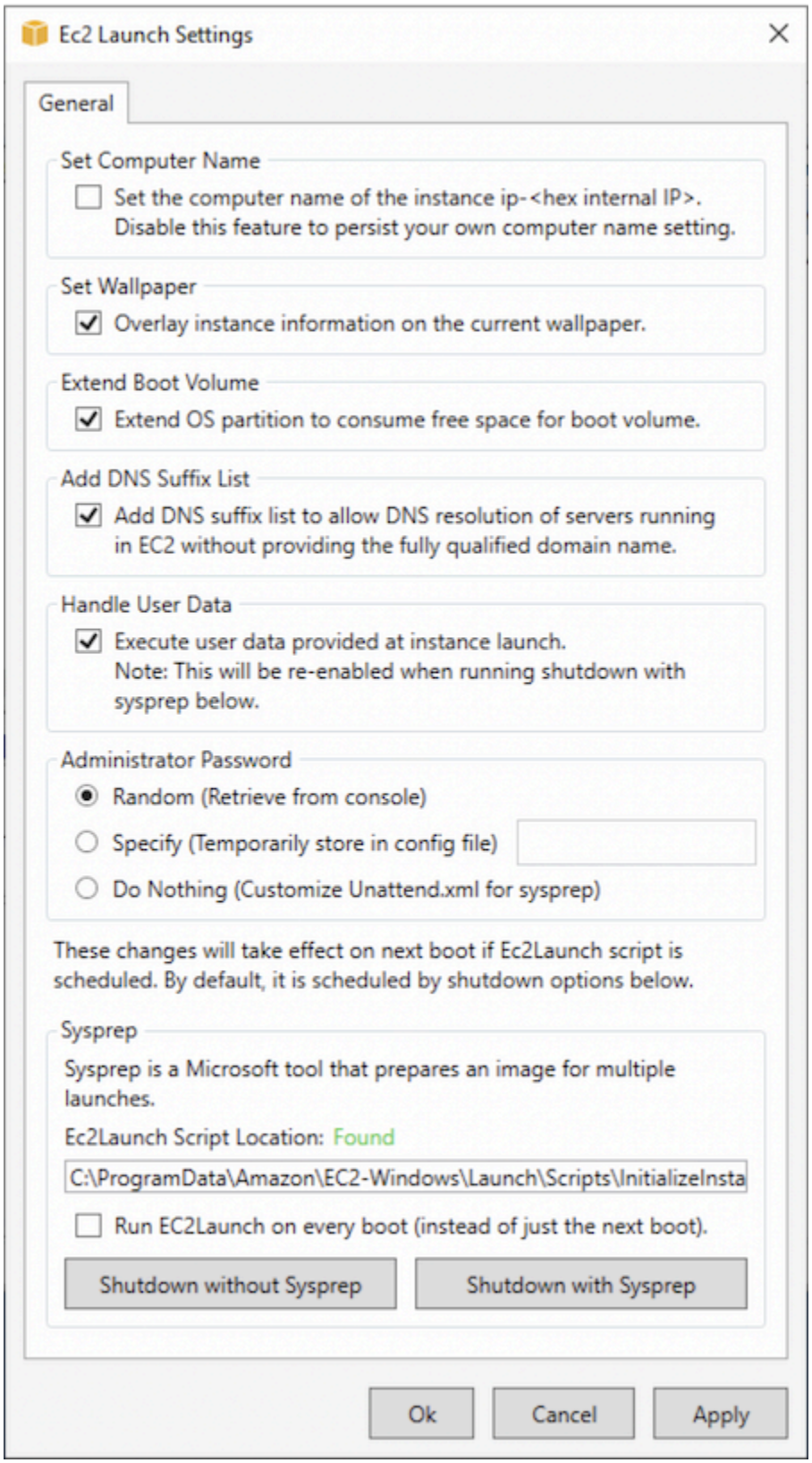
Personalize esse arquivo em lotes para executar comandos durante a fase de especialização do Sysprep.

Executar o Sysprep com o EC2Launch

Na instalação completa do Windows Server 2016 e posterior (com uma experiência de desktop), é possível executar o Sysprep com o EC2Launch manualmente ou usar a aplicação EC2 Launch Settings (Configurações de execução do EC2).

Para executar o Sysprep usando a aplicação de configurações do EC2Launch

1. No console do Amazon EC2, localize ou crie uma AMI do Windows Server 2016 ou posterior.
2. Execute uma instância do Windows a partir da AMI.
3. Conecte-se à sua instância do Windows e personalize-a.
4. Pesquise e execute a aplicação EC2LaunchSettings. Por padrão, ele está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Selecione ou limpe as opções conforme for necessário. Essas configurações são armazenadas no arquivo `LaunchConfig.json`.

6. Em Administrator password, faça uma das seguintes ações:

   - Escolha Random. O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.
   - Escolha Specify e digite a senha que atende aos requisitos do sistema. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. Se você fechar agora, a senha será definida imediatamente. O EC2Launch criptografa a senha usando a chave de usuário.
   - Escolha DoNothing e especifique uma senha no arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.

7. Escolha Shutdown with Sysprep (Desligar com Sysprep).

Para usar o Sysprep manualmente usando o EC2Launch

1. No console do Amazon EC2, localize ou crie uma AMI Datacenter Edition do Windows Server 2016 ou posterior que você deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize a instância.
4. Especifique as configurações no arquivo `LaunchConfig.json`. Por padrão, esse arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Para `adminPasswordType`, especifique um dos seguintes valores:

   `Random`

   O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

   `Specify`

   O EC2Launch usa a senha que você especifica `adminPassword`. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

`DoNothing`

O EC2Launch usa a senha que você especifica o arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.

5. (Opcional) Especifique as configurações em `unattend.xml` e em outros arquivos de configuração. Se o plano atender à instalação, você não precisará fazer alterações nesses arquivos. Por padrão, os arquivos estão localizados no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. No Windows PowerShell, execute `./InitializeInstance.ps1 -Schedule`. Por padrão, o script está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Esse script agenda a instância para ser inicializada durante a próxima inicialização. Execute esse script antes de executar o script `SysprepInstance.ps1` na próxima etapa.
7. No Windows PowerShell, execute `./SysprepInstance.ps1`. Por padrão, o script está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Você é desconectado da instância, e a instância é encerrada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância será alterado de `Running` para `Stopping` e, em seguida, para `Stopped`. Nesse momento, é seguro criar uma AMI com base nessa instância.

Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada

Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada, siga estas etapas:

- Execute a GUI EC2LaunchSettings (C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe) e selecione a opção para encerrar com o Sysprep.
- Execute EC2LaunchSettings e desligue sem o Sysprep antes de criar a AMI. Isso configura as tarefas de inicialização do EC2 para serem executadas na próxima inicialização, que definirá as rotas com base na sub-rede da instância.
- Reprograme manualmente as tarefas de inicialização do EC2 antes de criar uma AMI do PowerShell.

> **Important**
>
> Observe o comportamento padrão de redefinição de senha antes de reprogramar as tarefas.

- Para atualizar as rotas em uma instância em execução que está passando por ativação do Windows ou comunicação com falhas de metadados de instância, consulte "Não é possível ativar o Windows".

Usar o Sysprep com o EC2Config

Esta seção contém os detalhes das diferentes fases de execução do Sysprep e das tarefas executadas pelo serviço EC2Config enquanto a imagem é preparada. Ela também inclui as etapas para criar uma AMI padronizada usando o Sysprep com o serviço EC2Config.

Sysprep com tópicos EC2Config

- Fases do Sysprep
- Ações do Sysprep
- Após Sysprep
- Executar o Sysprep com o serviço EC2Config

Fases do Sysprep

O Sysprep é executado nas seguintes fases:

- Generalizar: a ferramenta elimina informações e configurações específicas da imagem. Por exemplo, o Sysprep remove o identificador de segurança (SID), o nome do computador, os logs de evento e os drivers específicos, entre outros. Após essa fase ser encerrada, o sistema operacional (SO) estará pronto para criar a AMI.

> **Note**
>
> Quando você executa o Sysprep com o serviço EC2Config, o sistema impede que os drivers sejam removidos, pois a configuração PersistAllDeviceInstalls é definida como verdadeira por padrão.

- Especializar: o plug and play examina o computador e instala drivers para todos os dispositivos detectados. A ferramenta gera requisitos de SO, como nome de computador e SID. Opcionalmente, é possível executar comandos nessa fase.
- Out-of-Box Experience (OOBE): o sistema executa uma versão abreviada da configuração do Windows e pede para o usuário digitar informações como idioma do sistema, fuso horário e uma organização registrada. Quando você executa o Sysprep com o EC2Config, o arquivo de resposta automatiza essa fase.

Ações do Sysprep

O Sysprep e o serviço EC2Config executam as ações a seguir ao preparar uma imagem.

1. Quando você escolhe Encerrar com o Sysprep na caixa de diálogo Propriedades do EC2 Service), o sistema executa o comando ec2config.exe -sysprep.
2. O serviço EC2Config lê o conteúdo do arquivo `BundleConfig.xml`. Esse arquivo está localizado no diretório a seguir, por padrão: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   O arquivo `BundleConfig.xml` inclui as seguintes configurações. É possível alterar essas configurações:

   - AutoSysprep: indica se o Sysprep deve ser usado automaticamente. Você não precisará mudar esse valor se estiver executando o Sysprep pela caixa de diálogo de propriedades do serviço EC2. O valor padrão é `No`.
   - SetRDPCertificate: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use com segurança o Remote Desktop Protocol (RDP) para se conectar à instância. Altere o valor para `Yes` se as novas instâncias precisarem usar um certificado. Essa configuração não é usada com instâncias Windows Server 2012 porque esses sistemas operacionais podem gerar seus próprios certificados. O valor padrão é `No`.
   - SetPasswordAfterSysprep: define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor para `No` se novas instâncias não precisarem ser definidas com uma senha criptografada aleatória. O valor padrão é `Yes`.
   - PreSysprepRunCmd: o local do comando para execução. Por padrão, o comando está localizado no seguinte diretório:: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   A chave de registro desabilita as conexões RDP até serem re-habilitadas. Desabilitar as conexões RDP é uma medida de segurança necessária, pois, na primeira sessão de inicialização após o Sysprep ser executado, há um breve período no qual a RDP permite conexões e senha do Administrador fica em branco.

4. O serviço EC2Config chama o Sysprep executando o seguinte comando:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Generalizar a fase

- A ferramenta remove informações específicas da imagem e as configurações, como nome de computador e SID. Se a instância pertencer a um domínio, ela será removida do domínio. O arquivo de resposta `sysprep2008.xml` inclui as seguintes configurações que afetam a fase:
  - PersistAllDeviceInstalls: essa configuração impede que a Configuração do Windows remova e reconfigure dispositivos, o que acelera o processo de preparação de imagem, pois as AMIs da Amazon exigem a execução de determinados drivers e a nova detecção desses drivers tomaria o tempo.
  - DoNotCleanUpNonPresentDevices: essa configuração retém informações de plug and play para dispositivos que não estão presentes no momento.
- O Sysprep fecha o SO à medida que se prepara para criar a AMI. O sistema executa uma nova instância ou inicia a instância original.

Fase especializada

O sistema gera requisitos específicos de SO, como um nome de computador e um SID. O sistema também executa as ações a seguir com base em configurações que você especifica no arquivo de resposta sysprep2008.xml.

- CopyProfile: o Sysprep pode ser configurado para excluir todos os perfis de usuário, incluindo o perfil incorporado do Administrador. Essa configuração retém a conta de Administrador incorporada, de forma que todas as personalizações que você fizer nessa conta serão transferidas para a nova imagem. O valor padrão é Verdadeiro.

  CopyProfile substitui o perfil padrão pelo perfil de administrador local existente. Todas as contas conectadas depois da execução de Sysprep receberão uma cópia desse perfil e do conteúdo no primeiro login.

  Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para falso. O Sysprep removerá todos os perfis de usuário; isso economiza tempo e espaço em disco.
- TimeZone: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /PASSWORDREQ:YES
- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança é projetada para impedir que a instância fique acessível após o Sysprep ser concluído, caso você não tenha habilitado a configuração ec2setpassword.

  C:\Program Files\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator
- Comando síncrono com pedido 3: o sistema executa o seguinte comando:

  C:\Program Files\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd

  Esse comando adiciona a seguinte chave de registro, que re-habilita a RDP:

  reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

Fase OOBE

1. Usando o arquivo de resposta do serviço EC2Config, o sistema especifica as seguintes configurações:
   - <InputLocale>en-US</InputLocale>

- <SystemLocale>en-US</SystemLocale>
- <UILanguage>en-US</UILanguage>
- <UserLocale>en-US</UserLocale>
- <HideEULAPage>true</HideEULAPage>
- <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
- <NetworkLocation>Other</NetworkLocation>
- <ProtectYourPC>3</ProtectYourPC>
- <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
- <TimeZone>UTC</TimeZone>
- <RegisteredOrganization>Amazon.com</RegisteredOrganization>
- <RegisteredOwner>Amazon</RegisteredOwner>

> **Note**
>
> Durante as fases de generalização e especialização, o serviço EC2Config monitora o status do SO. Se o EC2Config detectar que o sistema operacional está na fase Sysprep, ele publicará a seguinte mensagem no log do sistema: EC2ConfigMonitorState: 0 O Windows está sendo configurado. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Após a conclusão da fase OOBE, o sistema executa `SetupComplete.cmd` a partir do seguinte local: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Na AMIs públicas da Amazon antes de abril de 2015 este arquivo estava vazio e não executava nada na imagem. Em AMIs públicas posteriores a abril de 2015, o arquivo inclui o seguinte valor: call "C:\Program Files \Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. O sistema executa `PostSysprep.cmd`, que realiza as seguintes operações:
   - Define a senha do Administrador para não expirar. Se a senha expirou, os Administradores podem não conseguir fazer login.
   - Define o nome da máquina MSSQLServer (se instalada) para que o nome esteja em sincronia com a AMI.

Após Sysprep

Após o Sysprep ser concluído, os serviços do EC2Config enviam a seguinte mensagem para a saída do console:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

O EC2Config então executa as ações a seguir:

1. Lê o conteúdo do arquivo config.xml e lista todos os plug-ins habilitados.
2. Executa todos os plug-ins "Antes que o Windows esteja pronto" ao mesmo tempo.
   - Ec2SetPassword
   - Ec2SetComputerName
   - Ec2InitializeDrives
   - Ec2EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2SetDriveLetter
   - Ec2WindowsActivate
   - Ec2DynamicBootVolumeSize
3. Após estar concluído, envia uma mensagem "O Windows está pronto" para os logs do sistema de instância.
4. Executa todos os plug-ins "Após o Windows estar pronto" ao mesmo tempo.
   - Amazon CloudWatch Logs
   - UserData
   - AWS Systems Manager (Systems Manager)

Para obter mais informações sobre plug-ins do Windows, consulte Configuração de uma instância do Windows usando o serviço EC2Config (herdado).

Executar o Sysprep com o serviço EC2Config

Use o procedimento a seguir para criar uma AMI padronizada usando Sysprep e serviço EC2Config.

1. No console do Amazon EC2, localize ou crie a AMI que deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize-a.
4. Especifique as definições de configuração no arquivo de resposta do serviço EC2Config:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```

5. No menu Iniciar do Windows, escolha Todos os Programas e Configurações do EC2ConfigService.
6. Escolha a guia Image (Imagem) na caixa de diálogo Ec2 Service Properties (Propriedades do serviço Ec2). Para obter mais informações sobre as opções e as configurações da caixa de diálogo Ec2 Service Properties (Propriedades do serviço Ec2), consulte Propriedades do serviço Ec2.
7. Selecione uma opção para a senha do Administrador e selecione Shutdown with Sysprep (Desativação com Sysprep) ou Shutdown without Sysprep (Desativação sem Sysprep). O EC2Config edita os arquivos de configuração com base na opção de senha selecionada.
   - Random (Aleatório): o EC2Config gera uma senha, criptografa-a com a chave do usuário e exibe a senha criptografada no console. Nós desabilitamos essa configuração depois da primeira execução, de forma que essa senha persistirá se a instância for reinicializada ou parada e inicializada.
   - Specify (Especificar): a senha é armazenada no arquivo de resposta do Sysprep de forma não criptografada (texto aberto). Quando o Sysprep é executado em seguida, ele define a senha do Administrador. Se você fechar agora, a senha será definida imediatamente. Quando o serviço é reiniciado novamente, a senha do Administrador é removida. É importante recordar essa senha, pois você não poderá recuperá-la depois.
   - Keep Existing (Manter existente): a senha existente para a conta do Administrador não muda quando o Sysprep é executado ou o EC2Config é reiniciado. É importante recordar essa senha, pois você não poderá recuperá-la depois.
8. Escolha OK.

Quando houver uma solicitação para confirmar que você deseja executar o Sysprep e desativar a instância, clique em Yes (Sim). Você verá que o EC2Config executa Sysprep. Em seguida, você é desconectado da instância e a instância é desligada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância mudará de `Running` para `Stopping` e, finalmente, para `Stopped`. Nesse momento, é seguro criar uma AMI com base nessa instância.

É possível invocar manualmente a ferramenta Sysprep pela linha de comando usando o seguinte comando:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> As aspas duplas no comando não serão necessárias se o shell do seu CMD já estiver no diretório C:\Program Files\Amazon\EC2ConfigService\.

Contudo, é necessário ser muito cuidadoso para que as opções do arquivo XML especificadas na pasta `Ec2ConfigService\Settings` estejam corretas; caso contrário, pode não conseguir conectar-se à instância. Para obter mais informações sobre os arquivos de configurações, consulte Arquivos de configurações do EC2Config. Para ver um exemplo de como configurar e executar o Sysprep pela linha de comando, consulte `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Modificar uma AMI do

É possível modificar um conjunto limitado de atributos da imagem de máquina da Amazon (AMI), como a descrição da AMI e as propriedades de compartilhamento. No entanto, o conteúdo da AMI (dados binários de volume) não pode ser modificado. Para modificar o conteúdo da AMI, você deve criar uma nova AMI.

> **Important**
>
> Você não pode modificar o conteúdo (dados binários de volume) de uma AMI baseada em EBS porque os snapshots que o sustentam são imutáveis. Você também não pode modificar o conteúdo (dados binários de volume) de uma AMI do Linux baseada no armazenamento de instância (baseada no S3) porque o conteúdo é assinado e as inicializações de instância falharão se as assinaturas não corresponderem.

Para os atributos da AMI que podem ser modificados, consulte ModifyImageAttribute na Referência da API do Amazon EC2.

Os tópicos a seguir fornecem instruções para o uso do console do Amazon EC2 e da AWS CLI para modificar os atributos de uma AMI:

- Tornar um AMI pública
- Compartilhe uma AMI com organizações ou unidades organizacionais específicas
- Compartilhar uma AMI com contas específicas da AWS
- Usar suporte pago
- Configurar a AMI

Copiar um AMI

É possível copiar uma imagem de máquina da Amazon (AMI) dentro ou através de regiões da AWS. É possível copiar as AMIs baseadas no Amazon EBS e as AMIs baseadas em armazenamento de instâncias. É possível copiar AMIs baseadas no EMS com snapshots criptografados e também alterar o status de criptografia durante o processo de cópia. É possível copiar as AMIs que são compartilhadas com você.

Copiar uma AMI de origem resulta em uma nova AMI idêntica, mas separada, que também é chamada de AMI de destino. A AMI de destino tem o próprio ID de AMI exclusivo. É possível alterar ou cancelar o registro da AMI de origem sem afetar a AMI de destino. O inverso também é verdadeiro.

No caso de uma AMI baseada no EBS, cada um de seus snapshots de suporte é copiado para um snapshot de destino idêntico, mas separado. Se você copiar uma AMI para uma nova Região, os snapshots serão cópias completas (não incrementais). Se você criptografar snapshots de suporte não criptografados ou criptografá-los para uma nova chave KMS, os snapshots serão cópias completas (não incrementais). Operações de cópia subsequentes de uma AMI resultam em cópias incrementais dos snapshots de suporte.

Conteúdo

- Considerações
- Custos
- Permissões do IAM
- Copiar um AMI
- Parar uma operação de cópia de AMI pendente
- Cópia entre regiões
- Cópia entre contas

- Criptografar e copiar

Considerações

- Permissão para copiar AMIs: é possível usar políticas do IAM para conceder ou negar aos usuários permissão para copiar AMIs. As permissões no nível do recurso especificadas para a ação `CopyImage` se aplicam somente à nova AMI. Não é possível especificar permissões no nível do recurso para a AMI de origem.
- Permissões de execução e permissões de bucket do Amazon S3: a AWS não copia permissões de execução nem permissões de bucket do Amazon S3 da AMI de origem para a nova AMI. Após a conclusão da operação de cópia, você pode aplicar permissões de inicialização e permissões de bucket do Amazon S3 à nova AMI.
- Tags: é possível copiar somente as tags de AMI definidas pelo usuário que você anexou à AMI de origem. Tags do sistema (prefixadas com `aws:`) e tags definidas pelo usuário anexadas por outras Contas da AWS não serão copiadas. Ao copiar uma AMI, você pode anexar novas tags à AMI de destino e seus snapshots de suporte.

Custos

Não há cobrança para copiar uma AMI. Mas aplicam-se as taxas padrão de transferência de dados e armazenamento. Se copiar uma AMI baseada em EBS, você será cobrado pelo armazenamento de snapshots adicionais do EBS.

Permissões do IAM

Para copiar uma AMI baseada em EBS ou em armazenamento de instâncias, as seguintes permissões do IAM são necessárias:

- `ec2:CopyImage`: para copiar a AMI. Para AMIs baseadas no EBS, ele também concede permissão para copiar os snapshots de suporte da AMI.
- `ec2:CreateTags`: para marcar a AMI de destino. Para AMIs baseadas no EBS, ele também concede permissão para marcar os snapshots de apoio da AMI de destino.

Se você estiver copiando uma AMI baseada em uma instância armazenada, as seguintes permissões adicionais do IAM serão necessárias:

- `s3:CreateBucket`: para criar o bucket do S3 na região de destino da nova AMI

- `s3:GetBucketAcl`: para ler as permissões da ACL para o bucket de origem
- `s3:ListAllMyBuckets`: para encontrar um bucket do S3 existente para AMIs na região de destino
- `s3:GetObject`: para ler os objetos no bucket de origem
- `s3:PutObject`: para escrever os objetos no bucket de destino
- `s3:PutObjectAcl`: para escrever as permissões para os novos objetos no bucket de destino

Exemplo de política do IAM para copiar uma AMI baseada em EBS e marcar a AMI e os snapshots de destino

O exemplo de política a seguir concede a você permissão para copiar qualquer AMI baseada no EBS e marcar a AMI de destino e seus snapshots de apoio.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*::image/*"
    }]
}
```

Exemplo de política do IAM para copiar uma AMI baseada no EBS, mas negar a marcação de novos snapshots.

A permissão `ec2:CopySnapshot` é concedida automaticamente quando você recebe a permissão `ec2:CopyImage`. Isso inclui a permissão para marcar os novos snapshots de apoio da AMI de destino. A permissão para marcar os novos snapshots de apoio pode ser negada explicitamente.

O exemplo de política a seguir concede a você permissão para copiar qualquer AMI baseada no EBS, mas proíbe a marcação de novos snapshots de apoio da AMI de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [{
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Exemplo de política do IAM para copiar uma AMI baseada em armazenamento de instância e marcar a AMI de destino

O exemplo de política a seguir concede a você permissão para copiar qualquer AMI baseada em armazenamento de instância no bucket de origem especificado para a região especificada e para marcar a AMI de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
```

```
            "Resource": [
                "arn:aws:s3:::ami-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-account-in-region-hash"
            ]
        }
    ]
}
```

Para localizar o nome do recurso da Amazon (ARN) do bucket de origem da AMI, abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2. No painel de navegação, escolha AMIs e localize o nome do bucket na coluna Source (Origem).

> **Note**
>
> A permissão `s3:CreateBucket` só é necessária na primeira vez que o você copia uma AMI baseada armazenamento de instância para uma região individual. Depois disso, o bucket do Amazon S3 que foi criado na região será usado para armazenar todas as AMIs futuras que você copiar para essa região.

Copiar um AMI

É possível copiar uma AMI usando AWS Management Console, AWS Command Line Interface ou SDKs, ou a API do Amazon EC2, que dão suporte à ação `CopyImage`.

Console

Copiar uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. Pela barra de navegação do console, selecione a região que contém a AMI.
3. No painel de navegação, selecione AMIs para exibir a lista de AMIs disponíveis para você na região.
4. Caso não veja a AMI que deseja copiar, selecione um filtro diferente. É possível filtrar por AMIs Pertencentes a mim, Imagens privadas, Imagens públicas e Imagens desabilitadas.
5. Selecione a AMI para copiar e escolha Ações, Copiar AMI.
6. Na página Copy AMI (Copiar AMI), especifique as seguintes informações:

   a. AMI copy name (Nome da cópia da AMI): o nome da nova AMI. Você pode incluir informações do sistema operacional no nome, pois o Amazon EC2 não fornece essas informações ao exibir detalhes sobre a AMI.

   b. AMI copy description: (Descrição da cópia da AMI): por padrão, a descrição inclui informações sobre a AMI de origem, de forma que você possa distinguir uma cópia da original. É possível alterar essa descrição conforme necessário.

   c. Destination region (Região de destino): a região para a qual a AMI deve ser copiada. Para ter mais informações, consulte Cópia entre regiões.

   d. Copy tags (Copiar tags): marque essa caixa de seleção para incluir as tags de AMI definidas pelo usuário ao copiar a AMI. Tags do sistema (prefixadas com `aws:`) e tags definidas pelo usuário anexadas por outras Contas da AWS não serão copiadas.

   e. (Somente AMIs baseadas no EBS) Criptografar snapshots do EBS de uma cópia da AMI: marque essa caixa de seleção para criptografar os snapshots de destino ou para recriptografá-los usando uma chave diferente. Se a opção de criptografar por padrão estiver habilitada, a caixa de seleção Criptografar snapshots do EBS da cópia da AMI estará marcada e não poderá ser desmarcada. Para ter mais informações, consulte Criptografar e copiar.

   f. (Somente AMIs baseadas no EBS) Chave do KMS: a chave do KMS usada para criptografar os snapshots de destino.

   g. Tags: é possível marcar a nova AMI e os novos snapshots com as mesmas tags ou pode marcá-los com tags diferentes.

      - Para marcar a nova AMI e novos os snapshots com as mesmas tags, escolha Marcar imagem e snapshots juntos. As mesmas tags são aplicadas à nova AMI e a cada snapshot criado.
      - Para marcar a nova AMI e os snapshots com tags diferentes, escolha Marcar imagem e snapshots separadamente. Diferentes tags são aplicadas à nova AMI e aos

snapshots criados. Observe, no entanto, que todos os novos snapshots criados recebem as mesmas tags; não é possível marcar cada snapshot com uma tag diferente.

(Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

h. Quando estiver com tudo pronto para copiar a AMI, escolha Copiar AMI.

O status inicial da nova AMI é `Pending`. A operação de cópia da AMI estará concluída quando o status for `Available`.

AWS CLI

Para copiar uma AMI usando a AWS CLI

É possível copiar uma AMI usando o comando copy-image. Especifique as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `--source-region`. É possível especificar a região de destino usando o parâmetro `--region` ou uma variável de ambiente. Para obter mais informações, consulte Configurar a interface de linha de comando da AWS.

(Somente AMIs baseadas no EBS) Ao criptografar um snapshot de destino durante a cópia, é necessário especificar parâmetros adicionais: `--encrypted` e `--kms-key-id`.

Para ver exemplos de comandos, consulte Examples (Exemplos) em copy-image na AWS CLI Command Reference (Referência de comandos da).

PowerShell

Para copiar uma AMI usando a Tools for Windows PowerShell

É possível copiar uma AMI usando o comando Copy-EC2Image. Especifique as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `-SourceRegion`. É possível especificar a região de destino usando o parâmetro `-Region` ou o comando `Set-AWSDefaultRegion`. Para obter mais informações, consulte Especificação das regiões da AWS.

(Somente AMIs baseadas no EBS) Ao criptografar um snapshot de destino durante a cópia, é necessário especificar parâmetros adicionais: `-Encrypted` e `-KmsKeyId`.

Parar uma operação de cópia de AMI pendente

É possível interromper uma cópia pendente da AMI ao usar o AWS Management Console ou a linha de comando.

Console

Para parar uma operação de cópia de AMI usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região de destino com o seletor de região.
3. No painel de navegação, selecione AMIs.
4. Selecione a AMI cuja cópia será interrompida e escolha Ações e Cancelar registro da AMI.
5. Quando a confirmação for solicitada, escolha Deregister AMI (Cancelar registro da AMI).

Command line

Para parar uma operação de cópia de AMI usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- deregister-image (AWS CLI)
- Unregister-EC2Image (AWS Tools for Windows PowerShell)

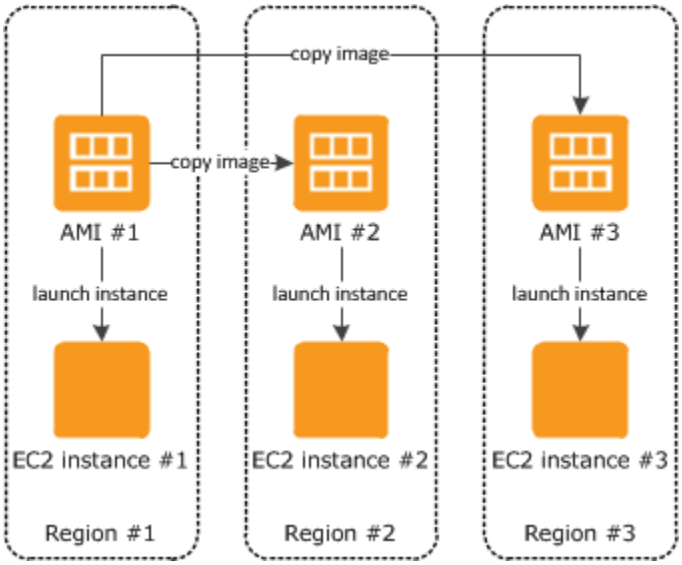
Cópia entre regiões

Copiar uma AMI entre regiões geograficamente diversas traz os seguintes benefícios:

- Implantação global consistente: copiar uma AMI de uma região para outra permite que você execute instâncias consistentes com base na mesma AMI em diferentes regiões.
- Escalabilidade: É possível mais facilmente projetar e construir aplicações globais que atendam às necessidades dos seus usuários, onde quer que estejam.
- Performance: é possível aumentar a performance ao distribuir sua aplicação, além de localizar os componentes essenciais do sua aplicação em maior proximidade de seus usuários. Também é possível aproveitar recursos específicos da região, como tipos de instância ou outros serviços da AWS.

- Alta disponibilidade: é possível projetar e implantar aplicações nas regiões da AWS, de forma a aumentar a disponibilidade.

O diagrama a seguir mostra as relações entre uma AMI de origem e duas AMIs copiadas em regiões diferentes, assim como as instâncias do EC2 executadas por cada uma. Ao executar uma instância a partir de uma AMI, ela residirá na mesma região em que a AMI reside. Se você fizer alterações à AMI de origem e quiser que essas alterações sejam refletidas nas AMIs das regiões de destino, deve recopiar a AMI de origem nas regiões de destino.



Ao copiar pela primeira vez uma AMI com armazenamento de instâncias para uma região, criaremos um bucket do Amazon S3 para as AMIs copiadas para essa região. Todas as AMIs com armazenamento de instâncias que você copiar para essa região serão armazenadas nesse bucket. Os nomes do bucket têm o seguinte formato: amis-for-*account*-in-*region*-*hash*. Por exemplo: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Pré-requisito

Antes de copiar uma AMI, é preciso garantir que o conteúdo da AMI de origem seja atualizado para oferecer suporte à execução em uma região diferente. Por exemplo, atualize todas as string de conexão com o banco de dados ou dados de configuração de aplicação para apontarem para os recursos apropriados. Caso contrário, as instâncias executadas pela nova AMI na região de destino ainda poderão usar os recursos da região de origem, o que pode afetar a performance e o custo.

Limitações

- As regiões de destino estão limitadas a 100 cópias simultâneas de AMI.

- Não é possível copiar uma AMI paravirtual (PV) em uma região que não oferece suporte a AMIs PV. Para ter mais informações, consulte Tipos de virtualização de AMI.

Cópia entre contas

É possível compartilhar uma AMI com outra conta da AWS. O compartilhamento da AMI não afeta propriedade da AMI. A conta proprietária é cobrada pelo armazenamento na região. Para obter mais informações, consulte Compartilhar uma AMI com contas específicas da AWS.

Se você copiar uma AMI que foi compartilhada com sua conta, será o proprietário da AMI de destino na sua conta. Do proprietário da AMI de origem são cobradas taxas de transferência padrão do Amazon EBS ou do Amazon S3, e você será cobrado pelo armazenamento da AMI de destino na região de destino.

Permissões de recursos

Para copiar uma AMI compartilhada com você de outra conta, o proprietário da AMI de origem deve conceder permissão de leitura para o armazenamento que suporta a AMI. O armazenamento é o snapshot do EBS associado (para uma AMI baseada no Amazon EBS) ou um bucket S3 associado (para uma AMI baseada em armazenamento de instância). Se a AMI compartilhada criptografou snapshots, o proprietário deve compartilhar a chave ou as chaves com você também. Para obter mais informações sobre como conceder permissões de recursos para snapshots do EBS, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS. Para buckets do S3, consulte Gerenciamento de identidade e acesso no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Para copiar uma AMI com as tags, você deve ter permissões de inicialização para a AMI de origem.

Criptografar e copiar

A tabela a seguir mostra o suporte a criptografia para vários cenários de cópia de AMI. Apesar de ser possível copiar um snapshot não criptografado para render um snapshot criptografado, você não pode copiar um snapshot criptografado para render um não criptografado.

Cenário	Descrição	Compatível
1	Não criptografado para não criptografado	Sim
2	Criptografado para criptografado	Sim
3	Não criptografado para criptografado	Sim
4	Criptografado para não criptografado	Não

> **Note**
>
> A criptografia durante a ação `CopyImage` se aplica somente a AMIs com Amazon EBS. Como uma AMI com armazenamento de instâncias não depende de snapshots, você não pode usar a cópia para alterar seu status de criptografia.

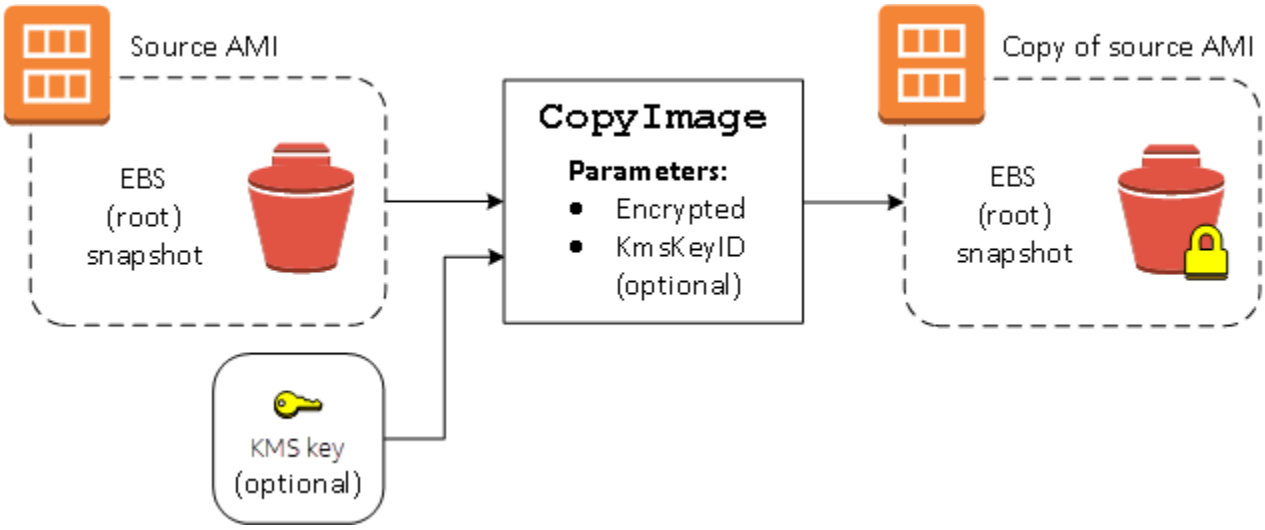
Por padrão (isto é, sem especificar parâmetros de criptografia), o snapshot de suporte de uma AMI é copiado com seu status de criptografia original. Copiar uma AMI baseada em um snapshot não criptografado resulta em um snapshot de destino idêntico que também não é criptografado. Se a AMI de origem for baseada em um snapshot criptografado, copiá-la resultará em um snapshot de destino idêntico que é criptografado pela mesma chave do AWS KMS. Copiar uma AMI com vários snapshots preserva, por padrão, o status de criptografia de origem em cada snapshot de destino.

Se você especificar parâmetros de criptografia enquanto copia uma AMI, poderá criptografar seus snapshots de suporte ou criptografá-los novamente. O exemplo a seguir mostra um caso não padrão que fornece parâmetros de criptografia à ação `CopyImage` para alterar o estado de criptografia da AMI de destino.

Copiar uma AMI de origem não criptografada para uma AMI de destino criptografada

Nesse cenário, uma AMI baseada em um snapshot raiz não criptografado é copiada para uma AMI com um snapshot raiz criptografado. A ação `CopyImage` é invocada com dois parâmetros de criptografia, incluindo uma chave gerenciada pelo cliente. Como resultado, o status de criptografia do snapshot raiz muda, de modo que a AMI de destino tenha suporte de um snapshot raiz contendo os mesmos dados que o snapshot de origem, mas criptografado usando a chave especificada. Você incorre em custos de armazenamento para os snapshots em ambas as AMIs, bem como cobranças para todas as instâncias iniciadas a partir de uma AMI.

> **Note**
>
> Habilitar a criptografia por padrão tem o mesmo efeito que configurar o parâmetro `Encrypted` como `true` para todos os snapshots na AMI.



Configurar o parâmetro `Encrypted` criptografa o snapshot único dessa instância. Se você não especificar o parâmetro `KmsKeyId`, a chave gerenciada pelo cliente padrão será usada para criptografar a cópia do snapshot.

Para obter mais informações sobre como copiar AMIs com snapshots criptografados, consulte Usar criptografia com AMIs com EBS.

Armazenar e restaurar uma AMI usando o S3

É possível armazenar uma imagem de máquina da Amazon (AMI) em um bucket do Amazon S3, copiar a AMI para outro bucket do S3 e restaurá-la a partir do bucket do S3. Ao armazenar e restaurar uma AMI usando buckets do S3, é possível copiar AMIs de uma partição da AWS para outra, por exemplo, da principal partição comercial para a partição AWS GovCloud (US). Também é possível fazer cópias de arquivamento de AMIs armazenando-as em um bucket do S3.

As APIs compatíveis para armazenar e restaurar uma AMI usando o S3 são `CreateStoreImageTaskDescribeStoreImageTasks` e `CreateRestoreImageTask`.

`CopyImage` é a API recomendada para copiar AMIs dentro de uma partição da AWS. No entanto, `CopyImage` não pode copiar uma AMI para outra partição.

Para obter mais informações sobre as partições da AWS, consulte *partição* na página Nomes do recurso da Amazon (ARN) no Guia do usuário do IAM.

> **Warning**
>
> Certifique-se de cumprir todas as leis e requisitos de negócios aplicáveis ao mover dados entre partições daAWS ou regiões da AWS, incluindo, entre outros, quaisquer regulamentos governamentais aplicáveis e requisitos de residência de dados.

Tópicos

- Casos de uso
- Como as APIs de armazenamento e restauração da AMI funcionam
- Limitações
- Custos
- Proteger suas AMIs
- Permissões para armazenar e restaurar AMIs usando o S3
- Trabalhar com o armazenamento da AMI e restaurar APIs
- Usar caminhos de arquivo no S3

Casos de uso

Use as APIs de armazenamento e restauração para fazer o seguinte:

- Copiar uma AMI de uma partição da AWS para outra partição da AWS
- Fazer cópias de arquivamento de AMIs

Copiar uma AMI de uma partição da AWS para outra partição da AWS

Ao armazenar e restaurar uma AMI usando buckets do S3, é possível copiar uma AMI de uma partição da AWS para outra ou de uma região da AWS para outra. No exemplo a seguir, você copia uma AMI da partição comercial principal para a partição AWS GovCloud (US), especificamente da região `us-east-2` para a região `us-gov-east-1`.

Para copiar uma AMI de uma partição para outra, siga estas etapas:

- Armazene a AMI em um bucket do S3 na região atual usando `CreateStoreImageTask`. Neste exemplo, o bucket do S3 está localizado em `us-east-2`. Para obter um exemplo de comando, consulte Armazenar uma AMI em um bucket do S3.
- Monitore o andamento da tarefa de armazenamento usando `DescribeStoreImageTasks`. O objeto fica visível no bucket do S3 quando a tarefa é concluída. Para obter um exemplo de comando, consulte Descrever o andamento de uma tarefa de armazenamento de AMI.
- Copie o objeto da AMI armazenado para um bucket do S3 na partição de destino usando um procedimento de sua escolha. Neste exemplo, o bucket do S3 está localizado em `us-gov-east-1`.

> **Note**
>
> Como você precisa de credenciais diferentes da AWS para cada partição, você não pode copiar um objeto S3 diretamente de uma partição para outra. O processo para copiar um objeto S3 entre partições está fora do escopo desta documentação. Fornecemos os processos de cópia a seguir como exemplos, mas use o processo de cópia que atenda aos seus requisitos de segurança.
>
> - Para copiar uma AMI entre partições, o processo de cópia pode ser tão simples quanto o seguinte: baixe o objeto do bucket de origem para um host intermediário (por exemplo, uma instância do EC2 ou um laptop) e carregue o objeto do host intermediário no bucket de destino. Para cada etapa do processo, use as credenciais da AWS para a partição.
> - Para um uso mais sustentável, considere desenvolver uma aplicação que gerencia as cópias, potencialmente usando downloads e uploads de várias partesdo S3.

- Restaure a AMI do bucket do S3 na partição de destino usando `CreateRestoreImageTask`. Neste exemplo, o bucket do S3 está localizado em `us-gov-east-1`. Para obter um exemplo de comando, consulte Restaurar uma AMI de um bucket do S3.
- Monitore o andamento da tarefa de restauração descrevendo a AMI para verificar quando seu estado se torna disponível. Também é possível monitorar as porcentagens de progresso dos snapshots que compõem a AMI restaurada descrevendo os instantâneos.

Fazer cópias de arquivamento de AMIs

É possível fazer cópias de arquivamento de AMIs armazenando-as em um bucket do S3. Para obter um exemplo de comando, consulte Armazenar uma AMI em um bucket do S3.

A AMI é embalada em um único objeto no S3 e todos os metadados da AMI (excluindo informações de compartilhamento) são preservados como parte da AMI armazenada. Os dados da AMI são compactados como parte do processo de armazenamento. AMIs que contêm dados que podem ser facilmente compactados resultarão em objetos menores no S3. Para reduzir custos, é possível usar camadas de armazenamento S3 mais econômicas. Para obter mais informações, consulte Classes de armazenamento do Amazon S3 e definição de preço do Amazon S3

Como as APIs de armazenamento e restauração da AMI funcionam

Para armazenar e restaurar uma AMI usando o S3, use as seguintes APIs:

- `CreateStoreImageTask` – Armazena a AMI em um bucket do S3
- `DescribeStoreImageTasks` – Fornece o andamento da tarefa de armazenamento da AMI
- `CreateRestoreImageTask` – Restaura a AMI de um bucket do S3

Como as APIs funcionam

- CreateStoreImageTask
- DescriboesToreImageTasks
- CreateRestoreImageTask

CreateStoreImageTask

A API CreateStoreImagetAsk armazena uma AMI como um único objeto em um bucket do S3.

A API cria uma tarefa que lê todos os dados da AMI e seus snapshots e, a seguir, usa um multipart upload do S3 para armazenar os dados em um objeto do S3. A API leva todos os componentes da AMI, incluindo a maioria dos metadados de AMI não específicos da região e todos os snapshots do EBS contidos na AMI, e os empacota em um único objeto no S3. Os dados são compactados como parte do processo de upload para reduzir a quantidade de espaço usado no S3; portanto, o objeto no S3 pode ser menor do que a soma dos tamanhos dos snapshots na AMI.

Se houver tags de AMI e de snapshot visíveis para a conta chamando essa API, elas serão preservadas.

O objeto no S3 tem o mesmo ID que a AMI, mas com uma extensão `.bin`. Os dados a seguir também são armazenados como tags de metadados do S3 no objeto do S3: nome da AMI, descrição

da AMI, data de registro da AMI, conta de proprietário da AMI e um timestamp para a operação de armazenamento.

O tempo necessário para concluir a tarefa depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. É possível acompanhar o andamento da tarefa chamando a API DescribestoreImageTasks.

A soma dos tamanhos de todas as AMIs em andamento é limitada a 600 GB de dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite. Por exemplo, se uma AMI com 100 GB de dados de snapshot e outra AMI com 200 GB de dados de snapshot estiverem sendo armazenadas no momento, outra solicitação será aceita, pois o total em andamento é de 300 GB, que é inferior ao limite. Mas se uma única AMI com 800 GB de dados de snapshot estiver sendo armazenada no momento, outras tarefas serão rejeitadas até que a tarefa seja concluída.

DescriboesToreImageTasks

A API DescribestoreImageTasks descreve o andamento das tarefas de armazenamento da AMI. É possível descrever tarefas para AMIs especificadas. Se você não especificar AMIs, receberá uma lista paginada de todas as tarefas de imagem de armazenamento que foram processadas nos últimos 31 dias.

Para cada tarefa de AMI, a resposta indica se a tarefa é `InProgressCompleted` ou `Failed`. Para tarefas `InProgress`, a resposta mostra um andamento estimado como uma porcentagem.

As tarefas são listadas em ordem cronológica inversa.

No momento, somente as tarefas do mês anterior podem ser visualizadas.

CreateRestoreImageTask

A API CreateRestoreImagetAsk inicia uma tarefa que restaura uma AMI de um objeto do S3 que foi criado anteriormente usando uma solicitação CreateStoreImagetAsk.

A tarefa de restauração pode ser executada na mesma região ou em uma região diferente daquela em que a tarefa de armazenamento foi executada.

O bucket do S3 a partir do qual o objeto da AMI será restaurado deve estar na mesma região em que a tarefa de restauração é solicitada. A AMI será restaurada nessa região.

A AMI é restaurada com seus metadados, como o nome, a descrição e os mapeamentos de dispositivos de blocos correspondentes aos valores da AMI armazenada. O nome deve ser exclusivo

para AMIs na região dessa conta. Se você não fornecer um nome, a nova AMI obterá o mesmo nome da AMI original. A AMI obtém um novo ID de AMI que é gerado no momento do processo de restauração.

O tempo necessário para a conclusão da tarefa de restauração da AMI depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. É possível visualizar o andamento da tarefa descrevendo a AMI (describe-images) ou seus snapshots do EBS (describe-snapshots). Se a tarefa falhar, a AMI e os snapshots serão movidos para um estado com falha.

A soma dos tamanhos de todas as AMIs em andamento é limitada a 300 GB (com base no tamanho após a restauração) dos dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite.

Limitações

- Para armazenar uma AMI, sua Conta da AWS deve possuir a AMI e seus snapshots, ou a AMI e seus snapshots devem ser compartilhados diretamente com sua conta. Você não pode armazenar uma AMI se ela for compartilhada publicamente apenas.
- Somente AMIs baseadas no EBS podem ser armazenadas usando essas APIs.
- Não há suporte a AMIs paravirtuais (PV).
- O tamanho de uma AMI (antes da compactação) que pode ser armazenada é limitado a 5.000 GB.
- Cota em solicitações de imagem de armazenamento : 600 GB de trabalho de armazenamento (dados de snapshots) em andamento.
- Cota em solicitações de imagem de restauração : 300 GB de trabalho de restauração (dados de snapshots) em andamento.
- Durante a tarefa de armazenamento, os snapshots não devem ser excluídos e a entidade principal do IAM que faz o armazenamento deve ter acesso aos snapshots, caso contrário o processo de armazenamento apresentará falha.
- Não é possível criar várias cópias de uma AMI no mesmo bucket do S3.
- Uma AMI armazenada em um bucket do S3 não pode ser restaurada com seu ID de AMI original. É possível mitigar isso usando Alias de AMI.
- Atualmente, as APIs de armazenamento e restauração só são compatíveis se for utilizada a AWS Command Line Interface, os AWS SDKs e a API do Amazon EC2. Não é possível armazenar e restaurar uma AMI usando o console do Amazon EC2.

Custos

Quando você armazena e restaura AMIs usando o S3, é cobrado pelos serviços usados pelas APIs de armazenamento e restauração e pela transferência de dados. As APIs usam o S3 e a API direta do EBS (usadas internamente por essas APIs para acessar os dados do snapshot). Para obter mais informações, consulte Definição de preço do Amazon S3 e Definição de preço do Amazon EBS.

Proteger suas AMIs

Para usar as APIs de armazenamento e restauração, o bucket do S3 e a AMI devem estar na mesma região. É importante garantir que o bucket do S3 esteja configurado com segurança suficiente para proteger o conteúdo da AMI e que a segurança seja mantida enquanto os objetos da AMI permanecerem no bucket. Se isso não puder ser feito, o uso dessas APIs não será recomendado. Não permita acesso público ao bucket do S3. Recomendamos que você ative a Server Side Encryption (Criptografia do lado do servidor) para o bucket do S3 no qual você armazena as AMIs, embora não seja necessário.

Para obter informações sobre como definir as configurações de segurança apropriadas para os buckets do S3, consulte os seguintes tópicos de segurança:

- Bloquear o acesso público ao armazenamento do Amazon S3
- Definir o comportamento padrão da criptografia para os buckets do Amazon S3
- Qual política de bucket do S3 devo usar para seguir a regra s3-bucket-ssl-requests-only do AWS Config?
- Habilitar o log de acesso ao servidor do Amazon S3

Quando os snapshots da AMI são copiados para o objeto S3, os dados são copiados em conexões TLS. É possível armazenar AMIs com snapshots criptografados, mas os snapshots são descriptografados como parte do processo de armazenamento.

Permissões para armazenar e restaurar AMIs usando o S3

Caso as entidades principais do IAM armazenem ou restaurem AMIs usando o Amazon S3, você precisará conceder a elas as permissões necessárias.

A política de exemplo a seguir inclui todas as ações necessárias para permitir que uma entidade principal do IAM execute as tarefas de armazenamento e restauração.

Também é possível criar políticas do IAM que concedam às entidades principais acesso apenas a recursos específicos. Para obter mais exemplos de políticas, consulte Gerenciamento de acesso para recursos da AWS no Guia do usuário do IAM.

> **Note**
>
> Se os snapshots que compõem a AMI estiverem criptografados ou se a conta estiver habilitada para criptografia por padrão, seu principal do IAM deverá ter permissão para usar a chave KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabalhar com o armazenamento da AMI e restaurar APIs

Tópicos

- Armazenar uma AMI em um bucket do S3
- Descrever o andamento de uma tarefa de armazenamento de AMI
- Restaurar uma AMI de um bucket do S3

Armazenar uma AMI em um bucket do S3

Para armazenar uma AMI (AWS CLI)

Use o comando create-store-image-task. Especifique o ID da AMI e o nome do bucket do S3 no qual a AMI será armazenada.

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket my-ami-bucket
```

Saída esperada

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Descrever o andamento de uma tarefa de armazenamento de AMI

Para descrever o andamento de uma tarefa de armazenamento de AMI (AWS CLI)

Use o comando describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks
```

Saída esperada

```
{
    "StoreImageTaskResults": [
        {
            "AmiId": "ami-1234567890abcdef0",
            "Bucket": "my-ami-bucket",
            "ProgressPercentage": 17,
```

```
            "S3objectKey": "ami-1234567890abcdef0.bin",
            "StoreTaskState": "InProgress",
            "StoreTaskFailureReason": null,
            "TaskStartTime": "2022-01-01T01:01:01.001Z"
        }
    ]
}
```

Restaurar uma AMI de um bucket do S3

Para restaurar uma AMI (AWS CLI)

Use o comando create-restore-image-task. Usando os valores de `Bucket` e `S3ObjectKey` da `describe-store-image-tasks` saída, especifique a chave de objeto da AMI e o nome do bucket do S3 para o qual a AMI foi copiada. Especifique também um nome para a AMI restaurada. O nome deve ser exclusivo para AMIs na região dessa conta.

> **Note**
>
> A AMI restaurada obtém um novo ID de AMI.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket my-ami-bucket \
    --name "New AMI Name"
```

Saída esperada

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Usar caminhos de arquivo no S3

É possível usar caminhos de arquivo ao armazenar e restaurar AMIs, da seguinte forma:

- Ao armazenar uma AMI no S3, o caminho do arquivo pode ser adicionado ao nome do bucket. Internamente, o sistema separa o caminho do nome do bucket e, em seguida, adiciona o caminho à chave do objeto que é gerada para armazenar a AMI. O caminho completo do objeto é mostrado na resposta da chamada de API.

- Ao restaurar a AMI, como um parâmetro de chave de objeto está disponível, o caminho pode ser adicionado ao início do valor da chave do objeto.

É possível usar caminhos de arquivo ao usar a AWS CLI e os SDKs.

Exemplo: use um caminho de arquivo ao armazenar e restaurar uma AMI (AWS CLI)

O exemplo a seguir primeiro armazena uma AMI no S3, com o caminho do arquivo anexado ao nome do bucket. O exemplo restaura então a AMI do S3, com o caminho do arquivo anexado ao parâmetro da chave do objeto.

1. Armazene a AMI. Em `--bucket`, especifique o caminho do arquivo após o nome do bucket, da seguinte forma:

   ```
   aws ec2 create-store-image-task \
       --image-id ami-1234567890abcdef0 \
       --bucket my-ami-bucket/path1/path2
   ```

   Saída esperada

   ```
   {
     "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"
   }
   ```

2. Restaure a AMI. Em `--object-key`, especifique o valor da saída na etapa anterior, o que inclui o caminho do arquivo.

   ```
   aws ec2 create-restore-image-task \
       --object-key path1/path2/ami-1234567890abcdef0.bin \
       --bucket my-ami-bucket \
       --name "New AMI Name"
   ```

Descontinuar uma AMI

É possível defasar uma AMI para indicar que ela está desatualizada e não deve ser usada. Também é possível especificar uma data de defasagem futura para uma AMI, indicando quando a AMI estará desatualizada. Por exemplo, é possível defasar uma AMI cuja manutenção não está mais ativa ou pode defasar uma AMI que foi substituída por uma versão mais recente. Por padrão, as AMIs defasadas não aparecem nas listagens de AMI, impedindo que novos usuários usem AMIs

desatualizadas. No entanto, os usuários existentes e os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar usando uma AMI defasada especificando seu ID. Para excluir a AMI, de modo que usuários e serviços não possam usá-la, é necessário cancelar o registro dela.

Depois que uma AMI estiver defasada:

- Para usuários de AMI, a AMI defasada não aparece nas chamadas de API DescribeImages, a menos que você especifique o ID dela ou especifique que AMIs defasadas devem ser exibidas. Os proprietários da AMI continuam a ver AMIs defasadas nas chamadas de API DescribeImages.
- Para usuários de AMI, a AMI defasada não está disponível para seleção no console do EC2. Por exemplo, uma AMI defasada não é exibida no catálogo da AMI no assistente de inicialização de instância. Os proprietários da AMI continuam a ver AMIs defasadas no console do EC2.
- Para os usuários da AMI, se você souber o ID de uma AMI defasada, poderá continuar a iniciar instâncias usando a AMI defasada com a API, a CLI ou os SDKs.
- Os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar referenciando a AMIs defasadas.
- As instâncias do EC2 que foram iniciadas usando uma AMI que posteriormente é defasada não são afetadas e podem ser interrompidas, iniciadas e reinicializadas.

É possível defasar AMIs privadas e públicas.

Também é possível criar políticas de AMI apoiadas pelo EBS Amazon Data Lifecycle Manager para automatizar a defasagem das AMIs apoiadas pelo EBS. Para obter mais informações, consulte Automatizar ciclos de vida da AMI.

> **Note**
>
> Por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos a partir da data de criação da AMI. É possível definir a data de descontinuação para antes de dois anos. Para cancelar a data de descontinuação ou adiá-la para uma data posterior, você deve tornar a AMI privada compartilhando-a somente com contas específicas da AWS.

Tópicos

- Custos
- Limitações

- Descontinuar uma AMI
- Descrever AMIs defasadas
- Cancelar a defasagem de uma AMI

Custos

Quando você defasar uma AMI, a AMI não será excluída. O proprietário da AMI continuará pagando pelos snapshots da AMI. Para parar de pagar pelos instantâneos, o proprietário da AMI deve excluir a AMI cancelando o registro dela.

Limitações

- Para defasar uma AMI, é necessário ser o proprietário da AMI.

Descontinuar uma AMI

É possível defasar uma AMI em uma data e hora específicas. É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Para descontinuar uma AMI em uma data específica

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Actions (Ações), Manage AMI Deprecation (Gerenciar descontinuação da AMI). É possível selecionar várias AMIs para definir a mesma data de descontinuação de várias AMIs de uma só vez.
5. Selecione a caixa de seleção Enable (Habilitar) e, em seguida, insira a data e a hora de descontinuação.

   O limite superior para a data de descontinuação é daqui a 10 anos, exceto para AMIs públicas, em que o limite superior é de 2 anos após a data de criação. Você não pode especificar uma data no passado.
6. Escolha Salvar.

AWS CLI

Para descontinuar uma AMI em uma data específica

Usar o comando disable-image-deprecation. Especifique o ID da AMI e a data e hora nas quais a AMI será defasada. Se você especificar um valor para segundos, o Amazon EC2 arredondará os segundos para o minuto mais próximo.

O limite superior para `deprecate-at` é daqui a 10 anos, exceto para AMIs públicas, em que o limite superior é de 2 anos após a data de criação. Você não pode especificar uma data no passado.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

Saída esperada

```
{
  "Return": "true"
}
```

Verificar quando uma AMI foi usada pela última vez

`LastLaunchedTime` é um carimbo de data/hora que indica quando sua AMI foi usada pela última vez para iniciar uma instância. AMIs que não tenham sido usadas recentemente para iniciar uma instância podem ser boas candidatas para descontinuação ou cancelamento de registro.

> **Note**
>
> - Quando uma AMI é usada para iniciar uma instância, há um atraso de 24 horas antes que o uso seja incluído em relatórios.
> - Os dados de `lastLaunchedTime` estão disponíveis a partir de abril de 2017.

Console

Como visualizar a última hora de início de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e marque o campo Deprecation time (Hora da descontinuação). Se você marcou a caixa de seleção ao lado da AMI, ele estará localizado na guia Details (Detalhes). O campo mostra a data e a hora em que a AMI foi usada pela última vez para iniciar uma instância.

AWS CLI

Como visualizar a última hora de início de uma AMI

Execute o comando describe-image-attribute e especifique `--attribute lastLaunchedTime`. É necessário ser o proprietário da AMI para executar esse comando.

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

Exemplo de saída

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

Descrever AMIs defasadas

É possível visualizar a data e a hora de descontinuação de uma AMI e filtrar todas as AMIs por data de descontinuação. Também é possível usar a AWS CLI para descrever todas as AMIs que foram descontinuadas, em que a data da descontinuação já passou.

Console

Para visualizar a data de descontinuação de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador, escolha AMIs e, em seguida, selecione a AMI.
3. Selecione o campo Deprecation time (Hora da descontinuação) (se você marcou a caixa de seleção ao lado da AMI, ele estará localizado na guia Details (Detalhes)). O campo mostra a data e a hora de descontinuação da AMI. Se o campo estiver vazio, a AMI não estará descontinuada.

Para filtrar AMIs por data de descontinuação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário) ou Private images (Imagens privadas) (as imagens privadas incluem AMIs compartilhadas com você e de sua propriedade).
4. Na Search bar (Barra de pesquisa), insira **`Deprecation time`** (à medida que você insere as letras, o filtro Deprecation time (Hora da descontinuação) aparece) e, em seguida, escolha um operador e uma data e hora.

AWS CLI

Quando você descreve todas as AMIs usando o comando describe-images, os resultados são diferentes, dependendo se você é usuário da AMI ou proprietário da AMI.

- Se você for um usuário da AMI:

  Por padrão, quando você descreve todas as AMIs usando o comando describe-images, as AMIs defasadas das quais você não é proprietário, mas que são compartilhadas com você, não são exibidas nos resultados. Isso acontece porque o padrão é `--no-include-deprecated`. Para incluir AMIs defasadas nos resultados, é necessário especificar o parâmetro `--include-deprecated`.

- Se você for o proprietário da AMI:

Quando você descreve todas as AMIs usando o comando describe-images, todas as AMIs das quais você é proprietário, inclusive AMIs defasadas, são exibidas nos resultados. Não é necessário especificar o parâmetro `--include-deprecated`. Além disso, não é possível excluir AMIs defasadas que você possui dos resultados usando `--no-include-deprecated`.

Se uma AMI estiver defasada, o campo `DeprecationTime` é exibido nos resultados.

> **Note**
>
> Uma AMI defasada é uma AMI cuja data de defasagem já passou. Se você tiver definido a data de defasagem como uma data futura, a AMI ainda não está defasada.

Para incluir todas as AMIs descontinuadas ao descrever todas as AMIs

Use o comando describe-images e especifique o parâmetro `--include-deprecated` para incluir nos resultados todas as AMIs defasadas das quais você não é proprietários.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

Para descrever a data de descontinuação de uma AMI

Use o comando describe-images e especifique o ID da AMI.

Se você especificar `--no-include-deprecated` com o ID da AMI, os resultados retornarão a AMI defasada.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Saída esperada

O campo `DeprecationTime` exibe a data definida para a defasagem da AMI. Se não houver data para a defasagem da AMI não estiver definida, o campo `DeprecationTime` não será exibido na saída.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Cancelar a defasagem de uma AMI

É possível cancelar a descontinuação de uma AMI, o que remove a data e a hora do campo Deprecation time (Hora da descontinuação) (console) ou o campo `DeprecationTime` da saída describe-images (AWS CLI). É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Para cancelar a descontinuação de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Actions (Ações), Manage AMI Deprecation (Gerenciar descontinuação da AMI). É possível selecionar várias AMIs para cancelar a descontinuação de várias AMIs de uma só vez.
5. Desmarque a caixa de seleção Enable (Habilitar) e escolha Save (Salvar).

AWS CLI

Para cancelar a descontinuação de uma AMI

Use o comando disable-image-deprecation e especifique o ID da AMI.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Saída esperada

```
{
  "Return": "true"
}
```

Desabilitar uma AMI

Você pode desabilitar uma AMI para evitar que ela seja usada em execuções de instâncias. Não é possível executar novas instâncias por meio de uma AMI desabilitada. Você pode reabilitar uma AMI desabilitada para que ela possa ser usada novamente em execuções de instâncias.

> **Warning**
>
> Ao desabilitar uma AMI, todas as permissões de execução são removidas.

Quando uma AMI é desabilitada:

- O estado da AMI muda para `disabled`.
- Uma AMI desabilitada não pode ser compartilhada. Se uma AMI era pública ou compartilhada, ela se tornará privada. Se uma AMI era compartilhada com uma Conta da AWS, organização ou unidade organizacional, elas perderão o acesso à AMI desabilitada.
- Por padrão, uma AMI desabilitada não é exibida nas chamadas da API DescribeImages.
- Uma AMI desabilitada não é exibida no filtro De minha propriedade do console. Para encontrar AMIs desabilitadas, use o filtro Imagens desabilitadas do console.
- Não é possível selecionar uma AMI desabilitada para execuções de instâncias no console do EC2. Por exemplo, uma AMI desabilitada não é exibida no catálogo de AMIs do assistente de execução da instância nem ao criar um modelo de execução.
- Os serviços de execução, como modelos de execução e grupos do Auto Scaling, podem continuar fazendo referência a AMIs desabilitadas. As execuções subsequentes de instâncias com base em uma AMI desabilitada vão falhar. Por isso, recomendamos atualizar os modelos de execução e os grupos do Auto Scaling para fazer referência somente às AMIs disponíveis.
- As instâncias do EC2 que eram executadas usando uma AMI que mais tarde foi desabilitada não serão afetadas e poderão ser interrompidas, iniciadas e reinicializadas.
- Não é possível excluir snapshots associados a AMIs desabilitadas. Tentar excluir um snapshot associado resulta no erro `snapshot is currently in use`.

Quando uma AMI é reabilitada:

- O estado da AMI muda para `available`, e ela pode ser usada para executar instâncias.
- A AMI pode ser compartilhada.

- Contas da AWS, organizações e unidades organizacionais que perderam o acesso à AMI quando ela foi desabilitada não recuperam o acesso automaticamente, mas a AMI pode ser compartilhada com elas de novo.

É possível desabilitar AMIs privadas e públicas.

Tópicos

- Custos
- Pré-requisitos
- Permissões obrigatórias do IAM
- Desabilitar uma AMI
- Descrever AMIs desabilitadas
- Reabilitar uma AMI desabilitada

Custos

Quando você desabilita uma AMI, ela não é excluída. Se a AMI for uma AMI baseada no EBS, você continua pagando pelos snapshots do EBS da AMI. Se você quiser manter a AMI, talvez consiga reduzir os custos de armazenamento arquivando os snapshots. Para obter mais informações, consulte Arquivar snapshots do Amazon EBS no Guia do usuário do Amazon EC2. Se não quiser manter a AMI e seus snapshots, é preciso cancelar o registro da AMI e excluir os snapshots. Para ter mais informações, consulte Excluir recursos associados à sua AMI baseada no Amazon EBS.

Pré-requisitos

Para desabilitar ou reabilitar uma AMI, é preciso ser o proprietário da AMI.

Permissões obrigatórias do IAM

Para desabilitar e reabilitar uma AMI, é necessário ter as seguintes permissões do IAM:

- `ec2:DisableImage`
- `ec2:EnableImage`

Desabilitar uma AMI

Você pode desabilitar uma AMI usando o console do EC2 ou a AWS Command Line Interface (AWS CLI). É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Desabilitar uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Ações, Desativar a AMI. É possível selecionar várias AMIs para serem desabilitadas de uma vez.
5. Na janela Desativar AMI, escolha Desativar AMI.

AWS CLI

Desabilitar uma AMI

Use o comando disable-image e especifique o ID da AMI.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Saída esperada

```
{
  "Return": "true"
}
```

Descrever AMIs desabilitadas

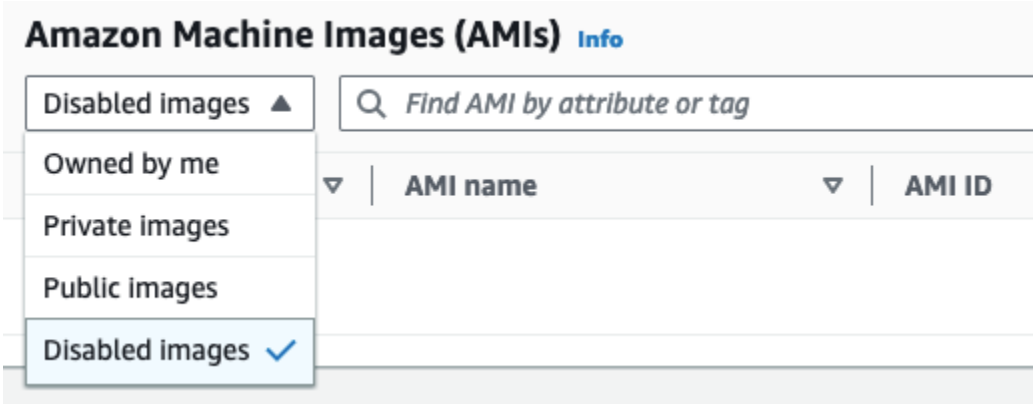
É possível visualizar as AMIs desabilitadas no console do EC2 usando a AWS CLI.

Você precisa ser o proprietário da AMI para ver as AMIs desabilitadas. Como as AMIs desabilitadas se tornam privadas, você não poderá ver as AMIs desabilitadas se não for o proprietário.

Console

Visualizar AMIs desabilitadas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtro, escolha Imagens desabilitadas.



AWS CLI

Por padrão, quando você usa o comando describe-images para descrever todas as AMIs, as AMIs desabilitadas não aparecem nos resultados. Isso acontece porque o padrão é `--no-include-disabled`. Para incluir as AMIs desabilitadas nos resultados, é necessário especificar o parâmetro `--include-disabled`.

Incluir todas as AMIs desabilitadas ao descrever todas as AMIs

Use o comando describe-images e especifique o parâmetro `--include-disabled` para recuperar as AMIs desabilitadas, além de todas as outras AMIs. Também é possível especificar `--owners self` para recuperar somente as AMIs das quais você é proprietário.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners self
    --include-disabled
```

Se você especificar o ID de uma AMI desabilitada, mas não especificar `--include-disabled`, a AMI desabilitada será retornada nos resultados.

```
aws ec2 describe-images \
```

```
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Recuperar somente AMIs desabilitadas

Especifique `--filters Name=state,Values=disabled`. Você também deve especificar `--include-disabled`. Caso contrário, receberá um erro.

```
aws ec2 describe-images \
    --include-disabled \
    --filters Name=state,Values=disabled
```

Exemplo de saída

O campo `State` exibe o estado de uma AMI. `disabled` indica que a AMI está desabilitada.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "disabled",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2023-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
```

```
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": false,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Reabilitar uma AMI desabilitada

Você pode reabilitar uma AMI desabilitada. É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Reabilitar uma AMI desabilitada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtro, escolha Imagens desabilitadas.
4. Selecione a AMI e escolha Ações, Habilitar a AMI. É possível selecionar várias AMIs para reabilitá-las ao mesmo tempo.
5. Na janela Habilitar AMI, escolha Habilitar.

AWS CLI

Reabilitar uma AMI desabilitada

Use o comando enable-image e especifique o ID da AMI.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Saída esperada

```
{
  "Return": "true"
}
```

Arquivar snapshots da AMI

É possível arquivar os snapshots associados às suas AMIs desabilitadas baseadas no EBS. Isso pode ajudar você a reduzir os custos de armazenamento associados às AMIs raramente usadas, que precisam ser retidas por períodos longos. Para obter mais informações, consulte Arquivar snapshots do Amazon EBS no Guia do usuário do Amazon EC2.

Arquivar snapshots associados a uma AMI

1. Desabilite a AMI.
2. Arquive os snapshots.

Você não poderá usar uma AMI enquanto ela estiver desabilitada e os snapshots associados a ela, arquivados.

Restaurar uma AMI desabilitada com snapshots arquivados para uso

1. Restaure os snapshots arquivados associados à AMI.
2. Habilite a AMI.

Cancelar o registro de uma AMI (excluir a AMI)

Quando você cancela o registro de uma AMI, o Amazon EC2 a exclui permanentemente. Após o cancelamento do registro, não será possível usar a AMI para iniciar novas instâncias. Considere cancelar o registro de uma AMI quando não pretender mais usá-la.

Para se proteger contra o cancelamento acidental ou mal-intencionado de uma AMI, é possível ativar a proteção contra cancelamento de registro. Se você cancelar acidentalmente o registro de uma AMI baseada no EBS, poderá usar a Lixeira para restaurá-la somente se o fizer dentro do período de tempo permitido antes que ela seja excluída permanentemente.

O cancelamento do registro de uma AMI não afetará nenhuma instância que já tenha sido iniciada pela AMI. Essas instâncias poderão continuar sendo usadas. O cancelamento do registro de

uma AMI também não afeta os snapshots criados durante o processo de criação da AMI. Você continuará incorrendo em custos de uso para essas instâncias e em custos de armazenamento para os snapshots. Assim, para evitar incorrer em custos extras, recomendamos encerrar quaisquer instâncias e excluir quaisquer snapshots desnecessários. Para ter mais informações, consulte Evite custos com recursos não utilizados.

Conteúdo

- Considerações
- Cancelar o registro de uma AMI
- Verificar quando uma AMI foi usada pela última vez
- Proteger uma AMI contra o cancelamento do registro
- Evite custos com recursos não utilizados

Considerações

- Você não pode cancelar o registro de uma AMI que não pertença à sua conta.
- Você não pode cancelar o registro de uma AMI gerenciada pelo serviço AWS Backup usando o Amazon EC2. Em vez disso, use o AWS Backup para excluir os pontos de recuperação correspondentes no cofre de backup. Para obter mais informações, consulte Exclusão de namespaces no Guia do desenvolvedor do AWS Backup.

Cancelar o registro de uma AMI

Use um dos métodos a seguir para cancelar o registro de uma AMI baseada no EBS ou AMI baseada em armazenamento de instância.

> **Tip**
>
> Quando o processo de desabilitar recursos da aplicação de uma AMI, isso não afetará nenhuma instância que você já tenha executado. Por exemplo, para AMIs baseadas no EBS, se os snapshots associados à AMI cancelada não forem mais necessários, exclua-os. Para ter mais informações, consulte Evite custos com recursos não utilizados.

Console

Para cancelar o registro de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI para cancelar o registro.
5. Escolha Actions (Ações) e Deregister AMI (Cancelar registro da AMI).
6. Quando a confirmação for solicitada, escolha Cancelar registro da AMI.

   A remoção da AMI da lista pelo console pode demorar alguns minutos. Escolha Refresh (Atualizar) para atualizar o status.

AWS CLI

Para cancelar o registro de uma AMI

Use o comando deregister-image e especifique o ID da AMI cujo registro será cancelado.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

Powershell

Para cancelar o registro de uma AMI

Use o cmdlet Unregister-EC2Image e especifique o ID da AMI cujo registro será cancelado.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Verificar quando uma AMI foi usada pela última vez

`LastLaunchedTime` é um carimbo de data/hora que indica quando sua AMI foi usada pela última vez para iniciar uma instância. AMIs que não tenham sido usadas recentemente para iniciar uma instância podem ser boas candidatas para cancelamento de registro ou descontinuação.

> **Note**
>
> - Quando a AMI é usada para iniciar uma instância, há um atraso de 24 horas antes que o uso seja incluído em relatórios.
> - Os dados de `lastLaunchedTime` estão disponíveis a partir de abril de 2017.

Console

Como visualizar a última hora de início de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e marque o campo Deprecation time (Hora da descontinuação). Se você marcou a caixa de seleção ao lado da AMI, ele estará localizado na guia Details (Detalhes). O campo mostra a data e a hora em que a AMI foi usada pela última vez para iniciar uma instância.

AWS CLI

É possível usar o comando describe-images ou describe-image-attribute para ver a hora da última inicialização de uma AMI.

Para visualizar a hora em que uma AMI foi iniciada pela última vez usando describe-images

Use o comando describe-images e especifique o ID da AMI.

```
aws ec2 describe-images --image-id ami-0123456789example
```

Exemplo de saída

> **Note**
>
> O campo `LastLaunchedTime` só aparece na saída das AMIs pertencentes a você.

```
{
```

```
    "Images": [
       {
           ...
           "LastLaunchedTime": {
               "Value": "2024-04-02T02:03:18Z"
           },
           ...
       }
   ]
}
```

Como visualizar a última hora de início de uma AMI

Execute o comando describe-image-attribute e especifique `--attribute lastLaunchedTime`. É necessário ser o proprietário da AMI para executar este comando.

```
aws ec2 describe-image-attribute \
    --image-id ami-0123456789example \
    --attribute lastLaunchedTime
```

Exemplo de saída

```
{
    "ImageId": "ami-1234567890example",
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    }
}
```

Proteger uma AMI contra o cancelamento do registro

É possível ativar a proteção contra cancelamento de registro em uma AMI para evitar exclusão acidental ou mal-intencionada. Quando a proteção contra cancelamento do registro estiver ativada, o registro da AMI não poderá ser cancelado por nenhum usuário, independente das permissões do IAM de cada um. Para cancelar o registro da AMI, desative primeiro a proteção contra cancelamento de registro na AMI.

Ao ativar a proteção contra cancelamento de registro em uma AMI, você terá a opção de incluir um período de espera de 24 horas. Esse período de espera é o tempo durante o qual a proteção contra cancelamento de registro permanece em vigor após você desativá-la. Durante esse período

de espera, o registro da AMI não poderá ser cancelado. Quando o período de espera terminar, o registro da AMI poderá ser cancelado.

A proteção contra cancelamento de registro é desativada por padrão em todas as AMI novas e existentes.

Ativar a proteção contra cancelamento do registro

Use qualquer um dos métodos a seguir para ativar a proteção contra cancelamento de registro em uma AMI. Para fazer isso, você deve ser o proprietário da AMI.

Console

Para ativar a proteção contra cancelamento do registro em uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI na qual você deseja ativar a proteção contra cancelamento de registro e, em seguida, escolha Ações, Gerenciar proteção contra cancelamento de registro da AMI.
5. Na caixa de diálogo Gerenciar proteção contra cancelamento de registro da AMI, é possível ativar a proteção contra cancelamento de registro com ou sem um período de espera. Escolha uma das seguintes opções:
   - Habilitar com período de espera de 24 horas: com um período de espera, o registro da AMI não poderá ser cancelado por 24 horas quando a proteção de cancelamento de registro estiver desativada.
   - Habilitar sem período de espera: sem um período de espera, o registro da AMI poderá ser cancelado imediatamente quando a proteção contra cancelamento de registro estiver desativada.
6. Escolha Salvar.

AWS CLI

Para ativar a proteção contra cancelamento do registro em uma AMI

Use o comando enable-image-deregistration-protection e especifique o ID da AMI. Para incluir o período de espera opcional de 24 horas, inclua `--with-cooldown` definido como `true`. Para excluir o período de espera, omita o parâmetro `--with-cooldown`.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0123456789example \
    --with-cooldown true
```

Desativar a proteção contra cancelamento do registro

Use qualquer um dos métodos a seguir para desativar a proteção contra cancelamento de registro em uma AMI. Para fazer isso, você deve ser o proprietário da AMI.

> **Note**
>
> Se você optou por incluir um período de espera de 24 horas ao ativar a proteção contra cancelamento de registro para a AMI, quando a proteção contra cancelamento de registro for desativada, o registro da AMI não poderá ser cancelado imediatamente. Esse período de espera é o período de 24 horas durante o qual a proteção contra cancelamento de registro permanece em vigor após você desativá-la. Durante esse período de espera, o registro da AMI não poderá ser cancelado. Quando o período de espera terminar, o registro da AMI poderá ser cancelado.

Console

Para desativar a proteção contra cancelamento do registro em uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI na qual você deseja desativar a proteção contra cancelamento de registro e, em seguida, escolha Ações, Gerenciar proteção contra cancelamento de registro da AMI.
5. Na caixa de diálogo Gerenciar proteção contra cancelamento de registro da AMI, escolha Desabilitar.
6. Escolha Salvar.

AWS CLI

Para desativar a proteção contra cancelamento do registro em uma AMI

Use o comando disable-image-deregistration-protection e especifique o ID da AMI.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Evite custos com recursos não utilizados

Ao cancelar o registro de uma AMI, você não exclui os recursos associados a ela. Esses recursos incluem os snapshots para AMIs baseadas no EBS e os arquivos no Amazon S3 para AMIs baseadas em armazenamento de instâncias. Quando o registro de uma AMI for cancelado, isso não encerrará nem interromperá nenhuma instância já iniciada via AMI.

Você continuará incorrendo em custos para armazenar os snapshots e os arquivos, e incorrerá em custos para qualquer instância em execução. Para ter mais informações, consulte Como você é cobrado.

Para evitar incorrer nestes tipos de custos extras, recomendamos excluir quaisquer recursos desnecessários.

Para determinar se a AMI é baseada no EBS ou baseada em armazenamento de instância, consulte Determinar o tipo de dispositivo raiz da AMI.

Excluir recursos associados à sua AMI baseada no Amazon EBS

Use qualquer um dos métodos a seguir para excluir os recursos associados à sua AMI baseada no EMS.

Console

Para excluir recursos associados à sua AMI baseada no EBS

1. Cancelar o registro da AMI

   Anote o ID da AMI. Isso pode ajudar a encontrar os snapshots a serem excluídos na próxima etapa.
2. Exclua os snapshots desnecessários.

O ID da AMI associada é exibido na coluna Descrição na tela Snapshots.

3. Encerre instâncias desnecessárias.

AWS CLI

Para excluir recursos associados à sua AMI baseada no EBS

1. Cancele o registro da AMI usando o comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Exclua os snapshots desnecessários usando o comando delete-snapshot.

```
aws ec2 delete-snapshot --snapshot-id snap-0123456789example
```

3. Encerre as instâncias desnecessárias usando o comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

Para excluir recursos associados à sua AMI baseada no EBS

1. Cancele o registro da AMI usando o cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

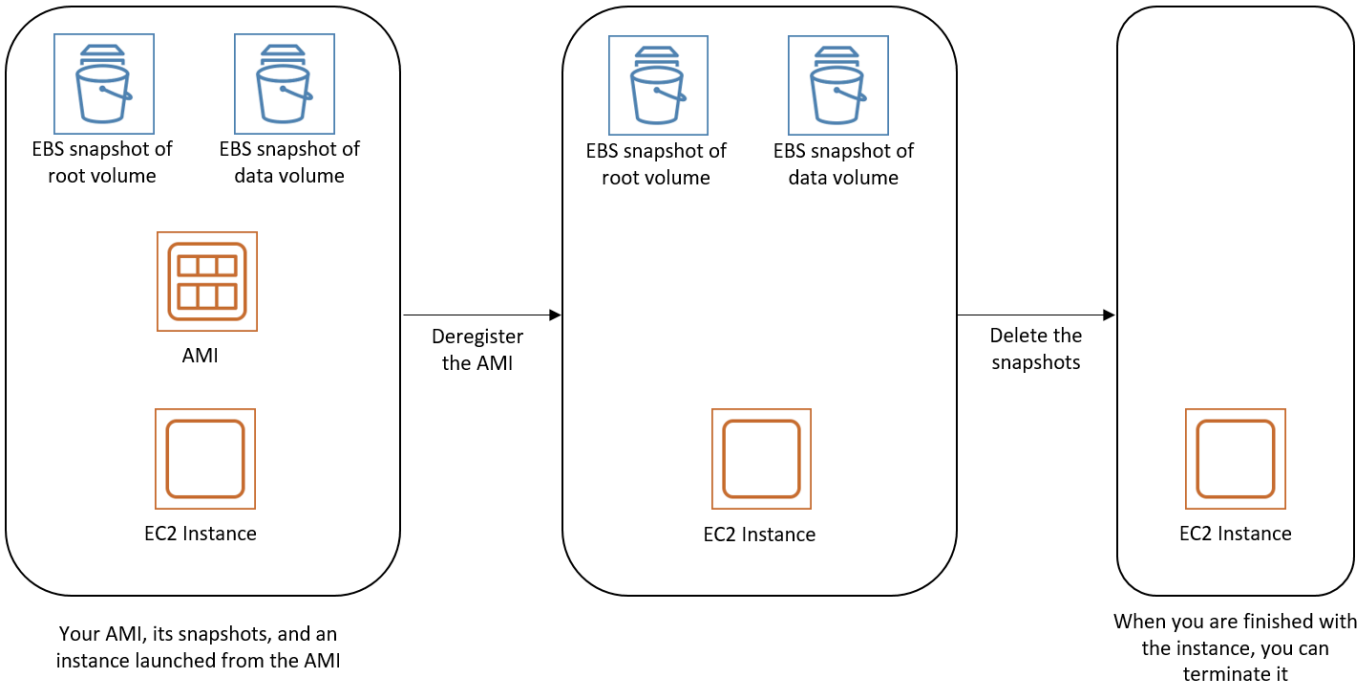
2. Exclua os snapshots desnecessários usando o cmdlet Remove-EC2Snapshot.

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Encerre as instâncias desnecessárias usando o cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-0123456789example
```

O diagrama a seguir ilustra o fluxo para excluir recursos associados a uma AMI baseada no EBS.



Excluir recursos associados à sua AMI baseada em armazenamento de instâncias

Use o método a seguir para excluir os recursos associados à sua AMI baseada em armazenamento de instâncias.

Para excluir recursos associados à sua AMI baseada em armazenamento de instâncias

1. Cancele o registro da AMI usando o comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Exclua o pacote no Amazon S3 usando o comando ec2-delete-bundle (ferramentas de AMI).

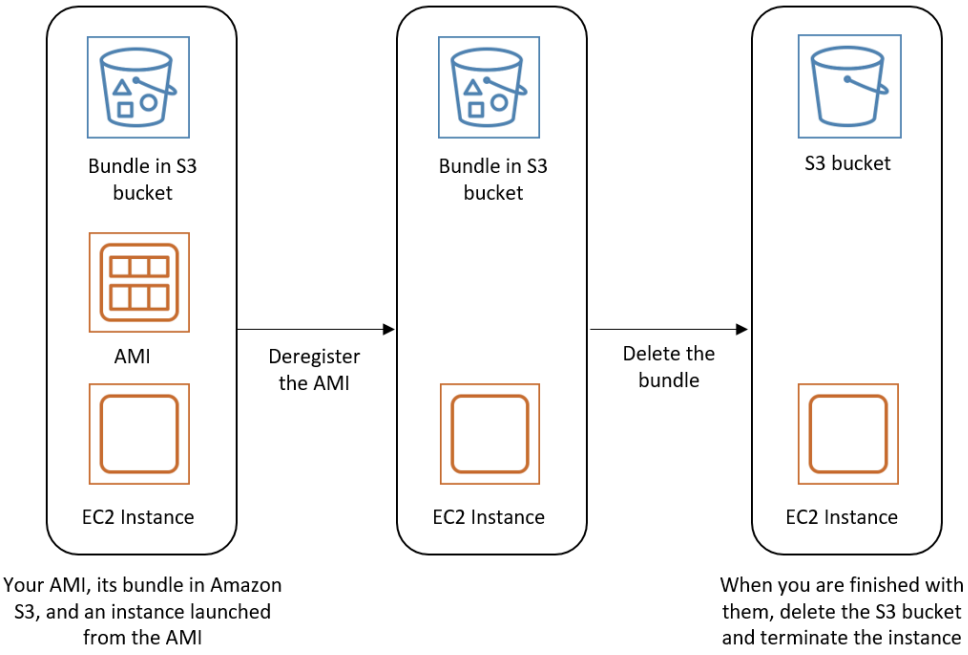
```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -
s your_secret_access_key -p image
```

3. Encerre as instâncias desnecessárias usando o comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Se você tiver terminado de usar o bucket do Amazon S3 no qual carregou o pacote, poderá excluí-lo. Para excluir um bucket do Amazon S3, abra o console do Amazon S3, selecione o bucket, escolha Actions (Ações) e selecione Delete (Excluir).

O diagrama a seguir ilustra o fluxo necessário para excluir recursos associados à sua AMI baseada em armazenamento de instâncias.



Automatizar o ciclo de vida da AMI com suporte do EBS

É possível usar Amazon Data Lifecycle Manager para automatizar a criação, a retenção, a cópia, a defasagem e a exclusão de AMIs baseadas no Amazon EBS e seus snapshots de backup. Para obter mais informações, consulte Amazon Data Lifecycle Manager.

Usar criptografia com AMIs com EBS

As AMIs com snapshots do Amazon EBS podem se beneficiar da criptografia do Amazon EBS. Os snapshots de volumes raiz e de dados podem ser criptografados e anexados a uma AMI. É possível executar instâncias e copiar imagens com suporte total à criptografia do EBS. Os parâmetros de criptografia para essas operações são compatíveis em todas as regiões em que o AWS KMS está disponível.

As instâncias do EC2 com volumes do EBS criptografados são executadas em AMIs da mesma forma que outras instâncias. Além disso, ao executar uma instância a partir de uma AMI baseada em snapshots não criptografados do EBS, será possível criptografar alguns ou todos os volumes durante a execução.

Como os volumes do EBS, os snapshots em AMIs podem ser criptografados pelo padrão do AWS KMS key ou por um chave gerenciada pelo cliente que você especificar. Em todos os casos, é necessário ter permissão para usar a Chave do KMS selecionada.

As AMIs com snapshots criptografados podem ser compartilhadas em todas as contas da AWS. Para obter mais informações, consulte AMIs compartilhadas.

Tópicos de criptografia em AMIs com EBS

- Cenários de execução de instância
- Cenários de cópia de imagem

Cenários de execução de instância

As instâncias do Amazon EC2 são iniciadas nas AMIs usando a ação `RunInstances` com parâmetros fornecidos pelo mapeamento de dispositivos de blocos, seja por meio do AWS Management Console ou diretamente usando a CLI ou a API do Amazon EC2. Para ter mais informações, consulte Mapeamentos de dispositivos de blocos. Para exemplos de mapeamento de dispositivos de blocos da AWS CLI, consulte Executar, listar e encerrar instâncias do EC2.

Por padrão, sem parâmetros de criptografia explícitos, uma ação `RunInstances` mantém o estado de criptografia existente dos snapshots de origem de uma AMI enquanto restaura os volumes do EBS a partir deles. Se a opção de criptografar por padrão estiver habilitada, todos os volumes criados com base na AMI (seja de snapshots criptografados ou não criptografados) serão criptografados. Se a opção de criptografar por padrão não estiver habilitada, a instância manterá o estado de criptografia da AMI.

Também é possível executar uma instância e aplicar simultaneamente um estado de criptografia aos volumes resultantes fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Executar sem parâmetros de criptografia

- Um snapshot não criptografado é restaurado para um volume não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os volumes recém-criados serão criptografados.
- Um snapshot criptografado que você possui é restaurado para um volume que é criptografado para a mesma Chave do KMS.

- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS.

Os comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

A instância executa comportamentos com **`Encrypted`** definido, mas sem **`KmsKeyId`** especificado

- Um snapshot não criptografado é restaurado em um volume do EBS que é criptografado pela chave do KMS padrão da sua conta da AWS.
- Um snapshot criptografado que você possui é restaurado para um volume do EBS criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)

A configuração dos parâmetros `Encrypted` e `KmsKeyId` permite especificar uma Chave do KMS não padrão para uma operação de criptografia. Os seguintes comportamentos resultam em:

A instância com **`Encrypted`** e **`KmsKeyId`** definidos

- Um snapshot não criptografado é restaurado para um volume do EBS criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é restaurado para um volume do EBS criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

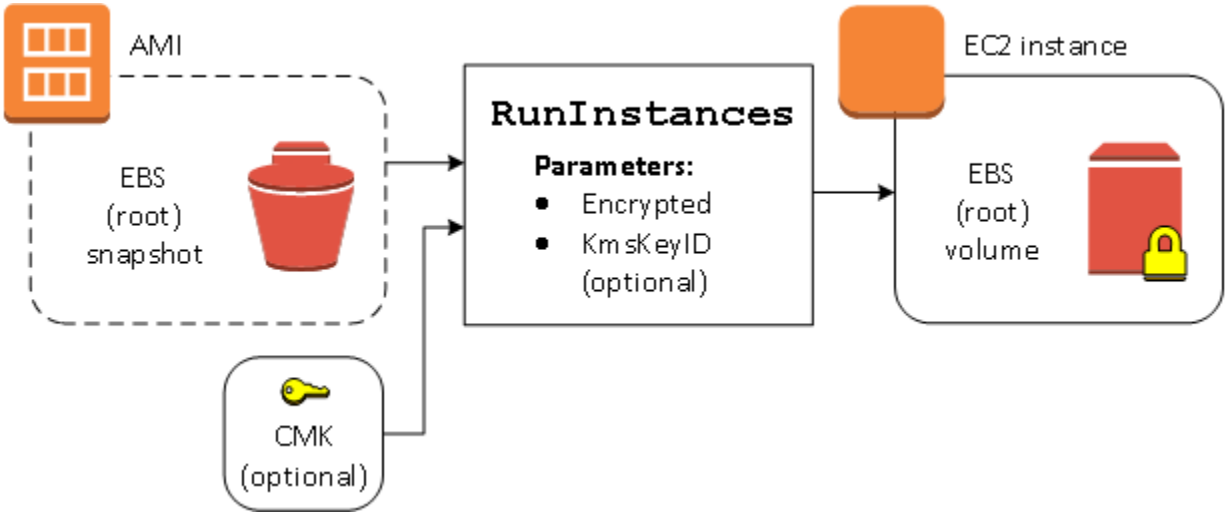
Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

As seções a seguir fornecem exemplos da execução de instâncias de AMIs usando parâmetros de criptografia não padrão. Em cada um desses cenários, os parâmetros fornecidos à ação `RunInstances` resultam em uma alteração do estado de criptografia durante a restauração de um volume a partir de um snapshot.

Para obter informações sobre como usar o console para executar uma instância a partir de uma AMI, consulte Executar sua instância.

Criptografar um volume durante a execução

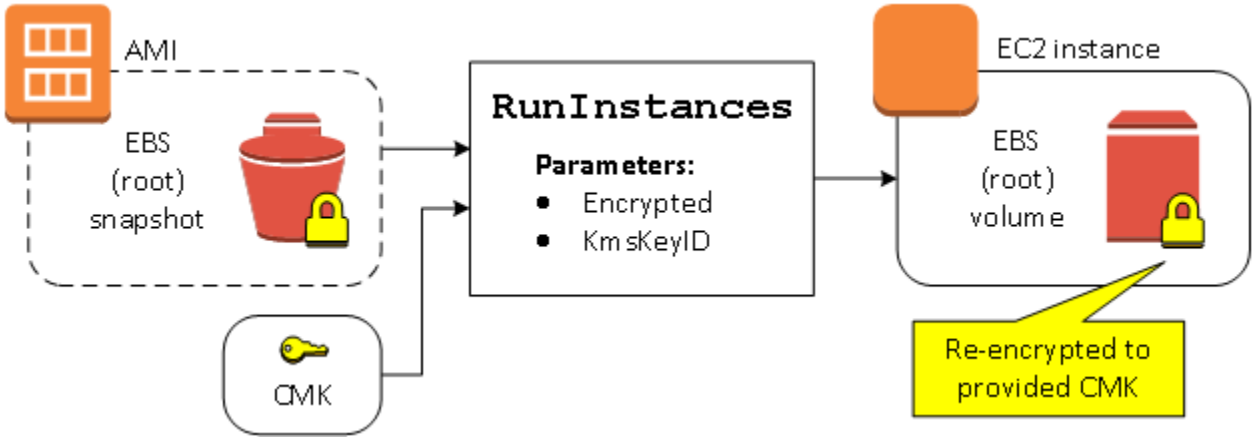
Neste exemplo, uma AMI baseada em um snapshot não criptografado é usada para executar uma instância do EC2 com um volume não criptografado do EBS.



Somente o parâmetro `Encrypted` resulta no volume que será criptografado para essa instância. É opcional fornecer um parâmetro `KmsKeyId`. Se nenhum ID de Chave do KMS for especificado, a Chave do KMS padrão da conta da AWS será usada para criptografar o volume. Para criptografar o volume em uma Chave do KMS diferente que pertença a você, forneça o parâmetro `KmsKeyId`.

Criptografar novamente um volume durante a execução

Neste exemplo, uma AMI baseada em um snapshot criptografado é usada para executar uma instância do EC2 com um volume do EBS criptografado por uma nova Chave do KMS.

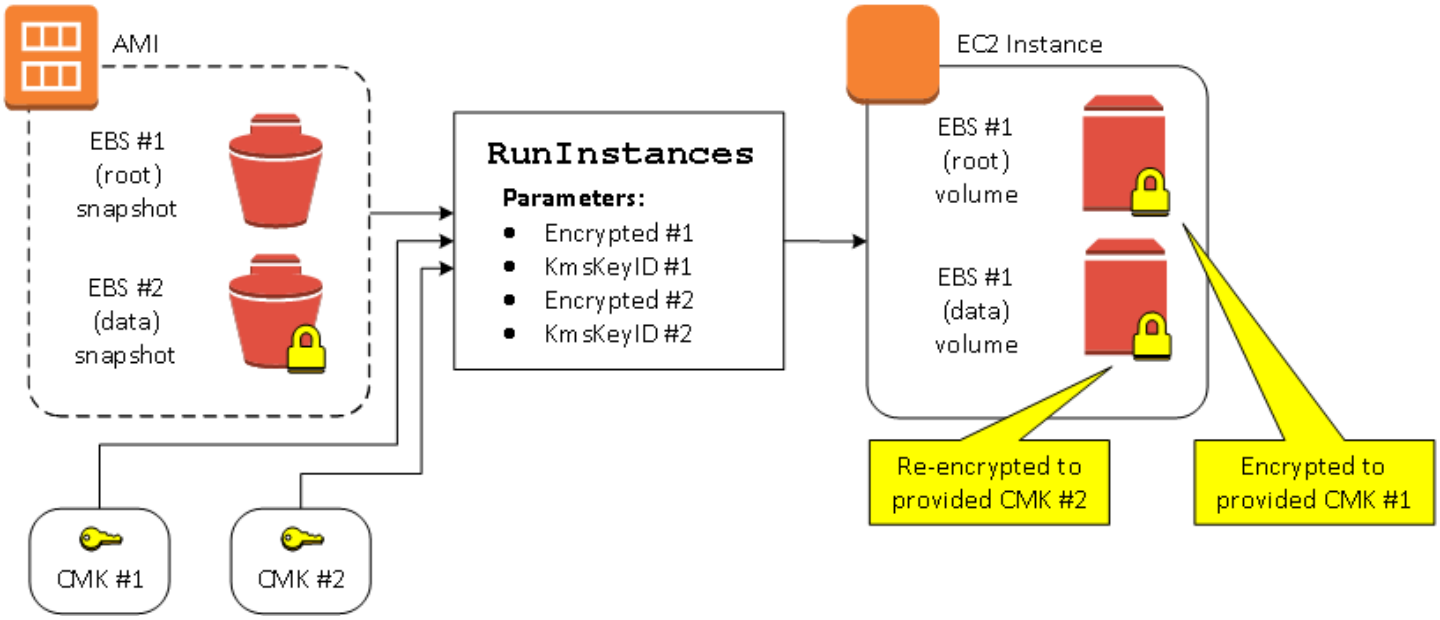


Se você possuir a AMI e não fornecer nenhum parâmetro de criptografia, a instância resultante terá um volume criptografado pela mesma chave do KMS do snapshot. Se a AMI for compartilhada e não pertencer a você, e nenhum parâmetro de criptografia for fornecido, o volume será criptografado pela

Chave do KMS padrão. Com os parâmetros de criptografia fornecidos conforme mostrado, o volume será criptografado pela Chave do KMS especificada.

Alterar o estado de criptografia de vários volumes durante a execução

Neste exemplo mais complexo, uma AMI baseada em vários snapshots (cada um com seu próprio estado de criptografia) é usada para executar uma instância do EC2 com um volume recém-criptografado e um volume criptografado novamente.



Neste cenário, a ação `RunInstances` é fornecida com parâmetros de criptografia para cada um dos snapshots de origem. Quando todos os parâmetros possíveis de criptografia forem especificados, a instância resultante será a mesma, independentemente de você possuir a AMI.

Cenários de cópia de imagem

As AMIs do Amazon EC2 são copiadas usando a ação `CopyImage`, seja pelo AWS Management Console ou diretamente usando a CLI ou a API do Amazon EC2.

Por padrão, sem parâmetros de criptografia explícitos, uma ação `CopyImage` mantém o estado de criptografia existente dos snapshots de origem de uma AMI durante a cópia. Também é possível copiar uma AMI e aplicar simultaneamente um novo estado de criptografia aos snapshots associados do EBS fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Copiar sem parâmetros de criptografia

- Um snapshot não criptografado é copiado para outro snapshot não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os snapshots recém-criados serão criptografados.
- Um snapshot criptografado de sua propriedade é copiado para um snapshot criptografado com a mesma Chave do KMS.
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um snapshot que é criptografado pela chave do KMS padrão da sua conta da AWS.

Todos esses comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

Comportamentos de cópia de imagem com **`Encrypted`** definido, mas nenhum **`KmsKeyId`** especificado

- Um snapshot não criptografado é copiado para um snapshot criptografado pela chave do KMS padrão da conta da AWS.
- Um snapshot criptografado é copiado para outro snapshot criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)

A configuração dos parâmetros `Encrypted` e `KmsKeyId` permite especificar uma Chave do KMS gerenciada pelo cliente para uma operação de criptografia. Os seguintes comportamentos resultam em:

Comportamentos de cópia de imagem com **`Encrypted`** e **`KmsKeyId`** definidos

- Um snapshot não criptografado é copiado para um snapshot criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é copiado para outro snapshot criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

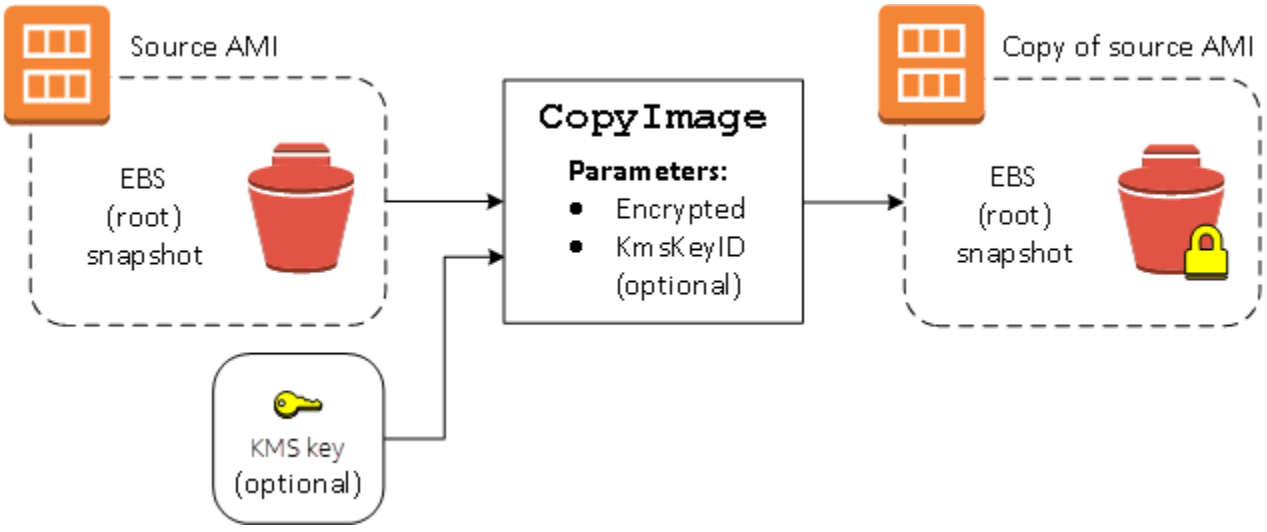
A seção a seguir fornece um exemplo de como copiar uma AMI usando parâmetros de criptografia não padrão, resultando em uma alteração do estado de criptografia.

Para obter instruções detalhadas usando o console, consulte Copiar um AMI.

Criptografar uma imagem não criptografada durante a cópia

Nesse cenário, uma AMI baseada em um snapshot raiz não criptografado é copiada para uma AMI com um snapshot raiz criptografado. A ação `CopyImage` é invocada com dois parâmetros de criptografia, incluindo uma chave gerenciada pelo cliente. Como resultado, o status de criptografia do snapshot raiz muda, de modo que a AMI de destino tenha suporte de um snapshot raiz contendo os mesmos dados que o snapshot de origem, mas criptografado usando a chave especificada. Você incorre em custos de armazenamento para os snapshots em ambas as AMIs, bem como cobranças para todas as instâncias iniciadas a partir de uma AMI.

> **Note**
>
> Habilitar a criptografia por padrão tem o mesmo efeito que configurar o parâmetro `Encrypted` como `true` para todos os snapshots na AMI.



Configurar o parâmetro `Encrypted` criptografa o snapshot único dessa instância. Se você não especificar o parâmetro `KmsKeyId`, a chave gerenciada pelo cliente padrão será usada para criptografar a cópia do snapshot.

> **Note**
>
> Também é possível copiar uma imagem com vários snapshots e configurar o estado de criptografia de cada uma individualmente.

Monitorar eventos da AMI usando o Amazon EventBridge

Quando o estado de uma imagem de máquina da Amazon (AMI) muda, o Amazon EC2 gera um evento que é enviado para o Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events). É possível usar o Amazon EventBridge para detectar e reagir a esses eventos. Você faz isso criando regras no EventBridge que acionem uma ação em resposta a um evento. Por exemplo, é possível criar uma regra do EventBridge que detecte quando o processo de criação da AMI foi concluído e, em seguida, invoque um tópico do Amazon SNS para enviar uma notificação por email para você.

O Amazon EC2 gera um evento quando uma AMI entra em qualquer um dos seguintes estados:

- `available`
- `failed`
- `deregistered`
- `disabled`

A tabela abaixo mostra as operações da AMI e os estados que podem ser atribuídos a ela. Na tabela, Sim indica os estados que podem ser atribuídos à AMI ao executar a operação correspondente.

Operações da AMI	available	failed	deregistered	disabled
CopyImage	Sim	Sim		
CreateImage	Sim	Sim		
CreateRestoreImageTask	Sim	Sim		

Operações da AMI	available	failed	deregistered	disabled
DeregisterImage			Sim	
DisableImage				Sim
EnableImage	Sim			
RegisterImage	Sim	Sim		

Os eventos são gerados com base no melhor esforço.

Tópicos

- Eventos da AMI
- Criar uma regra do Amazon EventBridge

Eventos da AMI

Existem quatro eventos de EC2 AMI State Change:

- available
- failed
- deregistered
- disabled

Os eventos são enviados para o barramento de eventos do EventBridge padrão no formato JSON.

Os campos a seguir no evento podem ser usados para criar regras que acionem uma ação:

`"source": "aws.ec2"`

Identifica que o evento é do Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica o nome do evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Fornece as seguintes informações:

- O ID da AMI: se você quiser rastrear uma AMI específica.
- O estado da AMI (`available`, `failed`, `deregistered` ou `disabled`).

`available`

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `available` após uma operação de `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` ou `EnableImage` com êxito.

`"State": "available"` indica que a operação teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

`failed`

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `failed` após uma operação de `CreateImage`, `CopyImage`, `RegisterImage` ou `CreateRestoreImageTask` com êxito.

Os campos a seguir fornecem informações pertinentes:

- `"State": "failed"`: indica que a operação falhou.

- `"ErrorMessage": ""`: Fornece o motivo da operação com falha.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

deregistered

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `deregistered` após uma operação de `DeregisterImage` com êxito. Se a operação falhar, nenhum evento será gerado. Qualquer falha será conhecida imediatamente, pois `DeregisterImage` é uma operação síncrona.

`"State": "deregistered"` indica que a operação `DeregisterImage` teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
```

```
        "ErrorMessage": ""
    }
}
```

`disabled`

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `disabled` após uma operação de `DisableImage` com êxito. Se a operação falhar, nenhum evento será gerado. Qualquer falha será conhecida imediatamente, pois `DisableImage` é uma operação síncrona.

`"State": "disabled"` indica que a operação `DisableImage` teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

Criar uma regra do Amazon EventBridge

Você é possível uma regra do Amazon EventBridge que especifique uma ação a ser executada quando o EventBridge receber um evento que corresponda ao padrão de evento na regra. Quando um evento corresponde, o EventBridge envia o evento para o destino especificado e aciona a ação definida na regra.

Os padrões de eventos têm a mesma estrutura que os eventos aos quais correspondem. Um padrão de evento corresponde a um evento ou não corresponde.

Ao criar uma regra para um evento de alteração de estado da AMI, é possível incluir os seguintes campos no padrão de evento:

`"source": "aws.ec2“`

Identifica que o evento é do Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica o nome do evento.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Fornece as seguintes informações:

- O ID da AMI: se você quiser rastrear uma AMI específica.
- O estado da AMI (`available`, `failed`, `deregistered` ou `disabled`).

Exemplo: Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivo móvel quando qualquer AMI estiver no estado `available` após a operação `CreateImage` ter sido concluída com êxito.

Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra do EventBridge para enviar uma notificação quando uma AMI for criada e estiver no estado **`available`**

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:

   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.

   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).

d. Escolha Próximo.

4. Em Build event pattern (Criar padrão de evento), faça o seguinte:

   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.

   b. Em Event pattern (Padrão de evento), para este exemplo, você especificará o seguinte padrão de evento para corresponder a qualquer evento `EC2 AMI State Change` gerado quando uma AMI entra no estado `available`:

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 AMI State Change"],
 "detail": {"State": ["available"]}
}
```

      Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

      i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

         A. Escolha Event pattern form (Formulário de evento).

         B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

         C. Em AWS Service (Serviço da), escolha EC2.

         D. Em Event type (Tipo de evento), escolha EC2 AMI State Change (Alteração do estado da AMI do EC2).

         E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

      ii. Para especificar um padrão de evento personalizado, faça o seguinte:

         A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

         B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

   c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

   a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).
7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar Regra.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do Amazon EventBridge:

- Eventos do Amazon EventBridge
- Padrões de eventos do Amazon EventBridge
- Regras do Amazon EventBridge

Para obter um tutorial sobre como criar uma função do Lambda e uma regra do EventBridge que execute a função do Lambda, consulte Tutorial: Registrar em log o estado de uma instância do Amazon EC2 usando o EventBridge no Guia do desenvolvedor do AWS Lambda.

Noções básicas sobre as informações de faturamento da AMI

Há muitas Imagens de máquina da Amazon (AMIs) para escolher ao executar suas instâncias e elas oferecem suporte a uma variedade de plataformas e recursos do sistema operacional. Para entender como a AMI escolhida ao executar sua instância afeta os resultados da sua fatura da AWS, é possível pesquisar a plataforma do sistema operacional associada e as informações de

faturamento. Faça isso antes de executar qualquer on-demand ou Instâncias spot, ou comprar uma Instância reservada.

Aqui estão dois exemplos de como pesquisar sua AMI com antecedência pode ajudá-lo a escolher a AMI que melhor se adapte às suas necessidades:

- Para Instâncias spot, é possível usar os detalhes da plataforma da AMI para confirmar se há suporte à AMI para Instâncias spot.
- Ao comprar uma Instância reservada, é possível certificar-se de selecionar a plataforma do sistema operacional (Plataforma) que mapeia para os detalhes da Plataforma AMI.

Para obter mais informações sobre a definição de instâncias, consulte Definição de preço do Amazon EC2.

Tópicos

- Campos de informações de faturamento da AMI
- Localizando detalhes de faturamento e uso da AMI
- Verificar cobranças da AMI em sua fatura

Campos de informações de faturamento da AMI

Os campos a seguir fornecem informações de faturamento associadas a uma AMI:

Detalhes da plataforma

Os detalhes da plataforma associada ao código de faturamento da AMI. Por exemplo, `Red Hat Enterprise Linux`.

Operação de uso

A operação da instância do Amazon EC2 e o código de faturamento associado à AMI. Por exemplo, `RunInstances:0010`. A Usage operation (Operação de uso) corresponde à coluna lineitem/Operation (lineitem/Operação) no seu Relatório de custos e uso (CUR) da AWS e na API de tabela de preços da AWS.

É possível visualizar esses campos na página Instâncias ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando describe-images ou Get-EC2Image.

Dados de amostra: operação de uso por plataforma

A tabela a seguir lista os detalhes da plataforma e os valores de operação de uso que podem ser exibidos na página Instâncias ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando describe-images ou Get-EC2Image.

Detalhes da plataforma	Operação de uso [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0 [3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200

Detalhes da plataforma	Operação de uso [2]
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise [1]	RunInstances:0102
Windows with SQL Server Standard [1]	RunInstances:0006
Windows with SQL Server Web [1]	RunInstances:0202

[1] Se duas licenças de software estiverem associadas a uma AMI, o campo Detalhes da plataforma mostrará ambas.

[2] Se você estiver executando instâncias spot, o item lineitem/Operation no Relatório de Custos e Uso da AWS poderá ser diferente do valor da Operação de uso listado aqui. Por exemplo, se `lineitem/Operation` exibir `RunInstances:0010:SV006`, significa que o Amazon EC2 está executando a instância spot do Red Hat Enterprise Linux por hora no Leste dos EUA (Norte da Virgínia) na Zona 6.

[3] Isso aparece como RunInstances (Linux/UNIX) em seus relatórios de uso.

Localizando detalhes de faturamento e uso da AMI

No console do Amazon EC2, é possível visualizar as informações de faturamento da AMI na página AMIs ou na página Instances (Instâncias) . Também é possível encontrar informações de faturamento usando a AWS CLI ou o serviço de metadados da instância.

Os campos a seguir podem ajudá-lo a verificar as cobranças da AMI em sua fatura:

- Detalhes da plataforma
- Operação de uso

- ID DA AMI

Localizar informações de faturamento da AMI (console)

Siga estas etapas para visualizar as informações de faturamento da AMI no console do Amazon EC2:

Procure informações de faturamento da AMI na página AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMIs, e selecione uma AMI.
3. Na guia Details (Detalhes), verifique os valores para Platform details (Detalhes da plataforma) e Usage operation (Operação de uso).

Procure informações de faturamento da AMI na página Instances (Instâncias)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione uma instância.
3. Na guia Details (Detalhes) (ou na guia Description (Descrição) , se você estiver usando a versão anterior do console, verifique os valores para Platform details (Detalhes da plataforma) e Usage operation (Operação de uso).

Localizar informações de faturamento da AMI (AWS CLI)

Para localizar as informações de faturamento da AMI usando a AWS CLI, você precisa saber o ID da AMI. Se não souber o ID da AMI, é possível obtê-lo na instância usando o comando describe-instances (Descrever instâncias).

Para localizar o ID da AMI

Se você souber o ID da instância, poderá obter o ID da AMI para a instância usando o comando describe-instances (Descrever instâncias).

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

No resultado, o ID da AMI é especificado no campo `ImageId`.

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Para localizar as informações de faturamento da AMI

Se souber o ID da AMI, é possível usar o comando describe-images (Descrever imagens) para obter detalhes de operação de uso e da plataforma da AMI.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

A saída do exemplo a seguir mostra os campos `PlatformDetails` e `UsageOperation`. Neste exemplo, a plataforma ami-0123456789EXAMPLE é `Red Hat Enterprise Linux` e a operação de uso e o código de faturamento é `RunInstances:0010`.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
```

```
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Verificar cobranças da AMI em sua fatura

Para garantir que você não incorra em custos não planejados, verifique se as informações de faturamento de uma instância no Relatório de custos e uso (CUR) da AWS correspondem às informações de faturamento associadas à AMI que você usou para executar a instância.

Para confirmar as informações de faturamento, localize o ID da instância no CUR e verifique o valor correspondente na coluna `lineitem/Operation`. O valor deve corresponder ao valor da Usage operation (Operação de uso) associada à AMI.

Por exemplo, a AMI `ami-0123456789EXAMPLE` tem as seguintes informações de faturamento:

- Detalhes da plataforma = `Red Hat Enterprise Linux`
- Operação de uso = `RunInstances:0010`

Se você executou uma instância usando essa AMI, poderá localizar o ID da instância no CUR e verificar o valor correspondente na coluna `lineitem/Operation`. Neste exemplo, o valor deve ser `RunInstances:0010`.

Cotas de AMI

As cotas a seguir se aplicam à criação e ao compartilhamento de AMIs. Estas cotas são aplicáveis por Região da AWS.

Nome da cota	Descrição	Cota padrão por região
AMIs	O número máximo de AMIs públicas e privadas permitido por região. Isso inclui AMIs disponíveis, pendentes e desabilitadas e AMIs na Lixeira.	50.000
AMIs públicas	O número máximo de AMIs públicas, inclusive AMIs públicas na Lixeira, permitido por região.	5
Compartilhamento de AMIs	O número máximo de entidades (organizações, unidades organizacionais [UOs] e contas) com as quais uma AMI pode ser compartil hada em uma região. Se você compartilhar uma AMI com uma organização ou UO, o número de contas na organização ou na UO não contará para a cota.	1.000

Se exceder suas cotas e quiser criar ou compartilhar mais AMIs, você poderá fazer o seguinte:

- Se você exceder sua cota de AMIs total ou de AMIs públicas, considere cancelar o registro de imagens não usadas.
- Se você exceder sua cota de AMIs públicas, considere tornar uma ou mais AMIs públicas privadas.
- Se você exceder sua cota de compartilhamento de AMIs, considere compartilhar suas AMIs com uma organização ou UO em vez de contas separadas.
- Solicite um aumento de cota para AMIs.

Solicitar um aumento de cota para AMIs

Se precisar exceder a cota padrão de AMIs, solicite um aumento de cota.

Para solicitar um aumento de cota para AMIs

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. No painel de navegação, selecione serviços da AWS.
3. Escolha Amazon Elastic Compute Cloud (Amazon EC2) na lista ou digite o nome do serviço na caixa de pesquisa.
4. Escolha a cota da AMI para solicitar um aumento. As cotas da AMI que você pode selecionar são:
   - AMIs
   - AMIs públicas
   - Compartilhamento de AMI
5. Selecione Solicitar aumento de cota.
6. Em Change quota value (Alterar valor da cota), insira o novo valor da cota e escolha Request (Solicitar).

Para exibir quaisquer solicitações pendentes ou resolvidas recentemente, escolha Dashboard (Painel) no painel de navegação. Para solicitações pendentes, escolha o status da solicitação para abrir o recibo da solicitação. O status inicial de uma solicitação é Pending (Pendente). Depois que o status for alterado para Quota requested (Cota solicitada), você verá o número do caso em Support Center case number (Número do caso no Support Center). Escolha o número do caso para abrir o tíquete de sua solicitação.

Depois que a solicitação é resolvida, o Applied quota value (Valor da cota aplicada) para a cota é definido como o novo valor.

Para obter mais informações, consulte o Manual do usuário do Service Quotas.

Instâncias do Amazon EC2

Para executar um ambiente de produção, você precisará responder às seguintes perguntas.

P: Qual tipo de instância melhor atende às minhas necessidades?

O Amazon EC2 fornece tipos de instância diferentes para permitir que você escolha a CPU, a memória, o armazenamento e a capacidade de rede que você precisa para executar suas aplicações. Para obter mais informações, consulte Tipos de instância do Amazon EC2.

P: Qual opção de compra melhor atende às minhas necessidades?

O Amazon EC2 oferece suporte a Instâncias on-demand (o padrão), Instâncias spot e Instâncias reservadas. Para obter mais informações, consulte Opções de compra de instância.

P: Que tipo de volume raiz atende às minhas necessidades?

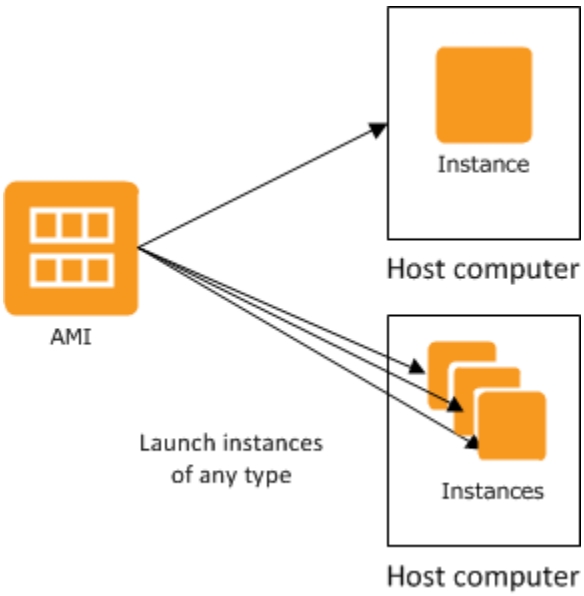
Cada instância é baseada no Amazon EBS ou no armazenamento de instâncias. Selecione uma AMI baseada no tipo de volume raiz necessário. Para obter mais informações, consulte Armazenamento para o dispositivo raiz.

P: Posso gerenciar remotamente uma frota de instâncias do EC2 e máquinas no meu ambiente híbrido?

O AWS Systems Manager permite gerenciar, de forma remota e segura, a configuração de suas instâncias do Amazon EC2, bem como suas instâncias e máquinas virtuais (VMs) on-premises em ambientes híbridos, incluindo VMs de outros provedores de nuvem. Para obter mais informações, consulte o Guia do usuário do AWS Systems Manager.

Instâncias e AMIs

Uma Imagem de máquina da Amazon (AMI) é um modelo que contém uma configuração de software (por exemplo, sistema operacional, servidor de aplicação e aplicações). A partir de uma AMI, execute uma instância, que é uma cópia da AMI que roda como servidor virtual na nuvem. É possível executar várias instâncias de uma AMI, conforme mostrado na figura a seguir.



Suas instâncias continuarão sendo executadas até que você as interrompa, hiberne ou encerre, ou até que elas falhem. Se uma instância falhar, é possível executar uma nova instância a partir da AMI.

Instâncias

Uma instância é um servidor virtual na nuvem . A configuração na execução é uma cópia da AMI que você especificou ao executar a instância.

É possível executar diferentes tipos de instâncias a partir de uma única AMI. O tipo de instância determina essencialmente o hardware do computador host usado para sua instância. Cada tipo de instância oferece recursos diferentes de computação e memória. Selecione um tipo de instância de acordo com a quantidade de capacidade de memória e computação necessária para a aplicação ou software que você pretende executar na instância. Para obter especificações detalhadas sobre o tipo de instância, consulte Specifications no Guia de tipos de instância do Amazon EC2. Para obter informações sobre os preços, consulte Preço sob demanda do Amazon EC2.

Após iniciar uma instância, ela se parecerá como um host tradicional, e você poderá interagir com ela assim como com qualquer computador. Você tem controle total de suas instâncias. É possível usar o sudo para executar os comandos que exigem privilégios raiz.

Sua conta da AWS tem um limite quanto ao número de instâncias que é possível ter em execução. Para obter mais informações sobre esse limite e sobre como solicitar um aumento, consulte Quantas instâncias posso executar no Amazon EC2 nas perguntas frequentes gerais do Amazon EC2.

Armazenamento para sua instância

O dispositivo raiz da sua instância contém a imagem usada para inicializar a instância. O dispositivo raiz é um volume do Amazon Elastic Block Store (Amazon EBS) ou um volume do armazenamento de instâncias. Para obter mais informações, consulte Volume raiz da instância do Amazon EC2.

Sua instância pode incluir os volumes de armazenamento locais, conhecidos como volumes de armazenamento de instâncias, que é possível configurar o momento da execução com o mapeamento de dispositivos de blocos. Para obter mais informações, consulte Mapeamentos de dispositivos de blocos. Depois de esses volumes serem adicionados e mapeados para sua instância, eles estarão disponíveis para você montar e usar. Se sua instância falhar, ou se sua instância for executada ou encerrada, os dados nesses volumes serão perdidos; portanto, esses volumes são mais bem usados para dados temporários. Para manter a segurança de dados importantes, use uma estratégia de replicação em várias instâncias ou armazenar seus dados persistentes em volumes do Amazon S3 ou do Amazon EBS. Para obter mais informações, consulte Opções de armazenamento para as instâncias do Amazon EC2.

Práticas recomendadas de segurança

- Use o AWS Identity and Access Management (IAM) para controlar o acesso aos seus recursos da AWS, incluindo suas instâncias. Para ter mais informações, consulte Identity and Access Management para o Amazon EC2.
- Restrinja o acesso permitindo somente que hosts ou redes confiáveis acessem as portas na sua instância. Por exemplo, é possível restringir o acesso a SSH ao restringir o tráfego de entrada na porta 22. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.
- Revise as regras de seus grupos de segurança regularmente e aplique o princípio do menor privilégio: abra somente as permissões que forem necessárias. Também é possível criar grupos de segurança diferentes para lidar com instâncias com requisitos de segurança diferentes. Pense em criar um grupo de segurança bastion que permita logins externos e mantenha o restante de suas instâncias em um grupo que não permita logins externos.
- Desabilite logins com senha das instâncias executadas a partir da sua AMI. As senhas podem ser localizadas ou roubadas, e são um risco para a segurança. Para obter mais informações, consulte Desabilitar logins remotos com senha para o usuário raiz. Para obter mais informações sobre compartilhamento seguro das AMIs, consulte AMIs compartilhadas.

Interromper e encerrar instâncias

É possível interromper ou encerrar uma instância em execução a qualquer momento.

Interromper uma instância

Quando uma instância for interrompida, ela executará a desativação normal e fará a transição para o estado `stopped`. Todos os volumes do Amazon EBS permanecem associados e é possível começar a instância novamente em um momento posterior.

Você não será cobrado pelo uso adicional da instância enquanto ela estiver em estado interrompido. Toda transição de um estado interrompido para um estado em execução é cobrada. Se o tipo de instância foi alterado enquanto a instância estava interrompida, a taxa do novo tipo de instância será cobrada depois que a instância for iniciada. O armazenamento do Amazon EBS associado para a instância, incluindo o volume de dispositivo raiz, também será cobrado.

Quando uma instância estiver em um estado interrompido, será possível associar ou separar os volumes do Amazon EBS. Também é possível criar AMIs a partir da instância e alterar o kernel, o disco de RAM e o tipo de instância.

Como encerrar uma instância

Quando uma instância é encerrada, ela executa uma desligamento normal. O volume do dispositivo raiz é excluído por padrão, mas todos os volumes do Amazon EBS anexados são preservados por padrão, que é determinado pela configuração do atributo `deleteOnTermination` de cada volume. A instância em si também é excluída, e você não pode iniciá-la novamente em um momento posterior.

Para evitar encerramento acidental, é possível desabilitar o encerramento da instância. Se você fizer isso, garanta que o atributo `disableApiTermination` esteja definido como `true` para a instância. Para controlar o comportamento da desativação da instância, como `shutdown -h` em Linux ou `shutdown` no Windows, defina o atributo da instância `instanceInitiatedShutdownBehavior` como `stop` ou `terminate`, conforme desejado. As instâncias com volumes do Amazon EBS para o dispositivo raiz usam `stop` como padrão, e as instâncias com dispositivos raiz de armazenamento de instâncias são sempre encerradas como resultado da desativação da instância.

Para ter mais informações, consulte Ciclo de vida da instância.

> **Note**
>
> Alguns recursos da AWS, como volumes do Amazon EBS e endereços IP elásticos, incorrem em cobranças independentemente do estado da instância. Para obter mais informações, consulte Evitar cobranças inesperadas no Manual do usuário do AWS Billing. Para obter mais informações sobre os custos do Amazon EBS, consulte a Definição de preço do Amazon EBS.

AMIs

A Amazon Web Services (AWS) publica as imagens de máquina da Amazon (AMIs) que contêm as configurações de software comuns para uso público. Além disso, os membros da comunidade de desenvolvedores da AWS publicaram suas próprias AMIs personalizadas. Também é possível criar suas próprias AMIs personalizadas, o que permite iniciar, com rapidez e facilidade, as novas instâncias que têm tudo de que você precisa. Por exemplo, se sua aplicação for um site ou serviço Web, sua AMI pode incluir um servidor Web, o conteúdo estático associado e o código para as páginas dinâmicas. Como resultado, depois de executar uma instância a partir dessa AMI, seu servidor Web é iniciado e sua aplicação fica pronta para aceitar solicitações.

Todas as AMIs são classificadas como com Amazon EBS, o que significa que o dispositivo raiz da instância executada a partir da AMI é um volume do Amazon EBS ou com armazenamento de instâncias, o que significa que o dispositivo raiz da instância executada a partir da AMI é um volume de armazenamento de instâncias criado a partir de um modelo armazenado em Amazon S3.

A descrição de uma AMI indica o tipo de dispositivo raiz (`ebs` ou `instance store`). Isso é importante, pois há diferenças significativas quanto a que é possível fazer com cada tipo de AMI. Para obter mais informações sobre essas diferenças, consulte Armazenamento para o dispositivo raiz.

É possível cancelar o registro de uma AMI quando tiver terminado de usá-la. Depois de cancelar o registro de uma AMI, você não poderá usá-la para executar novas instâncias. As instâncias existentes executadas na AMI não são afetadas. Portanto, se você também tiver terminado com as instâncias executadas por essas AMIs, deverá encerrá-las.

Tipos de instância do Amazon EC2

Quando executa uma instância, o tipo de instância que você especifica determina o hardware do computador host usado para sua instância. Cada tipo de instância oferece recursos de computação, memória e armazenamento diferentes, além de ser agrupado em famílias de instâncias de acordo com esses recursos. Selecione um tipo de instância com base nos requisitos da aplicação ou do software que você pretende executar na instância.

O Amazon EC2 dedica alguns recursos do computador host, como CPU, memória e armazenamento de instâncias, a uma instância específica. O Amazon EC2 compartilha outros recursos do computador host, como a rede e o subsistema de disco, entre instâncias. Se cada instância em um computador host tentar usar o máximo desses recursos compartilhados quanto for possível, cada uma receberá uma parte igual daquele recurso. No entanto, quando um recurso for pouco utilizado, uma instância poderá consumir uma parte maior desse recurso enquanto ele estiver disponível.

Cada tipo de instância fornece uma performance mínima superior ou inferior com base em um recurso compartilhado. Por exemplo, tipos de instância com performance alta de E/S têm uma alocação maior dos recursos compartilhados. A alocação de uma parte maior dos recursos compartilhados também reduz a variação da performance de E/S. Para a maioria das aplicações, a performance moderada de E/S é mais do que suficiente. No entanto, para aplicações que exigem uma performance de E/S maior ou mais consistente, considere um tipo de instância com performance mais alta de E/S.

Tópicos

- Tipos de instâncias disponíveis
- Especificações de hardware
- Tipos de virtualização de AMI
- Localizar um tipo de instância do Amazon EC2
- Obter recomendações de um tipo de instância
- Alterar o tipo de instância
- Instâncias expansíveis
- Aceleração de desempenho com instâncias de GPU

Tipos de instâncias disponíveis

O Amazon EC2 fornece uma ampla seleção de tipos de instância otimizadas para de adequarem a diferentes casos de uso. Os tipos de instância incluem combinações variadas de capacidade de CPU, memória, armazenamento e redes e oferecem a flexibilidade de escolher a combinação de recursos adequada para suas aplicações. Cada tipo de instância inclui um ou mais tamanhos de instância, permitindo escalar os recursos de acordo com os requisitos da workload de destino. Para obter mais informações sobre os recursos e sobre os casos de uso, consulte os detalhes dos tipos de instância do Amazon EC2.

Convenções de nomenclatura para o tipo de instância

Os nomes são baseados na família da instância, na geração, na família do processador, nas funcionalidades e no tamanho. Para obter mais informações, consulte Naming conventions no Guia de tipos de instância do Amazon EC2.

Localizar um tipo de instância do

Para determinar quais tipos de instância atendem aos seus requisitos, por exemplo, regiões, recursos de computação ou recursos de armazenamento compatíveis, consulte Localizar um tipo de instância do Amazon EC2 e Amazon EC2 instance type specifications no Guia de tipos de instância do Amazon EC2.

Instâncias da geração atual

- Uso geral: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | Mac1 | Mac2 | Mac2-m1ultra | Mac2-m2 | Mac2-m2pro | T2 | T3 | T3a | T4g
- Otimizada para computação: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-flex
- Otimizada para memória: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7gd | R7i | R7iz | U-3tb1 | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb | X1 | X2gd | X2idn | X2iedn | X2iezn | X1e | z1d
- Otimizada para armazenamento: D2 | D3 | D3en | H1 | I3 | I3en | I4g | I4i | Im4gn | Is4gen
- Com computação acelerada: DL1 | DL2q | F1 | G4ad | G4dn | G5 | G5g | G6 | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | Trn1n | VT1

- Com computação de alta performance: Hpc6a | Hpc6id | Hpc7a | Hpc7g

Instâncias da geração anterior

- Uso geral: A1 | M1 | M2 | M3 | M4 | T1
- Otimizada para computação: C1 | C3 | C4
- Otimizada para memória: R3 | R4
- Otimizada para armazenamento: I2
- Com computação acelerada: G3

Especificações de hardware

Para obter especificações detalhadas sobre o tipo de instância, consulte Specifications no Guia de tipos de instância do Amazon EC2. Para obter informações sobre os preços, consulte Preço sob demanda do Amazon EC2.

Para determinar que tipo de instância atende melhor às suas necessidades, recomendamos executar uma instância e usar seu própria aplicação de referência. Como você paga pelo segundo da instância, é conveniente e econômico testar vários tipos de instância antes de tomar uma decisão. Se suas necessidades mudarem, mesmo depois de tomar uma decisão, será possível alterar o tipo de instância mais tarde. Para ter mais informações, consulte Alterar o tipo de instância.

Recursos do processador Intel

Amazon EC2 as instâncias executadas nos processadores Intel podem incluir os seguintes recursos. Nem todos os recursos de processador a seguir são compatíveis com todos os tipos de instância. Para obter informações detalhadas sobre quais recursos estão disponíveis para cada tipo de instância, consulte Tipos de instância do Amazon EC2.

- Intel AES New Instructions (AES-NI) — O conjunto de instruções de criptografia Intel AES-NI aprimora o algoritmo Advanced Encryption Standard (AES) original para oferecer proteção de dados mais rápida e maior segurança. Todas as instâncias do EC2 da geração atual oferecem suporte a esse recurso de processador.
- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2 e AVX-512): o Intel AVX e o Intel AVX2 são extensões de conjunto de instruções de 256 bits e o Intel AVX-512 é uma extensão de conjunto de instruções de 512 bits projetadas para aplicações com uso intensivo de Floating Point (FP – Ponto flutuante). As instruções Intel AVX melhoram a performance de aplicações, como de

processamento de imagem, áudio e vídeo, simulações científicas, análise financeira e modelagem e análise 3D. Esses recursos só estão disponíveis em instâncias executadas com AMIs de HVM.

- Tecnologia Intel Turbo Boost — Os processadores com Tecnologia Intel Turbo Boost executam núcleos automaticamente com mais rapidez do que a frequência operacional básica.
- Intel Deep Learning Boost (Intel DL Boost) — Acelera os casos de uso de deep learning profundo da IA. Os processadores Intel Xeon Scalable da segunda geração ampliam o Intel AVX-512 com uma nova Vector Neural Network Instruction (VNNI/INT8), que aumenta significativamente a performance de inferência de deep learning em comparação com a geração anterior dos processadores Intel Xeon Scalable (com FP32), para reconhecimento/segmentação de imagens, detecção de objetos, reconhecimento de fala, tradução de idiomas, sistemas de recomendação, aprendizado por reforço e outros. A VNNI pode não ser compatível com todas as distribuições Linux.

  As seguintes instâncias oferecem suporte a VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` e `C6i`. As instâncias `C5` e `C5d` só oferecem suporte a VNNI para as instâncias `12xlarge`, `24xlarge` e `metal`.

As convenções de nomenclatura do setor para CPUs de 64 bits podem gerar confusão. A fabricante de chips Advanced Micro Devices (AMD) apresentou a primeira arquitetura 64 bits comercialmente bem-sucedida com base no conjunto de instruções do Intel x86. Consequentemente, a arquitetura é amplamente referida como AMD64, independente do fabricante do chip. O Windows e várias distribuições do Linux adotam essa prática. Isso explica por que as informações internas do sistema em uma instância que executa o Ubuntu ou o Windows exibe a arquitetura de CPU como AMD64, ainda que as instâncias estejam sendo executadas em hardware Intel.

Processadores AWS Graviton

O AWS Graviton é uma família de processadores projetada para oferecer a melhor relação entre preço e performance para as workloads executadas em instâncias do Amazon EC2.

Para obter mais informações, consulte Getting started with Graviton.

AWS Trainium

As instâncias desenvolvidas pelo AWS Trainium têm propósito específico para o treinamento de aprendizado profundo com alta performance e baixo custo. É possível usar essas instâncias para treinar modelos de processamento de linguagem natural, de visão computacional e de recomendação usados em um amplo conjunto de aplicações, como reconhecimento de fala,

recomendações, detecção de fraudes e classificação de imagens e vídeos. Use os fluxos de trabalho existentes em estruturas de ML conhecidas, como PyTorch e TensorFlow.

AWS Inferentia

As instâncias desenvolvidas pelo AWS Inferentia são projetadas para acelerar o machine learning. Essas instâncias fornecem inferência de machine learning de alta performance e baixa latência. Essas instâncias são otimizadas para implantar modelos de aprendizagem profunda (DL) para aplicações, como processamento de linguagem natural, detecção e classificação de objetos, personalização e filtragem de conteúdo e reconhecimento de fala.

É possível começar de diversas maneiras:

- Use o SageMaker, um serviço totalmente gerenciado que é a maneira mais fácil de começar a usar modelos de machine learning. Para obter informações, consulte What Is Amazon SageMaker? (O que é o Amazon SageMaker?) no Guia do desenvolvedor do Amazon SageMaker.
- Inicie uma instância Inf1 ou Inf2 usando a AMI de aprendizado profundo. Para obter mais informações, consulte AWS Inferentia com DLAMI no Guia do desenvolvedor do AWS Deep Learning AMI.
- Execute uma instância Inf1 ou Inf2 usando sua própria AMI e instale o AWS Neuron SDK, que permite compilar, executar e criar perfis de modelos de aprendizado profundo para o AWS Inferentia.
- Inicie uma instância de contêiner usando uma instância Inf1 ou Inf2 e uma AMI otimizada para o Amazon ECS. Para obter mais informações, consulte AMIs do Amazon Linux 2 (Inferentia) no Amazon Elastic Container Service Developer Guide.
- Crie um cluster do Amazon EKS com nós executando instâncias Inf1. Para obter mais informações, consulte Inferentia support (Suporte para Inferentia) no Amazon EKS User Guide (Manual do usuário do Amazon EKS).

Tipos de virtualização de AMI

O tipo de virtualização da sua instância é determinado pela AMI usada para executá-la. Os tipos de instância da geração atual oferecem suporte apenas a HVM. Alguns tipos de instância de geração anterior são compatíveis com paravirtual (PV) e algumas regiões da AWS são compatíveis com as instâncias PV. Para obter mais informações, consulte Tipos de virtualização de AMI.

Para a melhor performance, recomendamos usar uma AMI HVM. Além disso, as AMIs HVM são necessárias para aproveitar as maiores capacidades de rede. A virtualização da HVM usa tecnologia

assistida por hardware fornecida pela plataforma AWS. Com a virtualização da HVM, a VM guest é executada como se estivesse em uma plataforma de hardware nativa, exceto pelo fato de que ela ainda usa drivers de rede e armazenamento PV para melhorar a performance.

Localizar um tipo de instância do Amazon EC2

Para poder executar uma instância, é necessário selecionar um tipo de instância para usar. O tipo de instância escolhido pode depender dos recursos necessários para sua workload, como recursos de computação, memória ou armazenamento. Pode ser benéfico identificar vários tipos de instância possivelmente adequadas à sua workload e avaliar a performance deles em um ambiente de teste. Não há substituto para medir a performance de sua aplicação sob carga.

Se já tiver instâncias do EC2 em execução, será possível usar o AWS Compute Optimizer para obter recomendações sobre os tipos de instâncias que deve usar para melhorar a performance, economizar dinheiro ou ambos. Para ter mais informações, consulte the section called “Para workloads existentes”.

Tarefas

- Localizar um tipo de instância usando o console
- Localizar um tipo de instância usando a AWS CLI

Localizar um tipo de instância usando o console

É possível encontrar um tipo de instância que atenda às suas necessidades usando o console do Amazon EC2.

Como encontrar um tipo de instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel de navegação, selecione Instance Types (Tipos de instância).
4. (Opcional) Selecione o ícone de preferências (engrenagem) para escolher quais atributos de tipos de instância exibir, como a Definição de preço do Linux sob demanda e selecione Confirmar. Como alternativa, selecione o nome de um tipo de instância para abrir a respectiva página de detalhes e exibir todos os atributos disponíveis por meio do console. O console não exibe todos os atributos disponíveis por meio da API ou da linha de comando.

5. Use os atributos de tipo de instância para filtrar a lista de tipos de instância exibidos apenas para os tipos de instância que atendem às suas necessidades. Por exemplo, é possível filtrar com base nos seguintes atributos:

   - Availability zones (Zonas de disponibilidade): o nome da zona de disponibilidade, zona local ou zona Wavelength. Para ter mais informações, consulte the section called “A VPC abrange as zonas de disponibilidade e a zona Wavelength.”.
   - vCPUs (vCPUs) ou Cores (Núcleos): o número de vCPUs ou núcleos.
   - Memory (GiB) (Memória [GiB]): o tamanho da memória em GiB.
   - Network performance (Performance de rede): o desempenho da rede, em Gigabits.
   - Local instance storage (Armazenamento de instâncias locais): indica se o tipo de instância tem armazenamento de instância local (`true` | `false`).

6. (Opcional) Para ver um comparativo lado a lado, marque a caixa de seleção para vários tipos de instâncias. A comparação é exibida na parte inferior da tela.
7. (Opcional) Para salvar a lista de tipos de instância em um arquivo de valores separados por vírgula (.csv) para análise adicional, escolha Actions (Ações), Download list CSV (Baixar lista em CSV). O arquivo inclui todos os tipos de instância que correspondem aos filtros definidos.
8. (Opcional) Para executar instâncias usando um tipo de instância que satisfaça suas necessidades, marque a caixa de seleção para o tipo de instância e escolha Actions (Ações), Launch instance (Executar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Localizar um tipo de instância usando a AWS CLI

É possível usar comandos da AWS CLI para que o Amazon EC2 encontre um tipo de instância que atenda às suas necessidades.

Como encontrar um tipo de instância usando a AWS CLI

1. Se ainda não o fez, instale a AWS CLI. Para obter mais informações, consulte o Guia do usuário da AWS Command Line Interface.
2. Use o comando describe-instance-types para filtrar tipos de instância com base em atributos de instância. Por exemplo, é possível usar o comando a seguir para exibir somente os tipos de instância da geração atual com 64 GiB (65.536 MiB) de memória.

```
aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
 "Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

3. Use o comando describe-instance-type-offerings para filtrar os tipos de instância oferecidos por local (região ou zona). Por exemplo, é possível usar o comando a seguir para exibir os tipos de instância oferecidos na zona especificada.

```
aws ec2 describe-instance-type-offerings --location-type "availability-
zone" --filters Name=location,Values=us-east-2a --region us-east-2 --query
 "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

4. Após localizar tipos de instância que satisfaçam suas necessidades, salve a lista para que possa usar esses tipos de instância ao executar instâncias. Para obter mais informações, consulte Início da instância no Guia do usuário da AWS Command Line Interface.

Obter recomendações de um tipo de instância

As ferramentas a seguir podem ajudar você a selecionar os tipos de instância ideais para suas workloads novas ou existentes:

- Novas workloads: o assistente de seleção de tipo de instância do EC2 considera o caso de uso, o tipo de workload, a preferência do fabricante da CPU e como você prioriza preço e desempenho, bem como os parâmetros adicionais que você pode especificar. Em seguida, ele usa esses dados para fornecer sugestões e orientações sobre os tipos de instância do Amazon EC2 mais adequados às suas novas workloads.
- Workloads existentes: o AWS Compute Optimizer analisa as especificações de instância e as métricas de utilização existentes. Depois, usa os dados compilados para recomendar quais tipos de instância do Amazon EC2 são otimizados para custo ou performance, ou ambos, para as workloads existentes.

Obtenha recomendações de tipo de instância:

- Obter recomendações de tipo de instância para uma nova workload
- Obter recomendações de tipo de instância para uma workload existente

Obter recomendações de tipo de instância para uma nova workload

O assistente de seleção de tipo de instância do EC2 considera o caso de uso, o tipo de workload, a preferência do fabricante da CPU e como você prioriza preço e desempenho, bem como os parâmetros adicionais que você pode especificar. Em seguida, ele usa esses dados para fornecer sugestões e orientações sobre os tipos de instância do Amazon EC2 mais adequados às suas novas workloads.

Com tantos tipos de instância disponíveis, encontrar os tipos de instância mais adequados para sua workload pode ser demorado e complexo. Ao usar o assistente de seleção de tipo de instância do EC2, é possível se manter atualizado com os tipos de instância mais recentes e obter a melhor relação entre preço e desempenho para as workloads.

Este tópico descreve como obter sugestões e orientações para tipos de instância do EC2 por meio do console do Amazon EC2. Você também pode ir diretamente ao Amazon Q para obter conselhos sobre tipos de instância. Para obter mais informações, consulte o Guia do usuário do Amazon Q Developer.

Se você estiver procurando recomendações de tipo de instância para uma workload existente, use o AWS Compute Optimizer. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma workload existente.

Usar o assistente de seleção de tipo de instância do EC2

No console do Amazon EC2, é possível obter sugestões de tipo de instância no assistente de seleção de tipo de instância do EC2 no assistente de inicialização de instâncias ao criar um modelo de execução ou na página Tipos de instância.

Use as instruções apresentadas a seguir para obter sugestões e orientações para os tipos de instância do EC2 usando o assistente de seleção de tipo de instância do EC2 no console do Amazon EC2. Para visualizar uma animação dessas etapas, consulte Veja uma animação: como receber sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2.

Obter sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2

1. Inicie o processo ao usar qualquer um dos seguintes:

   - Siga o procedimento para iniciar uma instância. Ao lado de Tipo de instância, escolha o link Obter conselho.

- Siga o procedimento para criar um modelo de execução. Ao lado de Tipo de instância, escolha o link Obter conselho.
- No painel de navegação, escolha Tipos de instância e, em seguida, escolha o botão Assistente de seleção de tipo de instância.

2. Na tela Obter conselhos sobre a seleção do tipo de instância, faça o seguinte:

   a. Especifique os requisitos de tipo de instância ao selecionar opções para Tipo de workload, Caso de uso, Prioridade e Fabricantes de CPU.

   b. (Opcional) Para especificar requisitos mais detalhados para a workload, faça o seguinte:

      i. Expanda Parâmetros avançados.

      ii. Para adicionar um parâmetro, selecione um parâmetro, escolha Adicionar e especifique um valor para o parâmetro. Repita para cada parâmetro adicional que você deseja adicionar. Para não indicar um valor mínimo ou máximo, deixe o campo vazio.

      iii. Para remover um parâmetro após adicioná-lo, escolha o símbolo X ao lado do parâmetro.

   c. Escolha Obter conselho sobre tipo de instância.

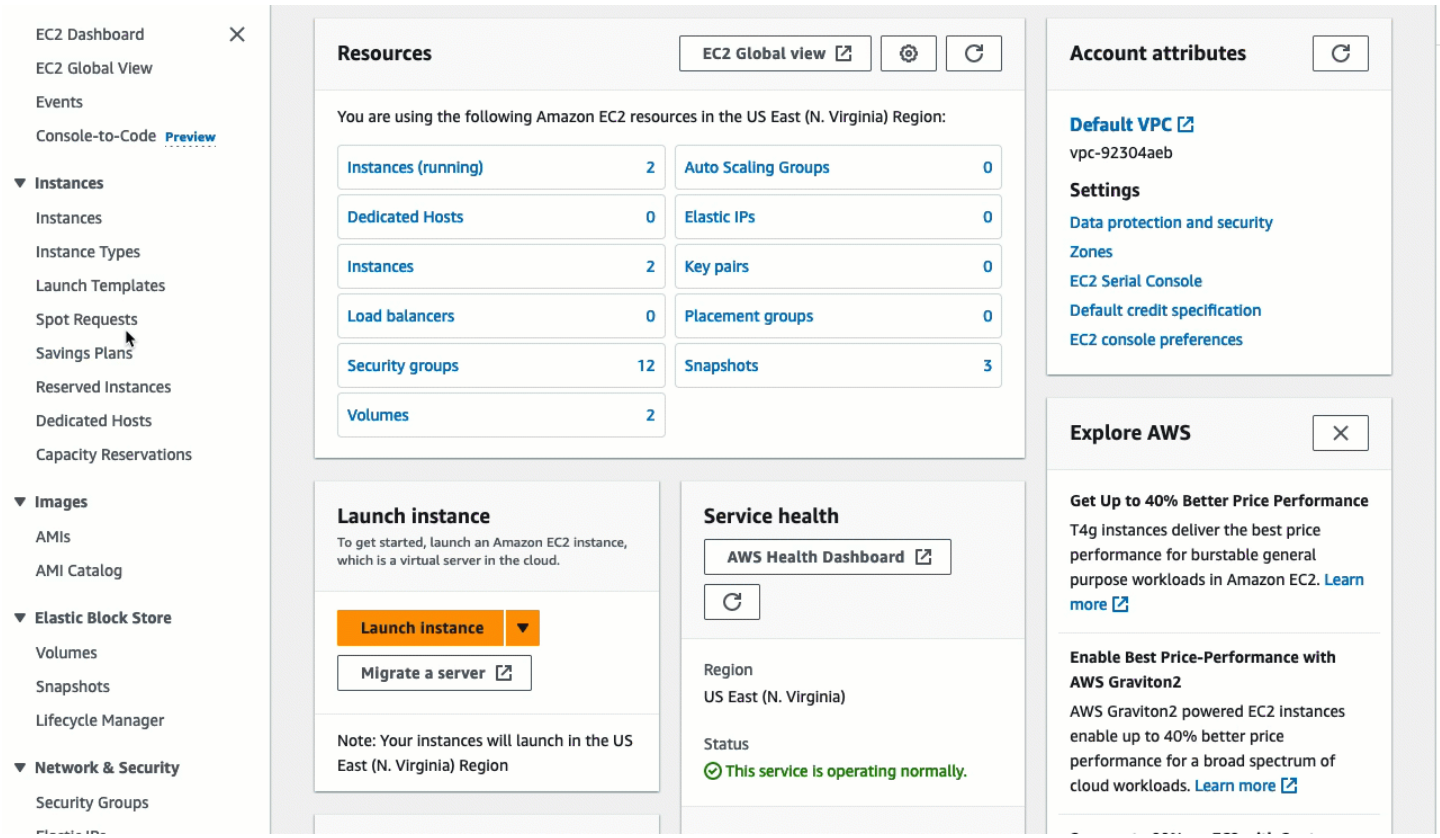
      O Amazon EC2 fornece sugestões de famílias de instâncias que atendem aos requisitos especificados.

3. Para visualizar os detalhes de cada tipo de instância nas famílias de instâncias sugeridas, escolha Exibir detalhes recomendados da família de instâncias.

4. Selecione um tipo de instância que atenda aos seus requisitos e escolha Ações e Iniciar instância ou Ações e Criar modelo de execução.

   Como alternativa, se você iniciou o processo no assistente de inicialização de instâncias ou na página do modelo de execução e prefere retornar para o fluxo original, faça uma anotação do tipo de instância que deseja usar. Em seguida, no assistente de inicialização de instâncias ou no modelo de execução, em Tipo de instância, escolha o tipo de instância e conclua o procedimento para iniciar uma instância ou criar um modelo de execução.

Veja uma animação: como receber sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2



Obter recomendações de tipo de instância para uma workload existente

O AWS Compute Optimizer fornece recomendações para instâncias do Amazon EC2 para ajudar a melhorar a performance, economizar dinheiro ou ambos. É possível usar essas recomendações para decidir se deseja passar para um novo tipo de instância.

Para fazer recomendações, o Compute Optimizer analisa as especificações de instância existentes e as métricas de utilização. Os dados compilados são usados para recomendar quais tipos de instância do Amazon EC2 são melhores para lidar com a workload existente. As recomendações são retornadas com a definição de preço de instância por hora.

Este tópico descreve como visualizar as recomendações por meio do console do Amazon EC2. Para obter mais informações, consulte o Guia do usuário do AWS Compute Optimizer.

> **Note**
>
> Para obter recomendações do Compute Optimizer, primeiro é necessário optar pelo Compute Optimizer. Para obter mais informações, consulte Conceitos básicos do AWS Compute Optimizer no Manual do usuário do AWS Compute Optimizer.

Se você estiver procurando recomendações de tipo de instância para uma nova workload, use o seletor de tipo de instância do EC2 Amazon Q. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma nova workload.

Conteúdo

- Limitações
- Descobertas
- Exibir recomendações
- Considerações para avaliação das recomendações
- Recursos adicionais

Limitações

Atualmente, o Compute Optimizer gera recomendações para os tipos de instância C, D, H, I, M, R, T, X e z. Outros tipos de instância não são considerados pelo Compute Optimizer. Se estiver usando outros tipos de instância, eles não serão listados na visualização de recomendações do Compute Optimizer. Para obter mais informações sobre os tipos de instâncias com suporte ou sem, consulte Requisitos de instâncias do Amazon EC2 no Guia do usuário do AWS Compute Optimizer.

Descobertas

O Compute Optimizer classifica suas descobertas para instâncias do EC2 da seguinte forma:

- Under-provisioned (Subprovisionada) – uma instância do EC2 será considerada subprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, não atender aos requisitos de performance de sua workload. Instâncias do EC2 subprovisionadas podem gerar performance ruim da aplicação.
- Over-provisioned (Superprovisionada) – uma instância do EC2 será considerada superprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, puder

ser reduzida sem deixar de atender aos requisitos de performance de sua workload e quando nenhuma especificação estiver subprovisionada. Instâncias do EC2 superprovisionadas podem gerar custos desnecessários de infraestrutura.

- Optimized (Otimizada) – uma instância do EC2 será considerada otimizada quando todas as especificações, como CPU, memória e rede, atenderem aos requisitos de performance de sua workload e a instância não estiver superprovisionada. Uma instância do EC2 otimizada executa suas workloads com performance e custo de infraestrutura ideais. Para instâncias otimizadas, o Compute Optimizer às vezes pode recomendar um tipo de instância de nova geração.
- None (Nenhum) – não há recomendações para essa instância. Isso pode ocorrer se você tiver optado pelo Compute Optimizer há menos de 12 horas, quando a instância estiver sendo executada há menos de 30 horas ou quando o tipo de instância não for compatível com o Compute Optimizer. Para obter mais informações, consulte Limitações na seção anterior.

Exibir recomendações

Depois de optar pelo Compute Optimizer, será possível visualizar as descobertas que Compute Optimizer gera para suas instâncias do EC2 no console do EC2. Depois, será possível acessar o console do Compute Optimizer para visualizar as recomendações. Caso tenha realizado a opção recentemente, as descobertas poderão não ser refletidas no console do EC2 durante até 12 horas.

Como visualizar uma recomendação para uma instância do EC2 por meio do console do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instâncias e, em seguida, escolha o ID da instância .
3. Na página de resumo da instância, no banner do AWS Compute Optimizer, próximo ao fim da página, escolha Visualizar detalhes.

   A instância será aberta no Compute Optimizer, onde ela será rotulada como a instância Current (Atual). Até três recomendações de tipo de instância diferentes, rotuladas como Option 1 (Opção 1), Option 2 (Opção 2) e Option 3 (Opção 3), serão fornecidas. A metade inferior da janela mostra dados recentes de métricas do CloudWatch para a instância atual: CPU utilization (Uso da CPU), Memory utilization (Uso da memória), Network in (Entrada da rede) e Network out (Saída da rede).
4. (Opcional) No console do Compute Optimizer, selecione o ícone de configurações () para alterar as colunas visíveis na tabela ou para visualizar as informações públicas de preços

com a finalidade de obter uma opção de aquisição diferente para os tipos de instância atuais e recomendados.

> **Note**
>
> Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.

Determine se deseja usar uma das recomendações. Decida se deseja otimizar para melhorar a performance, reduzir custos ou uma combinação dos dois. Para obter mais informações, consulte Exibição de recomendações de recursos no Guia do usuário do AWS Compute Optimizer.

Como visualizar as recomendações para todas as instâncias do EC2 em todas as regiões no console do Compute Optimizer

1. Abra o console do Compute Optimizer em https://console.aws.amazon.com/compute-optimizer/.
2. Escolha View recommendations for all EC2 instances (Visualizar recomendações para todas as instâncias do EC2).
3. É possível executar as seguintes ações na página de recomendações:

   a. Para filtrar recomendações para uma ou mais regiões da AWS, insira o nome da região na caixa de texto Filter by one or more Regions (Filtrar por uma ou mais regiões) ou escolha uma ou mais regiões na lista suspensa exibida.

   b. Para visualizar as recomendações para recursos em outra conta, escolha Account (Conta) e selecione um ID de conta diferente.

      Essa opção estará disponível somente se você estiver conectado a conta de gerenciamento de uma organização e tiver optado por todas as contas-membros da organização.

   c. Para limpar os filtros selecionados, escolha Clear filters (Limpar filtros).

   d. Para alterar a opção de aquisição que é exibida para os tipos de instância atuais e recomendados, selecione o ícone de configurações () e, em seguida, escolha Instâncias sob demanda, Instâncias reservadas, padrão de um ano sem pagamento adiantado ou Instâncias reservadas, padrão de três anos sem pagamento adiantado.

e. Para visualizar detalhes, como recomendações adicionais e uma comparação das métricas de utilização, escolha a descoberta (Under-provisioned (Subprovisionada), Over-provisioned (Superprovisionada) ou Optimized (Otimizada)) listada ao lado da instância desejada. Para obter mais informações, consulte Exibição de detalhes do recurso no Guia do usuário do AWS Compute Optimizer.

Considerações para avaliação das recomendações

Antes de alterar um tipo de instância, considere o seguinte:

- As recomendações não preveem seu uso. As recomendações são baseadas em seu histórico de uso durante os últimos 14 dias. Escolha um tipo de instância que tenha a expectativa de atender às suas necessidades futuras de recursos.
- Concentre-se nas métricas gráficas para determinar se o uso real é menor do que a capacidade da instância. Também é possível visualizar dados de métricas (média, pico, percentil) no CloudWatch para aprofundar a avaliação de suas recomendações de instâncias do EC2. Por exemplo, observe como as métricas de porcentagem da CPU mudam durante o dia e se há picos que precisem ser acomodados. Para obter mais informações, consulte Visualizar métricas disponíveis no Guia do usuário do Amazon CloudWatch.
- O Compute Optimizer pode fornecer recomendações para instâncias expansíveis, que são as instâncias T3, T3a e T2. Se você ultrapassa periodicamente a linha de base, verifique se poderá continuar a fazer isso com base nas vCPUs do novo tipo de instância. Para ter mais informações, consulte Principais conceitos e definições para instâncias expansíveis.
- Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.
- Considere conversões para instâncias da geração mais recente, sempre que possível.
- Ao migrar para uma família de instâncias diferente, verifique se o tipo de instância atual e o novo tipo de instância são compatíveis, por exemplo, em termos de virtualização, arquitetura ou tipo de rede. Para ter mais informações, consulte Compatibilidade para alterar o tipo de instância.
- Por fim, considere a classificação de risco de performance fornecida para cada recomendação. O risco de performance indica o esforço necessário para validar se o tipo de instância recomendado atende aos requisitos de performance da sua workload. Também recomendamos testes rigorosos de carga e performance antes e depois de fazer quaisquer alterações.

Há outras considerações ao redimensionar uma instância do EC2. Para ter mais informações, consulte Alterar o tipo de instância.

Recursos adicionais

Para obter mais informações:

- Tipos de instância do Amazon EC2
- Guia do usuário do AWS Compute Optimizer

Alterar o tipo de instância

À medida que suas necessidades mudarem, é possível descobrir que a instância está sobreutilizada (o tipo de instância é muito pequeno) ou subutilizada (o tipo de instância é muito grande). Se esse for o caso, será possível redimensionar a sua instância alterando o seu tipo de instância. Por exemplo, se a instância `t2.micro` for muito pequena para sua workload, é possível alterar o tamanho a para um tipo de instância T2 maior, como um `t2.large`. Ou é possível alterá-lo para outro tipo de instância, como `m5.large`. Também é possível migrar de um tipo de instância de uma geração anterior para um tipo de instância da geração atual para aproveitar alguns recursos, por exemplo, suporte para IPv6.

Se você quiser uma recomendação para um tipo de instância que esteja mais apto a lidar com sua workload existente, é possível usar o AWS Compute Optimizer. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma workload existente.

Ao alterar o tipo de instância, você começará a pagar a taxa do novo tipo de instância. Para obter as taxas sob demanda para todos os tipos de instância, consulte Preço sob demanda do Amazon EC2.

Para adicionar armazenamento extra à sua instância sem alterar o tipo de instância, adicione um volume do EBS à instância. Para obter mais informações, consulte Associar um volume do Amazon EBS a uma instância no Guia do usuário do Amazon EBS.

Quais as instruções a serem seguidas?

Existem instruções diferentes para alterar o tipo de instância. As instruções a serem usadas dependem do volume raiz da instância e se o tipo de instância é compatível com a configuração atual da instância. Para obter informações sobre como a compatibilidade é determinada, consulte Compatibilidade para alterar o tipo de instância.

Use a tabela a seguir para determinar quais instruções seguir.

Volume raiz	Compatibilidade	Siga estas instruções
EBS	Compatível	Alterar o tipo de instância de uma instância baseada no EBS
EBS	Não compatível	Alterar o tipo de instância com o início de uma nova instância
Armazenamento de instâncias	Não aplicável	Altere o tipo de instância de uma instância baseada em armazenamento de instâncias

Considerações sobre tipos de instância compatíveis

Considere o seguinte ao alterar o tipo de instância de uma instância existente:

- É necessário interromper sua instância com Amazon EBS para poder alterar o tipo de instância. Planeje tempo de inatividade enquanto a instância estiver parada. Interromper a instância e alterar o tipo de instância pode levar alguns minutos, e o tempo necessário para iniciar a instância pode variar dependendo dos scripts de startup da aplicação. Para ter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
- Quando você interrompe e inicia uma instância, nós movemos a instância para um novo hardware. Se sua instância tiver um endereço IPv4 público, nós liberamos o endereço e damos à instância um novo endereço IPv4 público. Se você precisar de um endereço IPv4 público que não seja alterado, use um endereço de IP elástico.
- Você não pode alterar o tipo de instância de uma instância spot.
- [Instâncias do Windows] Recomendamos atualizar o pacote de driver PV da AWS antes de alterar o tipo de instância. Para ter mais informações, consulte the section called “Atualizar drivers de PV”.
- Se sua instância estiver em um grupo do Auto Scaling, o serviço do Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para evitar isso, é possível suspender os processos de escalabilidade para o grupo enquanto estiver alterando o tipo de instância. Para obter mais informações, consulte Suspensão e retomada de um processo para um grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.
- Quando você altera o tipo de instância de uma instância com volumes de armazenamento de instâncias NVMe, a instância atualizada pode ter volumes adicionais de armazenamento, pois todos os volumes de armazenamento de instâncias NVMe estão disponíveis mesmo que não

estejam especificados na AMI ou no mapeamento de dispositivos de blocos de instâncias. Caso contrário, a instância atualizada tem o mesmo número de volumes de armazenamento de instância que você especificou ao iniciar a instância original.

- O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Não é possível mudar para um tipo ou tamanho de instância que não ofereça suporte ao número de volumes que já estão conectados à sua instância. Para ter mais informações, consulte Limites de volumes de instância.

Alterar o tipo de instância de uma instância baseada no EBS

Use as instruções a seguir para alterar o tipo de instância de uma instância baseada no EBS se o tipo de instância desejado for compatível com a configuração atual da instância.

Para alterar o tipo de instância de uma instância baseada no Amazon EBS

1. (Opcional) Se o tipo de instância requer drivers que não estejam instalados na instância atual, é necessário se conectar à sua instância e instalar os drivers primeiro. Para ter mais informações, consulte Compatibilidade para alterar o tipo de instância.
2. [Instâncias do Windows] Se você configurou a instância do Windows para usar o endereçamento IP estático e alterar de um tipo de instância que não é compatível com as redes aperfeiçoadas para um tipo de instância que é compatível com as redes aperfeiçoadas, você poderá receber um aviso sobre um possível conflito de endereço IP ao reconfigurar o endereçamento IP estático. Para evitar isso, habilite o DHCP na interface de rede da instância antes de alterar o tipo de instância. Na sua instância, abra a Network and Sharing Center (Central de rede e compartilhamento), vá para Internet Protocol Version 4 (TCP/IPv4) Properties (Propriedades do protocolo IP versão 4 (TCP/IPv4)) para a interface de rede e escolha Obtain an IP address automatically (Obter um endereço IP automaticamente). Altere o tipo de instância e reconfigure o endereçamento IP estático na interface de rede.
3. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
4. No painel de navegação, escolha Instances (Instâncias).
5. Selecione a instância e escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
6. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância). Essa ação ficará esmaecida se o estado da instância não for `stopped`.

7. Em Change Instance Type (Alterar tipo de instância), faça o seguinte:

   a. Em Instance type (Tipo de instância), selecione o tipo de instância desejado.

      Se o tipo de instância não estiver na lista, ele não é compatível com a configuração da sua instância. Em vez disso, use as seguintes instruções: Alterar o tipo de instância com o início de uma nova instância.

   b. (Opcional) Se o tipo de instância selecionado oferecer suporte à otimização para EBS, selecione EBS-optimized (Otimizado para EBS) ou desmarque a opção EBS-optimized (Otimizado para EBS) para desabilitar a otimização para EBS. Se, por padrão, o tipo de instância selecionado for otimizada para EBS, a opção EBS-optimized (Otimizada para EBS) estará selecionada e você não poderá desfazer a seleção.

   c. Escolha Apply para aceitar as novas configurações.

8. Para iniciar a instância, selecione a instância e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no estado `running`. Se a instância não iniciar, consulte Solucionar problemas de alteração de tipo de instância.

9. [Instâncias do Windows] Se a instância executar o Windows Server 2016 ou o Windows Server 2019 com EC2Launch v1, conecte-se à sua instância do Windows e execute o script do PowerShell para EC2Launch, apresentado a seguir, a fim de configurar a instância depois que o tipo de instância for alterado.

   > **Important**
   >
   > A senha do administrador será redefinida quando você habilitar o script de inicialização do EC2 da instância. É possível modificar o arquivo de configuração para desabilitar a redefinição da senha do administrador especificando-a nas configurações das tarefas de inicialização. Para obter as etapas para desabilitar a redefinição de senha, consulte Configure initialization tasks (EC2Launch) ou Change settings (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Alterar o tipo de instância com o início de uma nova instância

Se a configuração atual de instância baseada no EBS não for compatível com o novo tipo de instância desejado, você não poderá alterar o tipo de instância da instância original. Em vez disso, você deverá iniciar uma nova instância com uma configuração que seja compatível com o novo tipo de instância desejado e depois migrar sua aplicação para a nova instância. Por exemplo, se você iniciou a instância original usando uma AMI paravirtual (PV), mas deseja alterar para um tipo de instância de geração atual que requer uma AMI de máquina virtual de hardware (HVM), será necessário iniciar uma nova instância usando uma AMI de HVM. Para obter informações sobre como a compatibilidade é determinada, consulte Compatibilidade para alterar o tipo de instância.

Para migrar a aplicação para uma nova instância, faça o seguinte:

- Faça backup dos dados na sua instância original.
- Inicie uma nova instância com uma configuração que seja compatível com o novo tipo de instância desejado e anexe todos os volumes do EBS que estavam anexados à instância original.
- Instale a aplicação e qualquer software necessário na instância.
- Restaure todos os dados.
- Se a sua instância original tiver um endereço de IP elástico e você quiser garantir que os usuários possam continuar a usar as aplicações em sua nova instância sem interrupção, associe o endereço de IP elástico à nova instância. Para obter mais informações, consulte Endereço de IP elástico.

Para alterar o tipo de instância de uma nova configuração de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Faça backup dos dados que você precisar manter, da seguinte forma:
   - Para dados nos volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.
   - Para dados nos volumes do EBS, crie um snapshot dos volumes ou desassocie os volumes da instância para poder associá-los à nova instância mais tarde.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione Iniciar instâncias. Quando configurar as instâncias, faça o seguinte:
   a. Selecione uma AMI que suporte o tipo de instância desejado. Observe que os tipos de instância da geração atual requerem uma AMI de HVM.

b. Selecione o novo tipo de instância desejado. Se o tipo de instância desejado não estiver disponível, ele não é compatível com a configuração da AMI selecionada.

c. Se estiver usando um endereço de IP elástico, selecione a VPC na qual a instância original está sendo executada no momento.

d. Para permitir que algum tráfego atinja a nova instância, selecione o grupo de segurança que está associado à instância original.

e. Quando terminar de configurar sua nova instância, execute as etapas para selecionar um par de chaves e inicie sua instância. Pode demorar alguns minutos para que a instância entre no estado `running`.

5. Se necessário, anexe todos os novos volumes do EBS baseados nos snapshots que você criou ou todos os volumes do EBS que você desvinculou da instância original à nova instância.

6. Instale sua aplicação e o software necessário na nova instância.

7. Restaure todos os dados dos quais você fez backup dos volumes de armazenamento de instâncias da instância original.

8. Se estiver usando um endereço de IP elástico, atribua-o à instância recém-executada da seguinte forma:

   a. No painel de navegação, escolha Elastic IPs.

   b. Selecione o endereço IP elástico que está associado à instância original e escolha Actions (Ações) e Disassociate Elastic IP address (Desassociar endereço IP elástico). Quando a confirmação for solicitada, escolha Disassociate (Desassociar).

   c. Com o endereço IP elástico ainda selecionado, escolha Actions (Ações) e Associate Elastic IP address (Associar endereço IP elástico).

   d. Em Resource type (Tipo de recurso), escolha Instance (Instância).

   e. Em Instance (Instância), escolha a instância à qual associar o endereço de IP elástico.

   f. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.

   g. Escolha Associate.

9. (Opcional) É possível encerrar a instância original se ela não for mais necessária. Selecione a instância e confirme que está prestes a terminar a instância original e não a nova instância (por exemplo, confira o nome ou a hora do lançamento) e depois escolha Instance state (Estado da instância), Terminate instance (Terminar instância).

Compatibilidade para alterar o tipo de instância

Você só pode alterar o tipo de instância se a configuração atual da instância for compatível com tipo de instância desejado. Se o tipo de instância que você deseja não for compatível com a configuração atual da instância, é necessário iniciar uma nova instância com uma configuração que seja compatível com o tipo de instância e, em seguida, migrar sua aplicação para a nova instância.

[Instâncias do Linux] é possível usar o runbook `AWSSupport-MigrateXenToNitroLinux` para migrar instâncias do Linux compatíveis de um tipo de instância do Xen para um tipo de instância do Nitro. Para obter mais informações, consulte `AWSSupport-MigrateXenToNitroLinux runbook` na Referência do runbook do AWS Systems Manager Automation.

[Instâncias do Windows] Para obter orientações adicionais sobre a migração de instâncias do Windows compatíveis de um tipo de instância do Xen para um tipo de instância do Nitro, consulte Migrate to latest generation instance types.

A compatibilidade é determinada das seguintes maneiras:

Tipo de virtualização

As AMIs do Linux usam um dos dois tipos de virtualização: paravirtual (PV) ou máquina virtual de hardware (HVM). Se uma instância foi iniciada em uma AMI PV, você não poderá alterar para um tipo de instância que seja somente HVM. Para ter mais informações, consulte Tipos de virtualização de AMI. Para conferir o tipo de virtualização da instância, confira o valor do campo Virtualization (Virtualização) no painel de detalhes da tela Instances (Instâncias) no console do Amazon EC2.

Arquitetura

As AMIs são específicas da arquitetura do processador, portanto, é necessário selecionar um tipo de instância com a mesma arquitetura de processador que o tipo da instância atual. Por exemplo:

- Se o tipo de instância atual tiver um processador baseado na arquitetura Arm, você estará limitado aos tipos de instância que oferecem suporte a um processador baseado na arquitetura Arm, como o C6g e M6g.
- Os seguintes tipos de instância são os únicos tipos de instância que oferecem suporte a AMIs de 32 bits: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` e `c1.medium`. Se estiver alterando o tipo de instância de uma instância de 32 bits, você estará limitado a esses tipos de instância.

Adaptadores de rede

Se você alternar de um driver de um adaptador de rede para outro, as configurações do adaptador de rede serão redefinidas quando o sistema operacional criar o novo adaptador. Para redefinir as configurações, talvez seja necessário ter acesso a uma conta local com permissões de administrador. Veja a seguir exemplos de mudança de um adaptador de rede para outro:

- AWS PV (instâncias T2) para Intel 82599 VF (instâncias M4)
- Intel 82599 VF (maioria das instâncias M4) para ENA (instâncias M5)
- ENA (instâncias M5) para ENA de alta largura de banda (instâncias M5n)

Placas de rede

Alguns tipos de instância oferecem suporte a várias placas de rede. É necessário selecionar um tipo de instância que ofereça suporte ao mesmo número de placas de rede que o tipo de instância atual.

Redes avançadas

Tipos de instância que oferecem suporte a redes avançadas exigem que os drivers necessários estejam instalados. Por exemplo, as instâncias desenvolvidas no AWS Nitro System requerem AMIs baseadas no EBS com os drivers do Adaptador de Rede Elástica (ENA) instalados. Para alterar de um tipo de instância sem suporte para redes avançadas para um tipo com suporte para redes avançadas, é necessário instalar os drivers ENA ou os drivers ixgbevf na instância, conforme apropriado.

> **Note**
>
> Quando você redimensiona uma instância com o ENA Express habilitado, o novo tipo de instância também deve ser compatível com o ENA Express. Para obter uma lista dos tipos de instâncias compatíveis com o ENA Express, consulte Tipos de instâncias compatíveis com o ENA Express.
> Para alterar de um tipo de instância compatível com o ENA Express para um tipo de instância não compatível com o ENA Express, certifique-se de que o ENA Express não esteja habilitado antes de você redimensionar a instância.

NVMe

Os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias desenvolvidas no AWS Nitro System. Se você alterar de um tipo de instância sem suporte para

NVMe para um tipo de instância com suporte para NVMe, deverá primeiro instalar os drivers NVMe na sua instância. Além disso, os nomes dos dispositivos para os dispositivos especificados no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivos NVMe (`/dev/nvme[0-26]n1`).

[Instâncias do Linux] Portanto, para a montagem de sistemas de arquivos no momento da inicialização usando `/etc/fstab`, você deve utilizar um UUID, ou um rótulo, em vez de nomes de dispositivos.

Limites de volumes

O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para ter mais informações, consulte Limites de volumes de instância.

Só é possível mudar para um tipo ou tamanho de instância que ofereça suporte ao mesmo número ou a um número maior de volumes do que os anexados à instância no momento. Se você mudar para um tipo ou tamanho de instância que não ofereça suporte ao número de volumes anexados no momento, a solicitação falhará. Por exemplo, se você mudar de uma instância `m7i.4xlarge` com 32 volumes anexados para uma instância `m6i.4xlarge` compatível com um máximo de 27 volumes, a solicitação falhará.

Solucionar problemas de alteração de tipo de instância

Use as informações a seguir para ajudar a diagnosticar e corrigir os problemas que podem ocorrer com a alteração do tipo de instância.

A instância não inicia após a alteração do tipo de instância

Causa possível: requisitos de novo tipo de instância não atendidos

Se a sua instância não inicializar, é possível que um dos requisitos de novo tipo de instância não tenha sido atendido. Para obter mais informações, consulte Por que minha instância do Linux não está inicializando depois que mudei seu tipo?

Causa possível: a AMI não oferece suporte para o tipo de instância

Se você usar o console do EC2 para alterar o tipo de instância, somente os tipos de instância com suporte pela AMI selecionada estarão disponíveis. Porém, se você usar a AWS CLI para iniciar uma instância, é possível especificar uma AMI e um tipo de instância incompatíveis. Se a

AMI e o tipo de instância forem incompatíveis, a instância não poderá ser iniciada. Para ter mais informações, consulte Compatibilidade para alterar o tipo de instância.

Causa possível: a instância está no grupo de posicionamento de cluster

Se sua instância estiver em um grupo de posicionamento de cluster e, após a alteração do tipo de instância, a instância não iniciar, tente o seguinte:

1. Interrompa todas as instâncias no grupo de posicionamento de cluster.
2. Altere o tipo de instância da instância afetada.
3. Inicie todas as instâncias no grupo de posicionamento de cluster.

Aplicação ou site não acessíveis na Internet após a alteração do tipo de instância

Causa possível: o endereço IPv4 público foi liberado

Quando altera o tipo de instância, primeiro é necessário interromper a instância. Quando você interrompe uma instância, liberamos o endereço IPv4 público e fornecemos a sua instância um novo endereço IPv4 público.

Para reter o endereço IPv4 público entre as interrupções e inicializações da instância, recomendamos que você use um endereço de IP elástico, sem nenhum custo extra, desde que sua instância esteja em execução. Para ter mais informações, consulte Endereços IP elásticos.

Altere o tipo de instância de uma instância baseada em armazenamento de instâncias

Uma instância baseada em armazenamento de instâncias é uma instância com um volume raiz de armazenamento de instâncias. Você não pode alterar o tipo de instância de uma instância que tem um volume raiz de armazenamento de instâncias. Em vez disso, crie uma AMI da instância, iniciar uma nova instância nessa AMI e selecionar o tipo de instância desejado, depois migrar suas aplicação para a nova instância. Observe que o tipo de instância desejado deve ser compatível com a AMI que você criou. Para obter informações sobre como a compatibilidade é determinada, consulte Compatibilidade para alterar o tipo de instância.

Visão geral do processo

- Faça backup dos dados na sua instância original.
- Crie uma AMI a partir da sua instância original.
- Inicie uma nova instância nessa AMI e selecione o tipo de instância desejado.

- Instale sua aplicação na nova instância.
- Se a sua instância original tiver um endereço de IP elástico e você quiser garantir que os usuários possam continuar a usar as aplicações em sua nova instância sem interrupção, associe o endereço de IP elástico à nova instância. Para obter mais informações, consulte Endereço de IP elástico.

Para alterar o tipo de instância de uma instância baseada em armazenamento de instâncias

1. Faça backup dos dados que você precisar manter, da seguinte forma:
   - Para dados nos volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.
   - Para dados nos seus volumes do EBS, crie um snapshot dos volumes ou desvincule o volume da instância para poder anexá-lo à nova instância mais tarde.
2. Crie uma AMI da instância atendendo aos pré-requisitos e seguindo os procedimentos em Criar uma AMI em Linux com armazenamento de instâncias. Ao concluir a criação de uma AMI de sua instância, retorne para esse procedimento.
3. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
4. No painel de navegação, selecione AMIs. Na lista de filtros, selecione Owned by me (De minha propriedade) e selecione a imagem que você criou na etapa 2. Observe que o AMI Name (Nome da AMI) é o nome que você especificou quando registrou a imagem e Source (Origem) é seu bucket do Amazon S3.

   > **Note**
   >
   > Se você não vir a AMI que criou na etapa 2, verifique se selecionou a região na qual criou a AMI.

5. Com a AMI selecionada, escolha Launch instance from image (Iniciar instância a partir da imagem). Quando configurar as instâncias, faça o seguinte:
   a. Selecione o novo tipo de instância desejado. Se o tipo de instância desejado não estiver disponível, ele não é compatível com a configuração da AMI criada. Para ter mais informações, consulte Compatibilidade para alterar o tipo de instância.
   b. Se estiver usando um endereço de IP elástico, selecione a VPC na qual a instância original está sendo executada no momento.

c. Para permitir que algum tráfego atinja a nova instância, selecione o grupo de segurança que está associado à instância original.

d. Quando terminar de configurar sua nova instância, execute as etapas para selecionar um par de chaves e inicie sua instância. Pode demorar alguns minutos para que a instância entre no estado `running`.

6. Se necessário, anexe todos os novos volumes do EBS baseados nos snapshots que você criou ou todos os volumes do EBS que você desvinculou da instância original à nova instância.
7. Instale sua aplicação e o software necessário na nova instância.
8. Se estiver usando um endereço de IP elástico, atribua-o à instância recém-executada da seguinte forma:

   a. No painel de navegação, escolha Elastic IPs.

   b. Selecione o endereço IP elástico que está associado à instância original e escolha Actions (Ações) e Disassociate Elastic IP address (Desassociar endereço IP elástico). Quando a confirmação for solicitada, escolha Disassociate (Desassociar).

   c. Com o endereço IP elástico ainda selecionado, escolha Actions (Ações) e Associate Elastic IP address (Associar endereço IP elástico).

   d. Em Resource type (Tipo de recurso), escolha Instance (Instância).

   e. Em Instance (Instância), escolha a instância à qual associar o endereço de IP elástico.

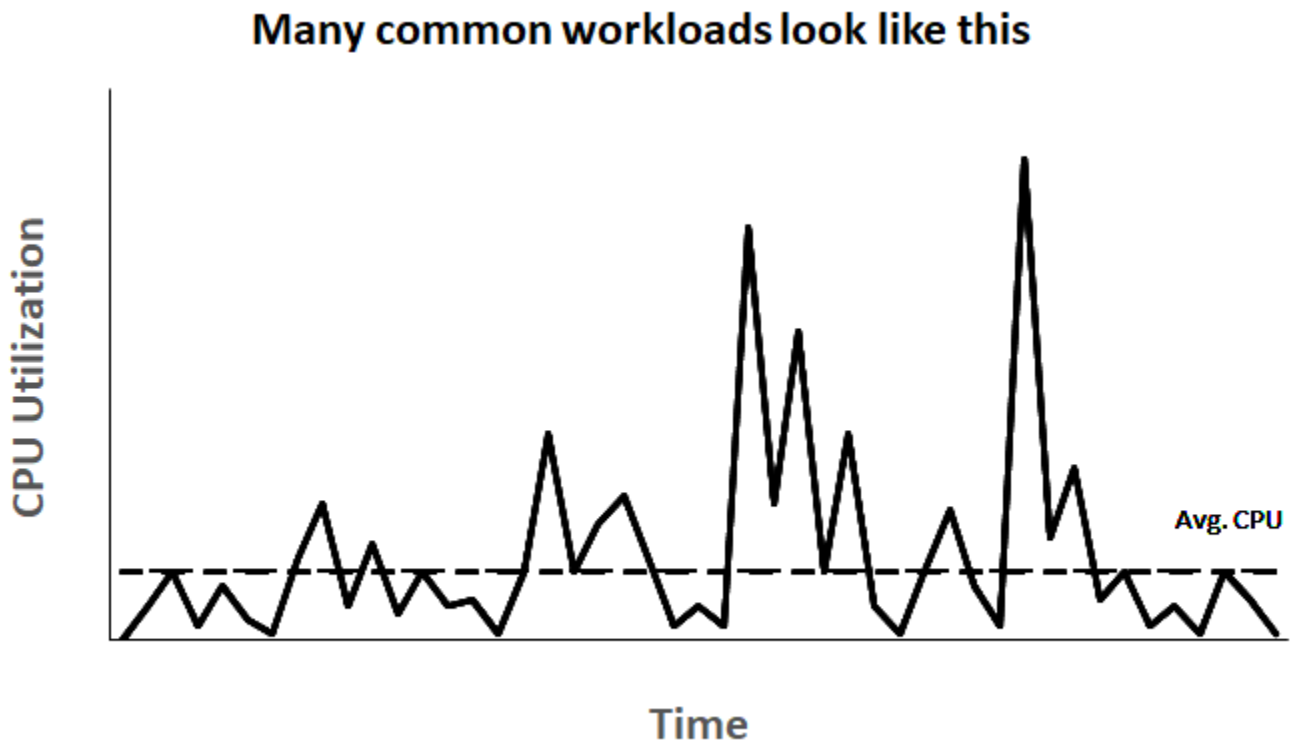
   f. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.

   g. Escolha Associate.

9. (Opcional) É possível encerrar a instância original se ela não for mais necessária. Selecione a instância e confirme que está prestes a terminar a instância original e não a nova instância (por exemplo, confira o nome ou a hora do lançamento) e depois escolha Instance state (Estado da instância), Terminate instance (Terminar instância).

Instâncias expansíveis

Muitas workloads de uso geral não estão, em média, ocupadas e não exigem alto nível de performance da CPU sustentada. O gráfico a seguir ilustra a utilização da CPU para muitas workloads comuns executadas por clientes na Nuvem AWS hoje.



Essas workloads de utilização de CPU de baixa a moderada causam desperdício de ciclos de CPU e, consequentemente, você paga por mais do que usa. Para superar isso, é possível aproveitar as instâncias de uso geral expansíveis com baixo custo, que são as instâncias T.

A família de instâncias T fornece performance de CPU de linha de base com capacidade de expansão acima da linha de base a qualquer momento, pelo tempo que for necessário. A CPU de linha de base é definida para atender às necessidades da maioria das workloads de uso geral, inclusive microsserviços de grande escala, servidores Web, bancos de dados pequenos e médios, registro em log de dados, repositórios de código, desktops virtuais, ambientes de desenvolvimento e teste e aplicações essenciais aos negócios. As instâncias T oferecem um equilíbrio de recursos de computação, memória e rede e fornecem a maneira mais econômica de executar um amplo espectro de aplicações de uso geral que têm uso de CPU de baixo a moderado. Podem economizar até 15% em custos, quando comparadas às instâncias M, e podem gerar ainda mais economia com tamanhos de instância menores e mais econômicas, oferecendo até 2 vCPUs e 0,5 GiB de memória. Os tamanhos de instância T menores, como nano, micro, pequeno e médio, são adequados para workloads que precisam de uma pequena quantidade de memória e não esperam alto uso da CPU.

> **Note**
>
> Este tópico descreve a CPU intermitente. Para obter mais informações sobre performance de rede intermitente, consulte Largura de banda de rede de instâncias do Amazon EC2.

Tipos de instância do EC2 expansíveis

As instâncias do EC2 expansíveis consistem em tipos de instância T4g, T3a e T3 e nos tipos de instância T2 da geração anterior.

Os tipos de instância T4g são a geração mais recente de instâncias expansíveis. Fornecem o melhor preço por performance e o menor custo entre todos os tipos de instância do EC2. Os tipos de instância T4g são alimentados por processadores AWS Graviton2 baseados em Arm com amplo suporte ao ecossistema de fornecedores de sistemas operacionais, fornecedores de software independentes e serviços e aplicações da AWS.

A tabela a seguir resume as principais diferenças entre os tipos de instância expansível.

Type	Descrição	Família de processadores
Última geração		
T4g	Tipo de instância do EC2 de menor custo com relação preço/performance até 40% mais alta e custos 20% menores em relação às T3	Processadores AWS Graviton2 com núcleos Arm Neoverse N1
T3a	Instâncias baseadas em x86 de menor custo com custos 10% mais baixos em relação às instâncias T3	Processadores AMD EPYC de 1.ª geração
T3	Melhor relação preço/per formance de pico para workloads x86 com preço/per formance até 30% mais baixos	Intel Xeon escalável (processa dores Skylake, Cascade Lake)

Type	Descrição	Família de processadores
	em relação às instâncias T2 da geração anterior	
Geração anterior		
T2	Instâncias expansíveis da geração anterior	Processadores Intel Xeon

Para obter informações sobre o preço de instâncias e outras especificações, consulte Preços do Amazon EC2 e Tipos de instância do Amazon EC2. Para obter mais informações sobre performance de rede intermitente, consulte Largura de banda de rede de instâncias do Amazon EC2.

Se sua conta tiver menos de 12 meses de vida, será possível usar uma instância `t2.micro` gratuitamente (ou uma instância `t3.micro` em regiões em que `t2.micro` estiver indisponível) em determinados limites de uso. Para obter mais informações, consulte Nível gratuito da AWS.

Opções de compra compatíveis com instâncias T

- On-Demand Instances
- Reserved Instances
- Instâncias dedicadas (apenas T3)
- Hosts dedicados (apenas T3, apenas no modo `standard`)
- Instâncias spot

Para ter mais informações, consulte Opções de compra de instância.

Tópicos

- Práticas recomendadas
- Principais conceitos e definições para instâncias expansíveis
- Modo ilimitado de instâncias expansíveis
- Modo padrão de instâncias expansíveis
- Trabalhar com instâncias expansíveis
- Monitore seus créditos da CPU para instâncias expansíveis

Práticas recomendadas

Siga estas melhores práticas para obter o benefício máximo com as instâncias expansíveis.

- Verifique se o tamanho da instância escolhido ultrapassa os requisitos mínimos de memória do sistema operacional e das aplicações. Os sistemas operacionais com interfaces gráficas de usuário que consomem memória e recursos de CPU significativos (por exemplo, o Windows) podem exigir um tamanho de instância `t3.micro`, ou maior, para muitos casos de uso. À medida que os requisitos de memória e de CPU de sua workload aumentam, você tem a flexibilidade nas instâncias T para escalar para tamanhos de instâncias maiores do mesmo tipo ou selecionar outro tipo de instância.
- Habilite o AWS Compute Optimizer para sua conta e verifique as recomendações do Compute Optimizer para sua workload. O Compute Optimizer pode ajudar a avaliar se as instâncias devem ser ampliadas para melhorar a performance ou reduzidas para economizar custos. O Compute Optimizer também pode recomendar um tipo de instância diferente com base no cenário. Para obter mais informações, consulte Visualizar recomendações de instância do EC2 no Guia do usuário do AWS Compute Optimizer.

Principais conceitos e definições para instâncias expansíveis

Os tipos de instância do Amazon EC2 tradicionais fornecem recursos fixos de CPU, enquanto as instâncias expansíveis fornecem um nível de linha de base de uso de CPU com capacidade para expandir o uso de CPU acima desse nível da linha de base. Isso garante que você pague somente pela CPU de linha de base, além dos usos adicionais de CPU de expansão, resultando em custos de computação mais baixos. O uso de linha de base e a capacidade de expansão são governados por créditos de CPU. As instâncias expansíveis são os únicos tipos de instância que usam créditos para uso de CPU.

Cada instância expansível ganha créditos continuamente quando permanece abaixo da linha de base da CPU e gasta créditos continuamente quando expande acima da linha de base. A quantidade de créditos obtidos ou gastos depende do uso da CPU da instância:

- Se a utilização da CPU for maior do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.
- Se a utilização da CPU for igual à linha de base, os créditos obtidos serão iguais aos créditos gastos.

- Se a utilização da CPU for maior do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.

Quando os créditos obtidos são maiores do que os créditos gastos, a diferença é chamada de créditos acumulados, que podem ser usados posteriormente para expandir acima da utilização da CPU de linha de base. Da mesma forma, quando os créditos gastos são maiores do que créditos obtidos, o comportamento da instância depende do modo de configuração de crédito (modo padrão ou modo ilimitado).

No modo padrão, quando os créditos gastos são maiores do que os créditos obtidos, a instância usa os créditos acumulados para expandir acima da utilização da CPU de linha de base. Se não houver mais créditos acumulados, a instância se reduzirá gradualmente à utilização da CPU de linha de base e não poderá expandir acima da linha de base até acumular mais créditos.

No modo ilimitado, se a instância expandir acima da utilização da CPU de linha de base, a instância usará primeiro os créditos acumulados para expandir. Se não houver mais créditos acumulados, a instância gastará créditos excedentes para expandir. Quando sua utilização de CPU ficar abaixo da linha de base, ela usará os créditos de CPU que ela ganhar para pagar os créditos excedentes gastos anteriormente. A capacidade de ganhar créditos de CPU para pagar créditos excedentes permite que o Amazon EC2 mantenha a média de utilização de CPU de uma instância em um período de 24 horas. Se o uso médio da CPU durante um período de 24 horas exceder a lista de referência, a instância será cobrada pelo uso adicional em uma taxa adicional fixa por hora de vCPU.

Conteúdo

- Principais conceitos e definições
- Ganhe créditos de CPU
- Taxa de ganhos de créditos de CPU
- Limite de acúmulo de créditos de CPU
- Duração dos créditos de CPU acumulados
- Utilização da linha de base

Principais conceitos e definições

Os principais conceitos e definições a seguir são aplicáveis a instâncias expansíveis.

Utilização da CPU

Utilização de CPU é o percentual de unidades de processamento EC2 alocadas que estão em uso na instância no momento. Essa métrica mede a porcentagem de ciclos de CPU alocados que estão sendo utilizados em uma instância. A métrica CPU Utilization do CloudWatch mostra o uso da CPU por instância e não o uso da CPU por núcleo. A especificação de CPU de linha de base de uma instância também se baseia no uso da CPU por instância. Para medir a utilização da CPU usando o AWS Management Console ou a AWS CLI, consulte Obter estatísticas para uma instância específica.

Crédito da CPU

Uma unidade de VCPU-time.

Exemplos:

1 crédito de CPU = 1 vCPU * 100% de utilização * 1 minuto.

1 crédito de CPU = 1 vCPU * 50% de utilização * 2 minutos

1 crédito de CPU = 2 vCPUs * 25% de utilização * 2 minutos

Utilização da linha de base

A utilização da lista de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido igual a zero, quando o número de créditos de CPU obtidos correspondem ao número de créditos de CPU usados. A utilização da linha de base também é conhecida como a linha de base. A utilização de linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma: % da utilização de referência = (número de créditos ganhos/número de vCPUs)/60 minutos.

Para a utilização de linha de base de cada tipo de instância expansível, consulte a tabela de crédito.

Créditos ganhos

Créditos obtidos continuamente por uma instância quando ela está em execução.

Número de créditos ganhos por hora = % de utilização da linha de base * número de vCPUs * 60 minutos

Exemplo:

Um t3.nano com 2 vCPUs e utilização de linha de base de 5% ganha 6 créditos por hora, calculados da seguinte forma:

2 vCPUs * 5% da linha de base * 60 minutos = 6 créditos por hora

Créditos gastos ou usados

Créditos usados continuamente por uma instância quando ela está em execução.

Créditos de CPU gastos por minuto = Número de vCPUs * utilização da CPU * 1 minuto

Créditos acumulados

Créditos de CPU que não são gastos quando uma instância usa menos créditos do que o necessário para a utilização da linha de base. Em outras palavras, créditos acumulados = (Créditos obtidos - Créditos usados) abaixo da linha de base.

Exemplo:

Se um t3.nano estiver sendo executado com 2% de utilização da CPU, que está abaixo de sua linha de base de 5% por uma hora, os créditos acumulados serão calculados da seguinte forma:

Créditos de CPU acumulados = (Créditos obtidos por hora - Créditos usados por hora) = 6 - 2 vCPUs * 2% de utilização da CPU * 60 minutos = 6 - 2,4 = 3,6 créditos acumulados por hora

Limite de acúmulo de créditos

Depende do tamanho da instância, mas em geral é igual ao número máximo de créditos obtidos em 24 horas.

Exemplo:

Para t3.nano, o limite de crédito acumulado = 24 * 6 = 144 créditos

Créditos de execução

Aplicável somente a instâncias T2 configuradas para o modo padrão. Os créditos de inicialização são um número limitado de créditos de CPU alocados para uma nova instância T2, de modo que, quando iniciada no modo padrão, possa expandir acima da linha de base.

Créditos excedentes

Créditos que são gastos por uma instância após esgotar o saldo de crédito acumulado. Os créditos excedentes são projetados para instâncias expansíveis para sustentar alta performance por um longo período e são usados somente no modo ilimitado. O saldo de créditos excedentes

é usado para determinar quantos créditos foram usados pela instância para expandir no modo ilimitado.

Modo padrão

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, gastando créditos acumulados no saldo de crédito.

Modo ilimitado

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, sustentando alta utilização da CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor. Se a instância for executada com maior utilização de CPU por um período prolongado, ela poderá fazê-lo por uma taxa adicional uniforme por hora de vCPU.

A tabela a seguir resume as principais diferenças de crédito entre os tipos de instância expansível.

Type	Tipo de créditos de CPU compatíveis	Modos de configuração de crédito	Vida útil de créditos de CPU acumulados entre a inicialização e a interrupção da instância
Última geração			
T4g	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
T3a	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedente	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)

Type	Tipo de créditos de CPU compatíveis	Modos de configuração de crédito	Vida útil de créditos de CPU acumulados entre a inicialização e a interrupção da instância
	s (somente no modo ilimitado)		
T3	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
Geração anterior			
T2	Créditos obtidos, créditos acumulados, Créditos gastos, créditos de inicialização (somente no modo padrão), créditos excedentes (somente no modo ilimitado)	Standard (padrão), ilimitado	0 dias (os créditos são perdidos quando uma instância é interrompida)

> **Note**
>
> O modo ilimitado não é compatível com instâncias T3 que são iniciadas em um host dedicado.

Ganhe créditos de CPU

Cada instância expansível ganha continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, de acordo com o tamanho da instância. O processo de

contabilidade de se os créditos são acumulados ou gastos também ocorre em uma resolução em nível de milissegundo, portanto, você não precisa se preocupar com gastos excessivos de créditos de CPU. Uma expansão curta da CPU usa uma pequena fração de um crédito de CPU.

Se uma instância expansível usar menos recursos de CPU do que o necessário para o uso de linha de base (como, por exemplo, quando está inativa), os créditos de CPU não gastos serão acumulados no saldo de créditos de CPU. Se uma instância expansível precisar de expansão acima do nível do uso da linha de base, ela gastará os créditos acumulados. Quanto mais créditos a instância expansível acumular, mais tempo de expansão ela poderá ter acima da linha de base quando mais uso de CPU for necessário.

A tabela a seguir lista os tipos de instância expansível, a taxa na qual os créditos de CPU são ganhos por hora, o número máximo de créditos de CPU ganhos que uma instância pode acumular, o número de vCPUs por instância e o uso da linha de base como uma porcentagem do total de um núcleo (usando uma única vCPU).

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* O número de créditos que podem ser acumulados é equivalente ao número de créditos que podem ser obtidos em um período de 24 horas.

**A porcentagem de utilização da linha de base na tabela é por vCPU. Em CloudWatch, a utilização da CPU é exibida por vCPU. Por exemplo, a utilização de CPU para uma instância `t3.large` que opera no nível de linha de base é mostrada como 30% nas métricas de CPU do CloudWatch. Para obter informações sobre como calcular a utilização da linha de base, consulte Utilização da linha de base.

*** Cada vCPU é uma thread de um núcleo Intel Xeon ou de um núcleo AMD EPYC, exceto para instâncias T2 e T4g.

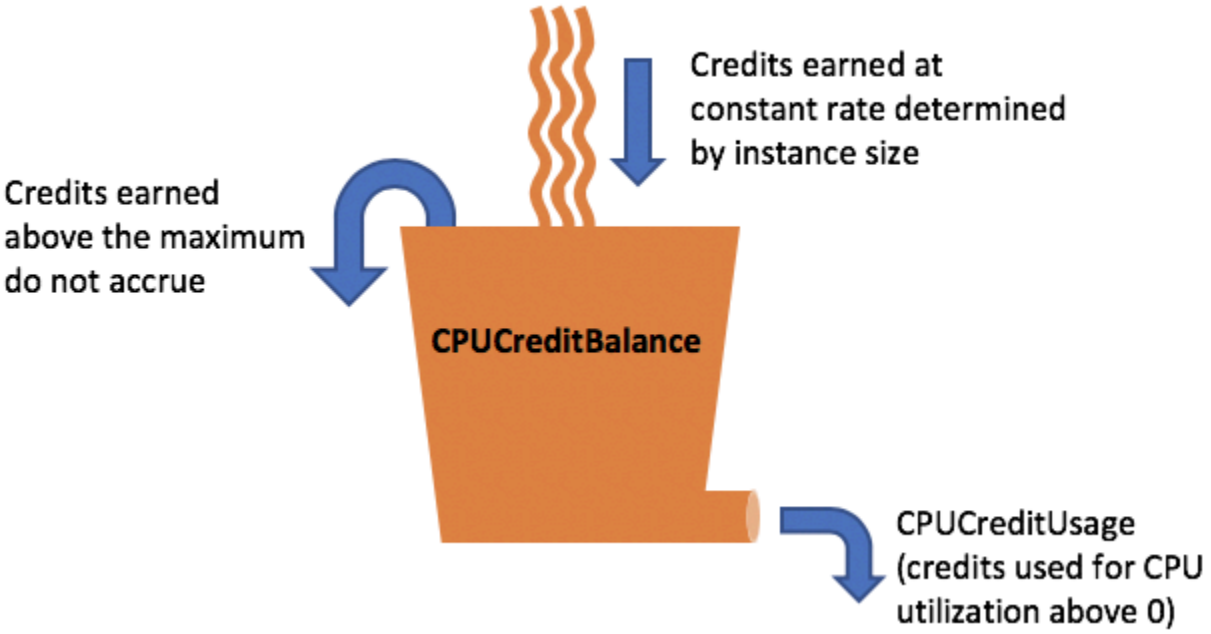
Taxa de ganhos de créditos de CPU

O número de créditos de CPU ganhos por hora é determinado pelo tamanho da instância. Por exemplo, `t3.nano` ganha seis créditos por hora, enquanto `t3.small` ganha 24 créditos por hora. A tabela anterior lista a taxa de ganhos de crédito de todas as instâncias.

Limite de acúmulo de créditos de CPU

Embora os créditos obtidos nunca expirem em uma instância em execução, há um limite para o número de créditos obtidos que uma instância pode acumular. O limite é determinado pelo limite de saldo de créditos de CPU. Após o limite ser atingido, todos os créditos novos que foram ganhos

serão rejeitados, como indicado na imagem a seguir. O bucket completo indica o limite de saldo de créditos de CPU, e o spillover indica os créditos ganhos recentemente que excedem o limite.



O limite de saldo de créditos de CPU difere para cada tamanho de instância de Por exemplo, uma instância `t3.micro` pode acumular no máximo 288 créditos no saldo de créditos de CPU. A tabela anterior lista o número máximo de créditos ganhos que cada instância pode acumular.

As instâncias T2 padrão também ganham créditos de execução. Os créditos de execução não são contabilizados para o limite de sado de créditos de CPU. Se uma instância T2 não gastar os créditos de execução e permanecer ociosa por um período de 24 horas, acumulando os créditos obtidos, seu saldo de créditos de CPU serão exibidos como acima do limite. Para obter mais informações, consulte Créditos de execução.

As instâncias T4g, T3a e T3 não ganham créditos de inicialização. Essas instâncias são executadas como `unlimited` por padrão e, portanto, podem apresentar expansão imediatamente desde o início, sem nenhum crédito de execução. Instâncias T3 iniciadas em um lançamento de host dedicado como `standard` por padrão; o modo `unlimited` não é compatível com instâncias T3 em um host dedicado.

Duração dos créditos de CPU acumulados

Os créditos de CPU de uma instância em execução não expiram.

Para T2, o saldo de créditos de CPU não persiste entre interrupções e inicializações da instância. Se você interromper uma instância T2, a instância perderá todos os créditos acumulados.

Para T4g, T3a e T3, o saldo de créditos de CPU persiste durante sete dias após uma instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

Para obter mais informações, consulte `CPUCreditBalance` na Tabela de métricas do CloudWatch.

Utilização da linha de base

A utilização da lista de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido igual a zero, quando o número de créditos de CPU obtidos correspondem ao número de créditos de CPU usados. A utilização da linha de base também é conhecida como a linha de base.

A utilização da linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma:

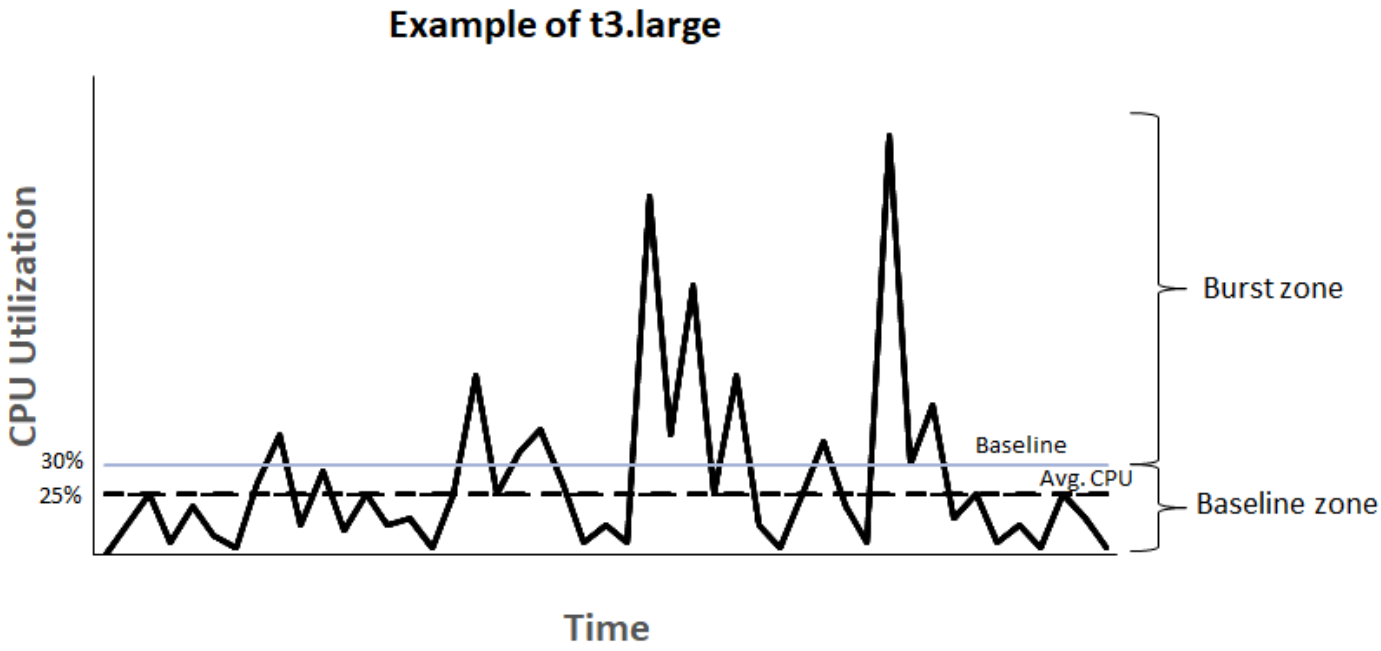
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline utilization
```

Por exemplo, uma instância `t3.nano`, com 2 vCPUs, ganha 6 créditos por hora, resultando em uma utilização de linha de base de 5%, que é calculada da seguinte forma:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Uma instância `t3.large`, com 2 vCPUs, ganha 36 créditos por hora, resultando em uma utilização básica de 30% (`(36/2)/60`).

O gráfico a seguir fornece um exemplo de `t3.large` com utilização média da CPU abaixo da linha de base.



Modo ilimitado de instâncias expansíveis

Uma instância expansível configurada como `unlimited` pode sustentar alta utilização de CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor.

Na grande maioria das workloads de uso geral, as instâncias configuradas como `unlimited` fornecem uma performance ampla sem encargos adicionais. Se a instância funcionar com maior utilização de CPU por um período prolongado, ela poderá fazer isso por uma taxa adicional uniforme por hora de vCPU. Para obter informações sobre preços, consulte a definição de preço do Amazon EC2 e definição de preço do modo ilimitado T2/T3/T4.

Se você usar uma instância `t2.micro` ou `t3.micro` na oferta de Nível gratuito da AWS e usá-la no modo `unlimited`, poderão ser aplicados encargos se a sua utilização média durante um período contínuo de 24 horas exceder a utilização de linha de base da instância.

As instâncias T4g, T3a e T3 são iniciadas como `unlimited` por padrão (a menos que você altere o padrão). Se a média de uso de CPU em um período de 24 horas exceder a linha de base, você incorrerá em cobranças por créditos excedentes. Se você executar Instâncias spot como `unlimited` e planejar usá-las imediatamente e por um curto período, sem tempo ocioso

para acumular créditos de CPU, serão cobrados créditos excedentes. Recomendamos iniciar as instâncias spot no modo padrão para evitar custos mais altos. Para ter mais informações, consulte Os créditos excedentes podem gerar cobranças e Instâncias expansíveis.

> **Note**
>
> Instâncias T3 iniciadas em um lançamento de host dedicado como `standard` por padrão; o modo `unlimited` não é compatível com instâncias T3 em um host dedicado.

Conteúdo

- Conceitos do modo ilimitado
  - Como funcionam as instâncias expansíveis
  - Quando usar o modo ilimitado versus CPU fixa
  - Os créditos excedentes podem gerar cobranças
  - Nenhum crédito de execução para T2 ilimitada
  - Ativar modo ilimitado
  - O que acontece com os créditos quando é feita alternância de ilimitada para padrão
  - Monitorar uso de crédito
- Exemplos de modo ilimitado
  - Exemplo 1: explicar o uso de créditos com T3 ilimitada
  - Exemplo 2: explicar o uso de créditos com T2 ilimitada

Conceitos do modo ilimitado

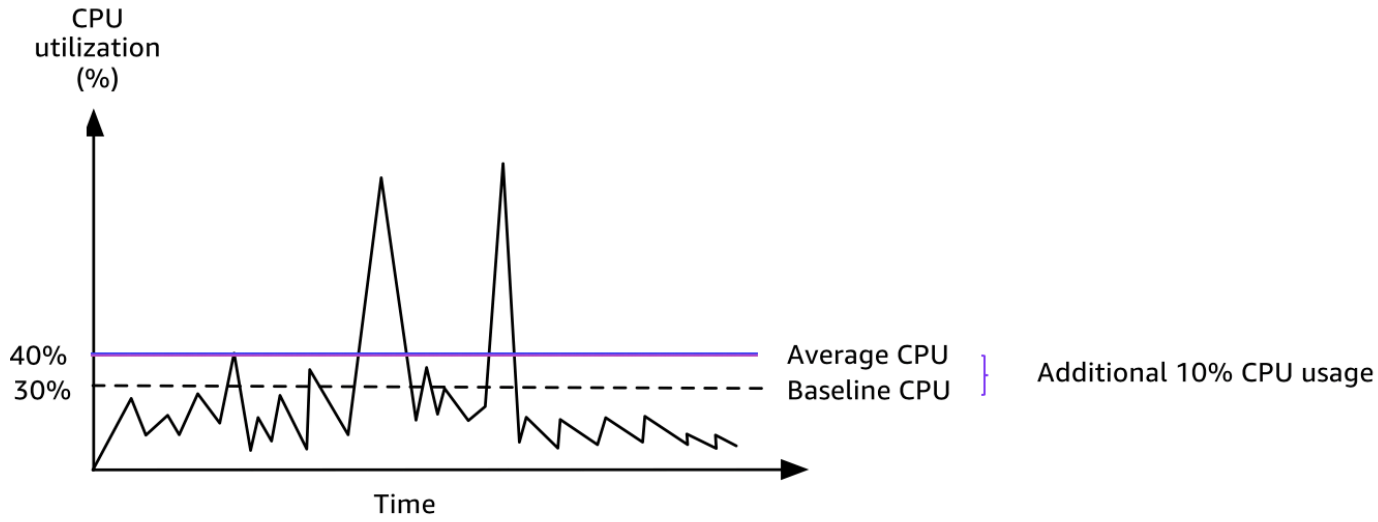
O modo `unlimited` é uma opção de configuração de crédito para instâncias expansíveis. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. É possível definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance expansível na conta sejam iniciadas usando a opção de crédito padrão.

Como funcionam as instâncias expansíveis

Se uma instância expansível configurada como `unlimited` esgota seu crédito de CPU, ela pode gastar créditos excedentes para ter expansão acima da linha de base. Quando sua utilização de CPU ficar abaixo da linha de base, ela usará os créditos de CPU que ela ganhar para pagar os

créditos excedentes gastos anteriormente. A capacidade de ganhar créditos de CPU para pagar créditos excedentes permite que o Amazon EC2 mantenha a média de utilização de CPU de uma instância em um período de 24 horas. Se o uso médio da CPU durante um período de 24 horas exceder a lista de referência, a instância será cobrada pelo uso adicional em uma taxa adicional fixa por hora de vCPU.

O gráfico a seguir mostra o uso da CPU de um `t3.large`. A utilização da CPU de linha de base para um `t3.large` é 30%. Se a instância for executada com 30% de utilização da CPU ou menos, em média, durante um período de 24 horas, não haverá cobrança adicional porque o custo já está coberto pelo preço por hora da instância. No entanto, se a instância for executada com 40% de utilização da CPU, em média, durante um período de 24 horas, conforme mostrado no gráfico, a instância será cobrada pelo uso adicional de 10% da CPU em uma taxa adicional fixa por hora de vCPU.



Para obter mais informações sobre a utilização da linha de base por vCPU para cada tipo de instância e quantos créditos cada tipo de instância recebe, consulte a tabela de créditos.

Quando usar o modo ilimitado versus CPU fixa

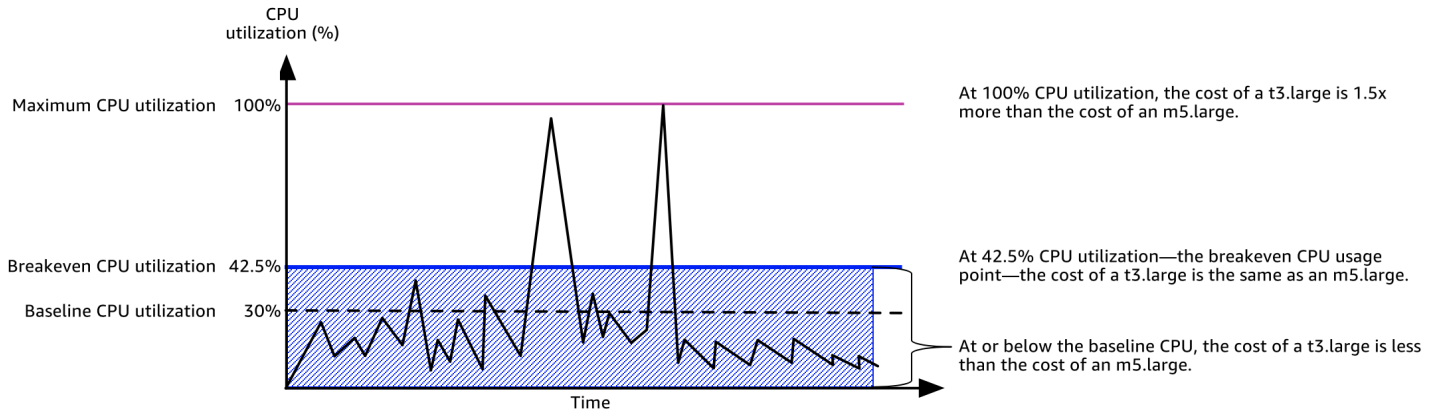
Ao determinar se use uma instância expansível no modo `unlimited`, como T3, ou uma instância de performance fixa, como M5, você precisa determinar o uso da CPU de equilíbrio. O uso da CPU de equilíbrio para uma instância expansível é o ponto em que uma instância expansível custa o mesmo que uma instância de performance fixa. O uso da CPU de equilíbrio ajuda a determinar o seguinte:

- Se o uso médio da CPU em um período de 24 horas estiver no uso de CPU de equilíbrio ou abaixo dele, use uma instância expansível no modo `unlimited` para que você possa se beneficiar do

preço mais baixo de uma instância expansível enquanto obtém ao mesma performance de uma instância de performance fixa.

- Se o uso médio da CPU durante um período de 24 horas estiver acima do uso de CPU de equilíbrio, a instância expansível custará mais do que a instância de performance fixa de tamanho equivalente. Se uma instância T3 apresentar uma expansão contínua para 100% da CPU, você acabará pagando aproximadamente 1,5 vezes o preço de uma instância M5 de tamanho equivalente.

O gráfico a seguir mostra o ponto de uso da CPU de equilíbrio em que um `t3.large` custa o mesma que um `m5.large`. O ponto de uso da CPU de equilíbrio para um `t3.large` é 42,5%. Se o uso médio da CPU estiver em 42,5%, o custo de executar o `t3.large` é o mesmo que um `m5.large`, e é mais caro se o uso médio da CPU estiver acima de 42,5%. Se a workload precisar de menos de 42,5% do uso médio da CPU, será possível se beneficiar do preço mais baixo do `t3.large` ao obter a mesma performance de um `m5.large`.



A tabela a seguir mostra como calcular o limite de uso da CPU de equilíbrio para que você possa determinar quando é mais barato usar uma instância expansível no modo `unlimited` ou uma instância de performance fixa. As colunas na tabela são rotuladas de A a K.

Tipo de instância	vCPUs	Preço*/ hora de T3	Preço*/ hora de M5	Diferença de preço	Utilização da linha de base T3 por vCPU (%)	Cobrança por hora de vCPU de créditos excedentes	Cobrança por minuto de vCPU	Mais minutos de expansão disponíveis por vCPU	% de CPU adicional disponível	% de CPU de equilíbrio
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	US$ 0,0835	0,096 USD	0,0125 US	30%	0,05 USD	US$ 0,000833	15	12,5%	42,5%

*O preço é baseado no us-east-1 e no SO Linux.

A tabela fornece as seguintes informações:

- A coluna A mostra o tipo de instância, `t3.large`.
- A coluna B mostra o número de vCPUs para o `t3.large`.
- A coluna C mostra o preço de um `t3.large` por hora.
- A coluna D mostra o preço de um `m5.large` por hora.
- A coluna E mostra a diferença de preço entre o `t3.large` e o `m5.large`.
- A coluna F mostra a utilização da linha de base por vCPU do `t3.large`, que é 30%. Na linha de base, o custo por hora da instância abrange o custo do uso da CPU.
- A coluna G mostra a taxa adicional fixa por hora de vCPU em que uma instância é cobrada, se apresentar uma expansão em 100% da CPU depois de ter esgotado seus créditos ganhos.
- A coluna H mostra a taxa adicional fixa por minuto de vCPU em que uma instância é cobrada, se apresentar uma expansão em 100% da CPU depois de ter esgotado seus créditos ganhos.

- A coluna I mostra o número de minutos adicionais que o `t3.large` pode apresentar uma expansão por hora para 100% da CPU pagando o mesmo preço por hora que um `m5.large`.
- A coluna J mostra o uso adicional da CPU (em %) ao longo da linha de base em que a instância pode apresentar uma expansão enquanto paga o mesmo preço por hora que um `m5.large`.
- A coluna K mostra o uso da CPU de equilíbrio (em%) em que o `t3.large` pode apresentar uma expansão sem pagar mais do que o `m5.large`. Qualquer coisa acima disso, e o `t3.large` custará mais do que o `m5.large`.

A tabela a seguir mostra o uso da CPU de equilíbrio (em%) para os tipos de instância T3 em comparação com os tipos de instância M5 de tamanho semelhante.

Tipo de instância do T3	Uso da CPU de equilíbrio (em %) para T3 comparado a M5
`t3.large`	42,5%
`t3.xlarge`	52,5 %
`t3.2xlarge`	52,5 %

Os créditos excedentes podem gerar cobranças

Se a utilização média de CPU de um instância for igual ou inferior à linha de base, a instância não incorrerá encargos adicionais. Como uma instância ganha um número máximo de créditos em um período de 24 horas (por exemplo, uma instância `t3.micro` pode ganhar no máximo 288 créditos em um período de 24 horas), ela pode gastar créditos excedentes até esse limite máximo sem gerar uma cobranças imediatamente.

Contudo, se a utilização de CPU permanecer acima da linha de base, a instância não poderá obter créditos suficientes para pagar os créditos excedentes que ela gastou. Os créditos excedentes que não são pagos são cobrados a uma taxa adicional fixa por hora de vCPU. Para obter informações sobre a taxa, consulte a definição de preço do modo ilimitado T2/T3/T4g.

Os créditos excedentes que foram gastos anteriormente são cobrados quando uma das seguintes situações ocorre:

- Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora.
- A instância é interrompida ou encerrada.
- A instância é alterada de `unlimited` para `standard`.

Os créditos excedentes gastos são monitorados pela métrica CloudWatch do `CPUSurplusCreditBalance`. Os créditos excedentes cobrados são monitorados pela métrica CloudWatch do `CPUSurplusCreditsCharged`. Para obter mais informações, consulte Métricas adicionais do CloudWatch para instâncias expansíveis.

Nenhum crédito de execução para T2 ilimitada

As instâncias T2 padrão recebem créditos de execução, mas as instâncias T2 ilimitadas não as recebem. Uma instância T2 ilimitada pode apresentar expansão acima da linha de base a qualquer momento, sem encargos adicionais, desde que sua utilização média de CPU seja igual ou inferior à linha de base em um período contínuo de 24 horas ou durante sua vida útil, o que for menor. Como tal, as instâncias T2 ilimitadas não requerem créditos de execução para atingir alta performance imediatamente após a execução.

Se uma instância T2 for alterada de `standard` para `unlimited`, todos os créditos de execução acumulados serão removidos do `CPUCreditBalance` antes do `CPUCreditBalance` restante ser transferido.

As instâncias T4g, T3a e T3 nunca recebem créditos de inicialização porque são compatíveis com o modo ilimitado. A configuração de crédito de modo ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Ativar modo ilimitado

É possível alterar de `unlimited` para `standard` e de `standard` para `unlimited` a qualquer momento em uma instância interrompida ou em execução. Para obter mais informações, consulte Iniciar uma instância expansível como ilimitada ou padrão e Modificar a especificação de crédito de uma instância expansível.

É possível definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance com capacidade de expansão na conta sejam executadas usando a opção de crédito padrão. Para obter mais informações, consulte Definir a especificação de crédito padrão para a conta.

É possível verificar se uma instância expansível está configurada como `unlimited` ou `standard` usando o console do Amazon EC2 ou a AWS CLI. Para obter mais informações, consulte Exibir a especificação de crédito de uma instância expansível e Visualizar a especificação de crédito padrão.

O que acontece com os créditos quando é feita alternância de ilimitada para padrão

`CPUCreditBalance` é uma métrica do CloudWatch que controla o número de créditos que uma instância acumulou. `CPUSurplusCreditBalance` é uma métrica do CloudWatch que monitora o número de créditos excedentes que uma instância gastou.

Ao alterar uma instância configurada como `unlimited` para `standard`, ocorre o seguinte:

- O valor `CPUCreditBalance` permanece inalterado e é transferido.
- O valor `CPUSurplusCreditBalance` é cobrado imediatamente.

Quando uma instância `standard` é alterada para `unlimited`, ocorre o seguinte:

- O valor `CPUCreditBalance` que contém créditos ganhos acumulados é transferido.
- Para instâncias T2 padrão, todos os créditos de execução são removidos do valor `CPUCreditBalance`, e o valor `CPUCreditBalance` que contém os créditos ganhos acumulados é transferido.

Monitorar uso de crédito

Para verificar se a instância está gastando mais créditos do que a linha de base fornece, é possível usar as métricas do CloudWatch no monitoramento do uso e configurar alarmes horários para ser notificado sobre o uso de crédito. Para obter mais informações, consulte Monitore seus créditos da CPU para instâncias expansíveis.

Exemplos de modo ilimitado

Os seguintes exemplos explicam o uso de créditos para instâncias configuradas como `unlimited`.

Exemplos

- Exemplo 1: explicar o uso de créditos com T3 ilimitada
- Exemplo 2: explicar o uso de créditos com T2 ilimitada

Exemplo 1: explicar o uso de créditos com T3 ilimitada

Neste exemplo, você verá a utilização de CPU de uma instância `t3.nano` executada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar a utilização de CPU.

A instância `t3.nano` ganha 144 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 144 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU — excedentes, que ela ainda não ganhou—, para ter expansão durante o tempo que precisar. Como uma instância `t3.nano` ganha no máximo 144 créditos em um período de 24 horas, ela poderá gastar os créditos excedentes até esse limite máximo, sem ser cobrada imediatamente por isso. Se ela gastar mais de 144 créditos de CPU, será cobrada pela diferença no final da hora.

A intenção do exemplo, ilustrada pelo gráfico a seguir, é mostrar como uma instância pode apresentar expansão usando créditos excedentes, mesmo após esgotar seu `CPUCreditBalance`. O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

P1 – às 0 horas no gráfico, a instância é executada como `unlimited` e começa a ganhar créditos imediatamente. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Nas primeiras 24 horas, `CPUCreditUsage` é de 0, e o valor `CPUCreditBalance` atinge seu máximo de 144.

P2 – nas próximas 12 horas, a utilização de CPU é de 2,5%, que é abaixo da linha de base de 5%. A instância ganha mais créditos do que gasta, mas o valor `CPUCreditBalance` não pode exceder seu máximo de 144 créditos.

P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

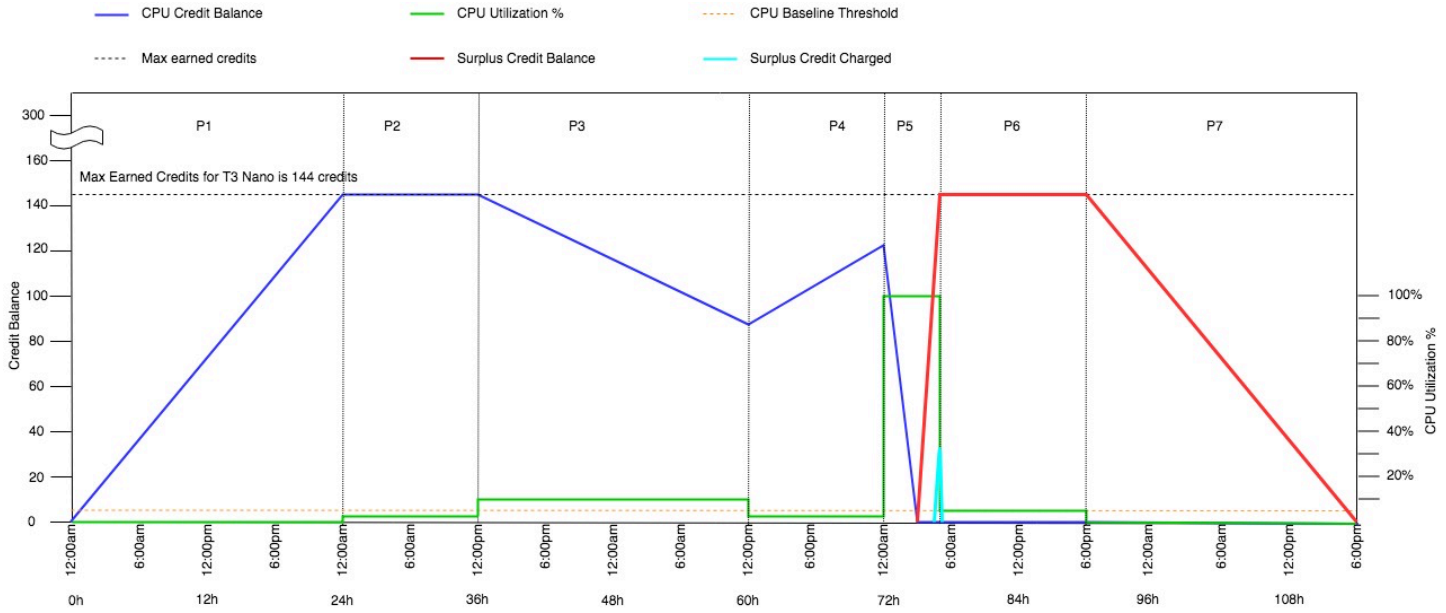
P4 – nas próximas 12 horas, a utilização de CPU diminui para 2,5% (abaixo da linha de base), o que exige um gasto de 36 créditos. Ao mesmo tempo, a instância ganha 72 créditos. A instância ganha mais créditos do que gasta, e o valor `CPUCreditBalance` aumenta para 122 créditos.

P5 – nas próximas 5 horas, a instância tem expansão para 100% de utilização de CPU e gasta um total de 570 créditos para sustentar a expansão. Após aproximadamente uma hora desse período, a instância esgota todo o `CPUCreditBalance` de 122 créditos e começa a gastar os créditos excedentes para sustentar o alto uso de CPU, totalizando 448 créditos excedentes nesse período (570 - 122 = 448). Quando o valor `CPUSurplusCreditBalance` atingir 144 créditos de

CPU (o máximo que uma instância `t3.nano` pode ganhar em um período de 24 horas), todos os créditos excedentes gastos após esse período não poderão ser compensados por créditos ganhos. Os créditos excedentes gastos depois desse período totalizam 304 créditos (448 - 144 = 304), resultando em uma pequena cobrança adicional ao fim dessa hora para 304 créditos.

P6 – nas próximas 13 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o número de créditos que gastar, sem precisar pagar por excessos do `CPUSurplusCreditBalance`. O valor `CPUSurplusCreditBalance` permanece em 144 créditos.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que usa para pagar o `CPUSurplusCreditBalance`.



Exemplo 2: explicar o uso de créditos com T2 ilimitada

Neste exemplo, você verá a utilização de CPU de uma instância `t2.nano` executada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar a utilização de CPU.

A instância `t2.nano` ganha 72 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 72 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU — excedentes, que ela ainda não ganhou—, para ter expansão durante o tempo que precisar. Como uma instância `t2.nano` ganha no máximo 72 créditos em um período de 24 horas, ela poderá gastar os créditos excedentes até esse limite máximo, sem ser cobrada imediatamente por isso. Se ela gastar mais de 72 créditos de CPU, será cobrada pela diferença no final da hora.

A intenção do exemplo, ilustrada pelo gráfico a seguir, é mostrar como uma instância pode apresentar expansão usando créditos excedentes, mesmo após esgotar seu `CPUCreditBalance`. É possível supor que, no início de linha de tempo no gráfico, a instância tem um saldo de créditos acumulados igual ao número máximo de créditos que ela pode ganhar em 24 horas. O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

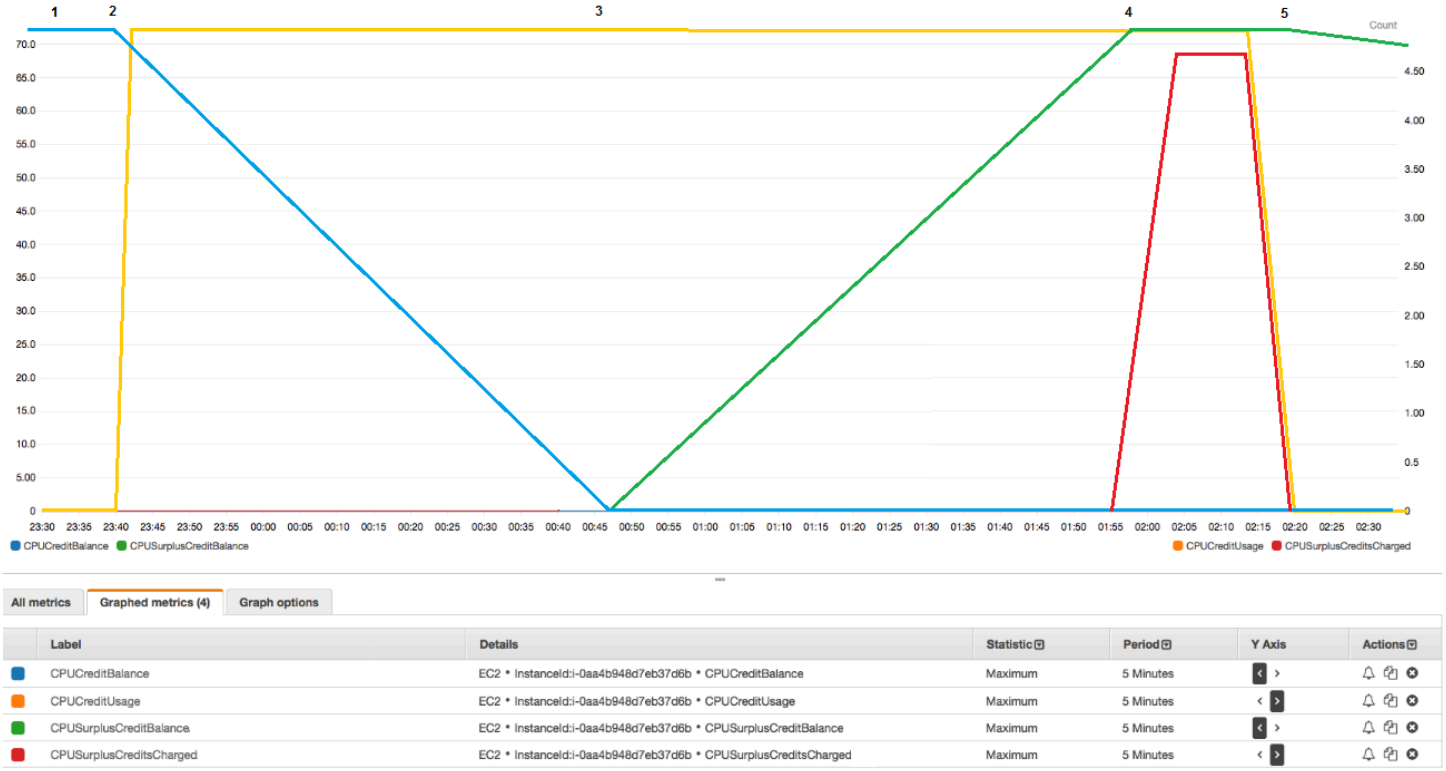
1 – Nos primeiros 10 minutos, `CPUCreditUsage` está em 0 e o valor `CPUCreditBalance` permanece no limite máximo de 72.

2 – Às 23H40, à medida que a utilização da CPU aumenta, a instância gasta os créditos de CPU e o valor `CPUCreditBalance` diminui.

3 – Por volta de 00h47, a instância esgota todo o seu `CPUCreditBalance` e começa a gastar os créditos excedentes para manter o alto uso da CPU.

4 – Os créditos excedentes são gastos até 01h55, quando o valor `CPUSurplusCreditBalance` atinge 72 créditos de CPU. Isso é igual ao limite máximo que uma instância `t2.nano` pode ganhar em um período de 24 horas. Qualquer crédito excedente gasto a partir daí não poderá ser compensado pelos créditos ganhos no período de 24 horas, o que resultará em uma pequena taxa adicional no final da hora.

5 – A instância continua a gastar os créditos excedentes até às 02h20. Nesse momento, a utilização da CPU cai abaixo da linha de base, e a instância começa a ganhar 3 créditos por hora (ou 0,25 crédito a cada 5 minutos), que ela usa para pagar o `CPUSurplusCreditBalance`. Quando o valor `CPUSurplusCreditBalance` reduz para 0, a instância começa a acumular créditos ganhos em seu `CPUCreditBalance` a 0,25 crédito a cada 5 minutos.



Como calcular a fatura (instância do Linux)

Os créditos excedentes custam USD 0,05 por hora de vCPU. A instância gastou cerca de 25 créditos excedentes entre 01h55 e 02h20, o que equivale a 0,42 horas de vCPU. As cobranças adicionais para essa instância são de USD 0,42 por hora de vCPU x USD 0,05/hora de vCPU = USD 0,021, que é arredondado para USD 0,02. Esta é a conta de final do mês desta instância T2 ilimitada:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Como calcular a fatura (instância do Windows)

Os créditos excedentes custam USD 0,096 por hora de vCPU. A instância gastou cerca de 25 créditos excedentes entre 01h55 e 02h20, o que equivale a 0,42 horas de vCPU. As cobranças adicionais para essa instância são de USD 0,42 por hora de vCPU x USD 0,096/hora de vCPU = USD 0,04032, que é arredondado para USD 0,04. Esta é a conta de final do mês desta instância T2 ilimitada:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

É possível configurar alertas de pagamento para ser notificado a cada hora sobre quaisquer cobranças acumuladas e tomar providências, se necessário.

Modo padrão de instâncias expansíveis

Uma instância expansível configurada como `standard` é adequada para workloads com uma utilização média de CPU consistentemente abaixo da utilização de CPU de linha de base da instância. Para expansões acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Se a instância estiver ficando sem créditos acumulados, o uso de CPU será gradualmente reduzido para o nível da linha de base, para que a instância não experimente uma queda de performance acentuada quando o saldo de créditos de CPU acumulado se esgotar. Para obter mais informações, consulte Principais conceitos e definições para instâncias expansíveis.

Tópicos

- Conceitos do modo padrão
  - Como funcionam as instâncias expansíveis padrão
  - Créditos de execução
  - Limites de crédito de execução
  - Diferenças entre créditos de execução e créditos ganhos
- Exemplos de modo padrão
  - Exemplo 1: explicar o uso de créditos com T3 padrão
  - Exemplo 2: explicar o uso de créditos com T2 padrão
    - Período 1: 1 a 24 horas
    - Período 2: 25 a 36 horas
    - Período 3: 37 a 61 horas
    - Período 4: 62 a 72 horas
    - Período 5: 73 – 75 horas
    - Período 6: 76 a 90 horas

- Período 7: 91 a 96 horas

Conceitos do modo padrão

O modo `standard` é uma opção de configuração para instâncias expansíveis Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. É possível definir `standard` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance expansível na conta sejam iniciadas usando a opção de crédito padrão.

Como funcionam as instâncias expansíveis padrão

Quando uma instância expansível configurada como `standard` estiver em um estado de execução, ela receberá continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. Para T2 padrão, quando a instância é interrompida, ela perde todos os créditos acumulados, e seu saldo de créditos é redefinido para zero. Quando é reiniciada, ela recebe um novo conjunto de créditos de execução e começa a acumular créditos ganhos. Para instâncias T4g, T3a e T3 padrão, o saldo de crédito de CPU persiste durante sete dias após a instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

As instâncias T2 Standard recebem dois tipos de créditos de CPU: créditos ganhos e créditos de inicialização. Quando uma instância T2 padrão estiver em um estado de execução, ela recebe continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. No começo, ela ainda não ganhou créditos para uma boa experiência de inicialização. Portanto, para oferecer uma boa experiência de startup, ela recebe créditos de execução para começar, que ela gasta primeiro ao acumular créditos ganhos.

As instâncias T4g, T3a e T3 não recebem créditos de inicialização porque são compatíveis com o modo Ilimitado. A configuração de crédito de modo ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Créditos de execução

As instâncias T2 Standard recebem 30 créditos de inicialização por vCPU ao serem iniciadas, e as instâncias T1 Standard recebem 15 créditos de inicialização. Por exemplo, uma instância `t2.micro` tem uma vCPU e recebe 30 créditos de execução, enquanto uma instância `t2.xlarge` tem quatro vCPUs e recebe 120 créditos de execução. Os créditos de execução foram criados para oferecer

uma boa experiência de startup, permitindo, assim, que as instâncias apresentem uma expansão imediatamente após a execução, antes que acumulem créditos ganhos.

Os créditos de execução são gastos primeiro, antes dos créditos ganhos. Os créditos de execução não gastos são acumulados no saldo de créditos de CPU, mas não são contabilizados para o limite de saldo de créditos de CPU. Por exemplo, uma instância `t2.micro` tem um limite de saldo de créditos de CPU de 144 créditos ganhos. Se for executada e permanecer inativa por 24 horas, seu saldo de créditos de CPU atingirá 174 (30 créditos de execução + 144 créditos ganhos), que é acima do limite. No entanto, depois que a instância gastar os 30 créditos de execução, o saldo não poderá exceder 144. Para obter mais informações sobre o limite de saldo de crédito de CPU para cada tamanho de instância, consulte a Tabela de créditos.

A tabela a seguir lista a alocação de crédito de CPU inicial recebida na execução ou no início, e o número de vCPUs.

Tipo de instância	Créditos de execução	vCPUs
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1
`t2.medium`	60	2
`t2.large`	60	2
`t2.xlarge`	120	4
`t2.2xlarge`	240	8

Limites de crédito de execução

Existe um limite para o número de vezes em que instâncias T2 padrão podem receber créditos de execução. O limite padrão é de 100 execuções ou inicializações de todas as instâncias T2 padrão combinadas por conta, por região, por período de 24 horas de acúmulo. Por exemplo, o limite é atingido quando uma instância é interrompida e iniciada 100 vezes em um período de 24 horas, ou

quando 100 instâncias são executadas em um período de 24 horas ou outras combinações que se igualem a 100 inicializações. As novas contas podem ter um limite inferior, que aumenta ao longo do tempo com base no seu uso.

> **Tip**
>
> Para garantir que as workloads sempre obtenham a performance de que precisam, alterne para Modo ilimitado de instâncias expansíveis ou considere o uso de uma instância maior.

Diferenças entre créditos de execução e créditos ganhos

A tabela a seguir lista as diferenças entre créditos de execução e créditos ganhos.

	Créditos de execução	Créditos ganhos
Taxa de ganhos de crédito	As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização. Se uma instância T2 for alterada de `unlimited` para `standard`, ela não obtém créditos de execução no momento em que é alterada.	Cada instância T2 obtém continuam ente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, dependend o do tamanho da instância. Para obter mais informações sobre o número de créditos de CPU ganhos por tamanho de instância, consulte a Tabela de créditos.
Limite de ganho de crédito	O limite para receber créditos de execução é de 100 execuções ou inicializações de todas as instância s T2 padrão combinadas por conta, por região, por período de 24 horas de acúmulo. As novas contas podem ter um limite inferior, que aumenta ao longo do tempo com base no seu uso.	Uma instância T2 não pode acumular mais créditos do que o limite de saldo de crédito de CPU. Se o saldo de créditos de CPU atingir o limite, todos os créditos que forem obtidos após o limite ser atingido serão descartad os. Os créditos de execução não contam para o limite. Para obter mais informações sobre o limite de saldo de créditos de CPU para cada tamanho de instância T2, consulte a Tabela de créditos.

	Créditos de execução	Créditos ganhos
Uso de crédito	Os créditos de execução são gastos primeiro, antes dos créditos ganhos.	Os créditos ganhos são gastos só após todos os créditos de execução serem gastos.
Expiração de crédito	Quando uma instância T2 está em execução, os créditos de execução não expiram. Quando uma instância padrão T2 para ou é alterada para T2 ilimitada, todos os créditos de execução são perdidos.	Quando uma instância T2 está em execução, os créditos ganhos que foram acumulados não expiram. Quando a instância T2 é interrompida, todos os créditos ganhos que foram acumulados são perdidos.

O número de créditos de execução e créditos ganhos acumulados é monitorado pela métrica `CPUCreditBalance` do CloudWatch. Para obter mais informações, consulte `CPUCreditBalance` na Tabela de métricas do CloudWatch.

Exemplos de modo padrão

Os seguintes exemplos explicam o uso de créditos quando as instâncias estão configuradas como `standard`.

Exemplos

- Exemplo 1: explicar o uso de créditos com T3 padrão
- Exemplo 2: explicar o uso de créditos com T2 padrão

Exemplo 1: explicar o uso de créditos com T3 padrão

Neste exemplo, você verá como uma instância `t3.nano` executada como `standard` ganha, acumula e gasta créditos ganhos. Você verá como o saldo de créditos reflete os créditos ganhos que foram acumulados.

Uma instância `t3.nano` em execução ganha 144 créditos a cada 24 horas. Seu limite de saldo de créditos é de 144 créditos ganhos. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a Tabela de créditos.

É possível iniciar uma instância T3 padrão e usá-la imediatamente. Ou, é possível iniciar uma instância padrão T3 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas a partir do momento em que é executada, o saldo de créditos atingirá seu limite, que é o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

P1 – às 0 horas no gráfico, a instância é executada como `standard` e começa a ganhar créditos imediatamente. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Nas primeiras 24 horas, `CPUCreditUsage` é de 0, e o valor `CPUCreditBalance` atinge seu máximo de 144.

P2 – nas próximas 12 horas, a utilização de CPU é de 2,5%, que é abaixo da linha de base de 5%. A instância ganha mais créditos do que gasta, mas o valor `CPUCreditBalance` não pode exceder seu máximo de 144 créditos. Todos os créditos ganhos que excedem o limite são descartados.

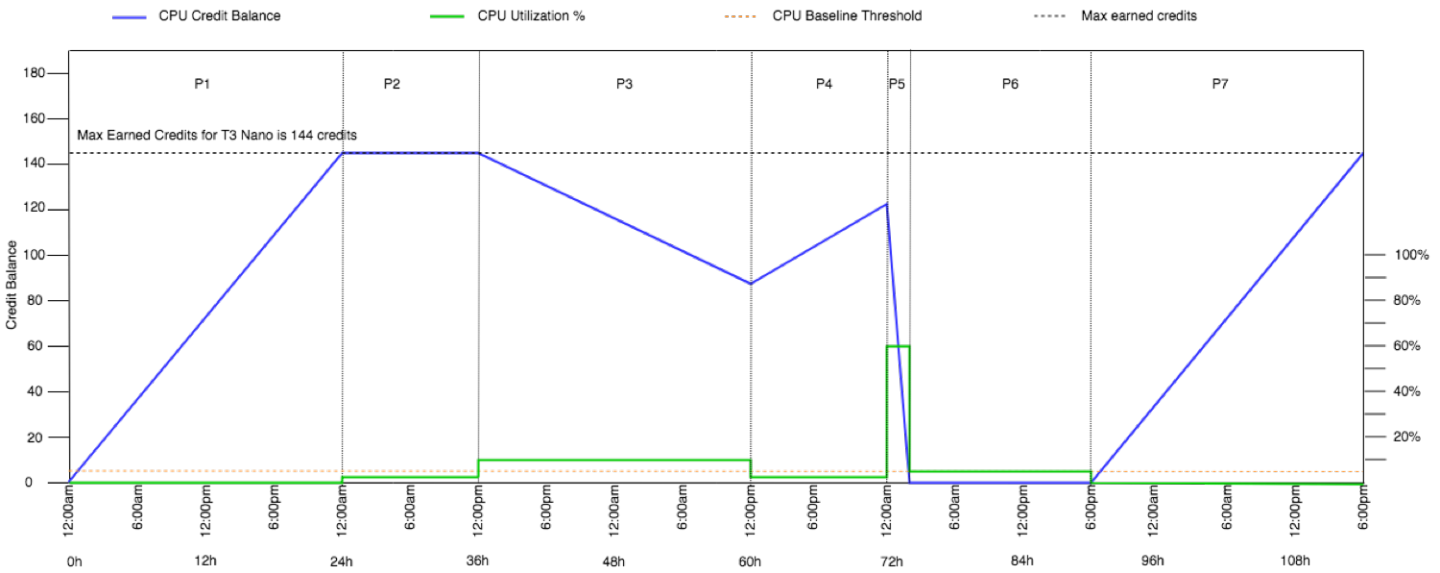
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

P4 – nas próximas 12 horas, a utilização de CPU diminui para 2,5% (abaixo da linha de base), o que exige um gasto de 36 créditos. Ao mesmo tempo, a instância ganha 72 créditos. A instância ganha mais créditos do que gasta, e o valor `CPUCreditBalance` aumenta para 122 créditos.

P5: nas próximas duas horas, a instância terá expansão para 60% de utilização de CPU e esgotará todo o valor `CPUCreditBalance` de 122 créditos. Ao fim desse período, com o `CPUCreditBalance` em zero, a utilização de CPU é forçada a diminuir para o nível de utilização de linha de base de 5%. Na linha de base, a instância ganha o mesmo número de créditos que são gastos.

P6 – nas próximas 14 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o mesmo número de créditos que são gastos. O valor de `CPUCreditBalance` permanece em 0.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que acumula em seu `CPUCreditBalance`.



Exemplo 2: explicar o uso de créditos com T2 padrão

Neste exemplo, você verá como uma instância `t2.nano` executada como `standard` ganha, acumula e gasta créditos ganhos e de execução. Você verá como o saldo de crédito reflete não somente os créditos ganhos acumulados, como também os créditos de execução acumulados.

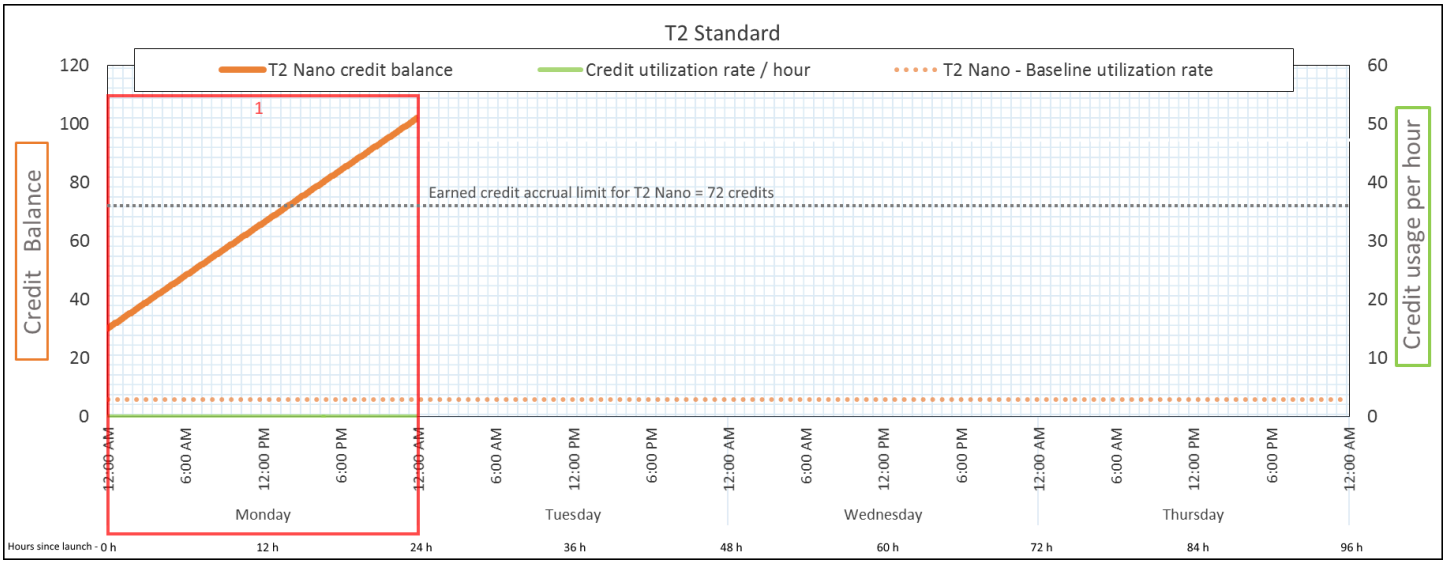
A instância `t2.nano` obtém 30 créditos de execução quando é executada e ganha 72 créditos a cada 24 horas. Seu limite de saldo é de 72 créditos ganhados. Os créditos de execução não são considerados no limite. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a Tabela de créditos. Para obter mais informações sobre limites, consulte Limites de crédito de execução.

É possível iniciar uma instância T2 padrão e usá-la imediatamente. Ou, é possível iniciar uma instância padrão T2 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas após sua execução, o saldo de crédito será exibido como ultrapassado do limite, pois reflete os créditos ganhos e de execução acumulados. No entanto, após o uso da CPU, os créditos de execução são gastos primeiro. Depois disso, o limite sempre reflete o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

Período 1: 1 a 24 horas

Na hora 0 do gráfico, a instância T2 é executada como `standard` e obtém imediatamente 30 créditos de execução. Ela ganha créditos durante o estado de execução. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Aproximadamente 14 horas após a execução, o saldo de crédito é 72 (30 créditos de execução + 42 créditos ganhos), que é equivalente ao que a instância pode ganhar em 24 horas. Após 24 horas da execução, o saldo ultrapassa 72 créditos, pois os créditos de execução não gastos são acumulados (o saldo é de 102 créditos: 30 créditos de execução + 72 créditos ganhos).



Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos)

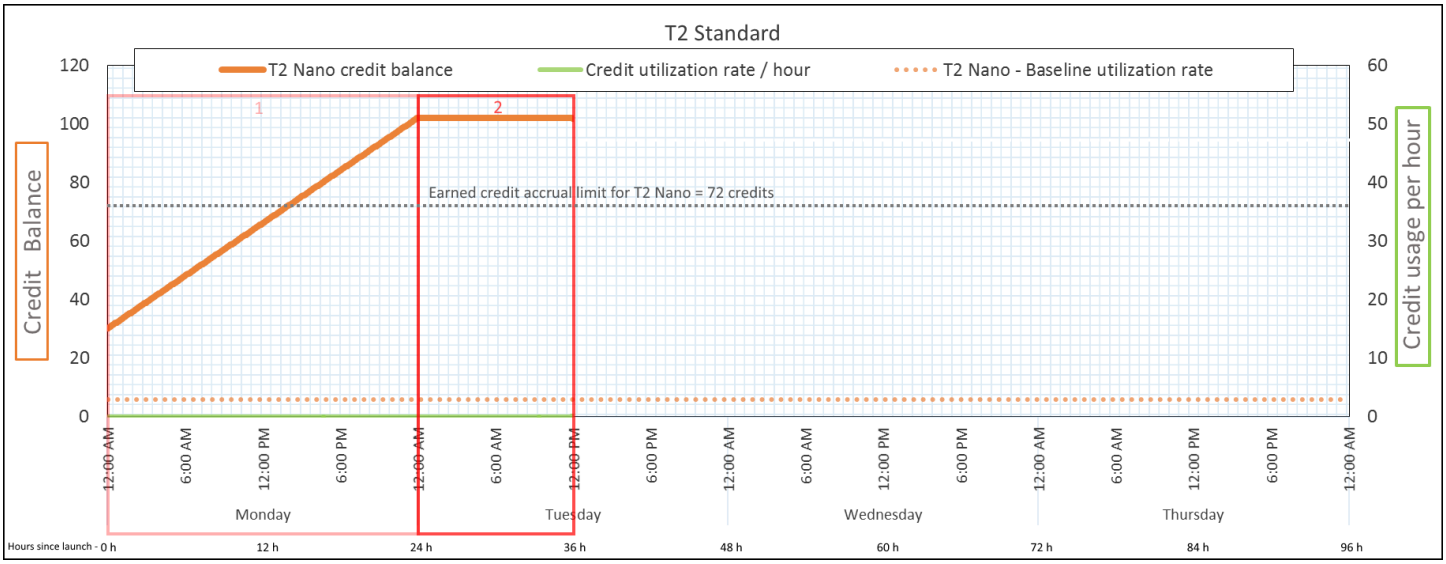
Conclusão

Se não houver uso da CPU após a execução, a instância acumulará mais créditos do que pode ganhar em 24 horas (30 créditos de execução + 72 créditos ganhos = 102).

Em um cenário real, uma instância do EC2 consome um pequeno número de créditos durante a execução. Isso impede que o saldo atinja o valor teórico máximo nesse exemplo.

Período 2: 25 a 36 horas

Nas próximas 12 horas, a instância continua ociosa e ganhando créditos, mas o saldo não aumenta. Ele estabiliza em 102 créditos (30 créditos de execução + 72 créditos ganhos). O saldo atingiu o limite de 72 créditos ganhos acumulados. Por isso, os créditos ganhos mais recentemente são descartados.



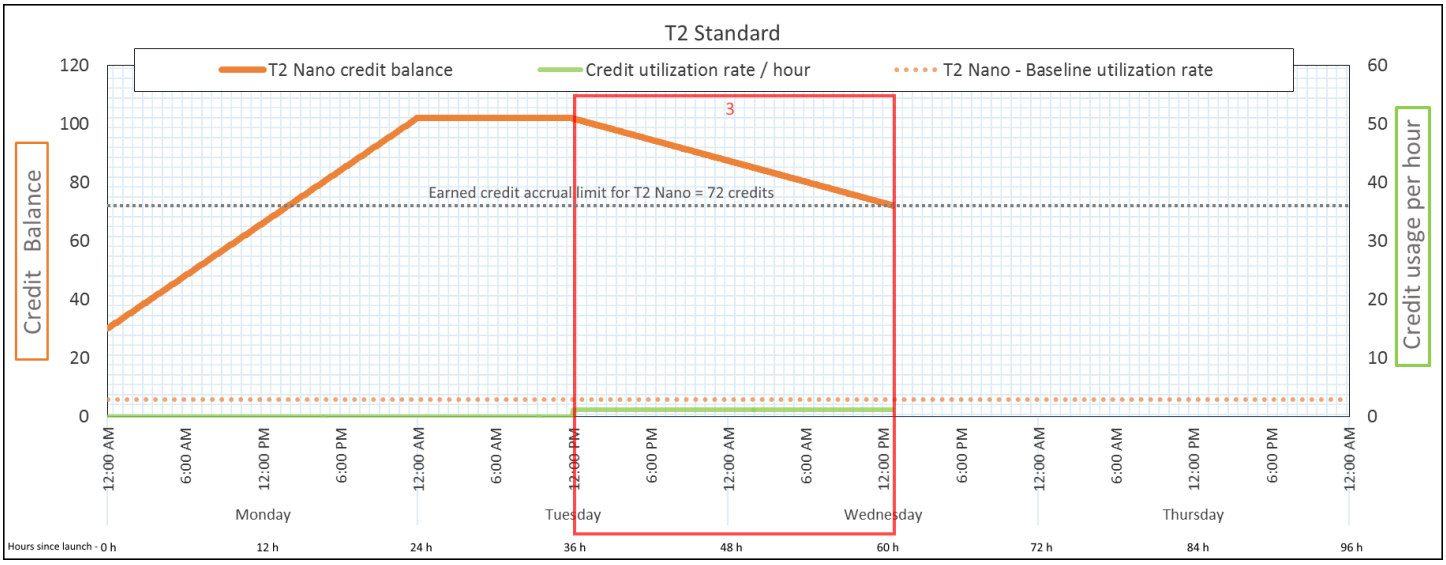
Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas (3 créditos por hora)
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos) – o saldo não é alterado

Conclusão

Uma instância ganha constantemente créditos, mas, se atingir o limite, não poderá acumular mais créditos. Assim que o limite é atingido, os créditos ganhos mais recentemente são descartados. Os créditos de execução não são contabilizados para o limite de sado de créditos de Se incluir créditos de execução acumulados, o saldo parecerá estar acima do limite.

Período 3: 37 a 61 horas

Nas próximas 25 horas, a instância usa 2% da CPU. Isso requer 30 créditos. No mesmo período, ela ganha 75 créditos, mas o saldo diminuir. O saldo diminui porque os créditos de execução acumulados são gastos primeiro, enquanto os créditos recém-ganhos são descartados, pois o saldo já está no limite de 72 créditos ganhos.



Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 30 créditos— em 25 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (30 créditos de execução foram gastados; 72 créditos ganhos continuam não gastos)

Conclusão

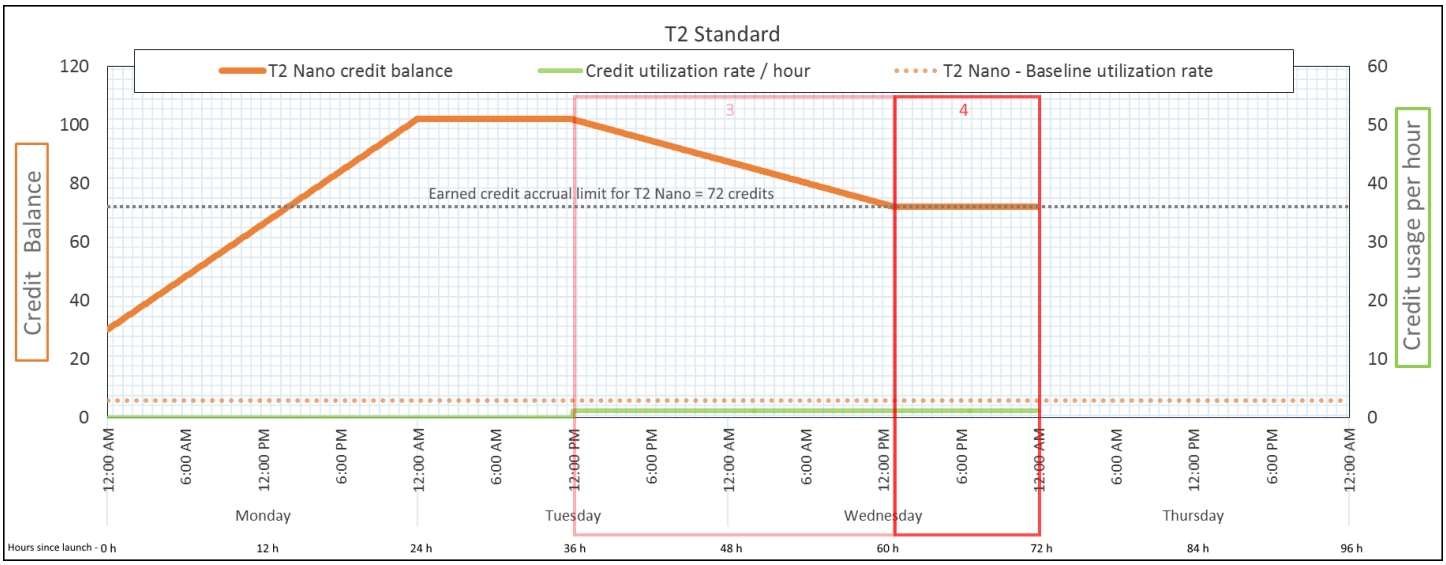
A instância gasta créditos de execução primeiro, antes dos crédito ganhos. Os créditos de execução não são contabilizados para o limite de créditos. Após o gasto dos créditos de execução, o saldo

nunca pode ultrapassar o número ganho em 24 horas. Além disso, durante sua execução, a instância não pode obter mais créditos de execução.

Período 4: 62 a 72 horas

Nas próximas 11 horas, a instância usa 2% da CPU. Isso requer 13.2 créditos. Esse é o mesmo uso de CPU que o do período anterior, mas o saldo não diminui. Ele permanece em 72 créditos.

O saldo não diminui pois a taxa de ganho é superior à taxa de gasto de crédito. No período em que gasta 13,2 créditos, a instância também ganha 33. No entanto, o limite de saldo é de 72 créditos. Portanto, todos os créditos ganhos que ultrapassam o limite são descartados. O saldo é estabilizado em 72 créditos, que é diferente do platô de 102 créditos durante o Período 2, pois não há crédito de execução acumulado.



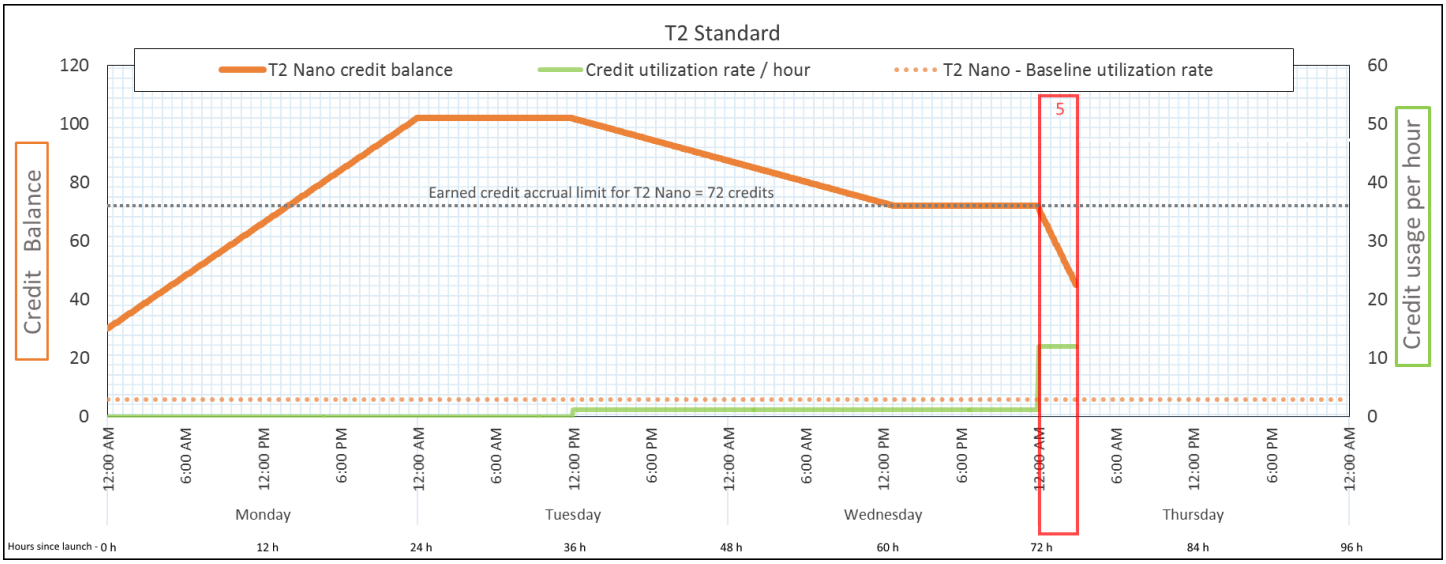
Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 13,2 —créditos em 11 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	43.2 créditos por 24 horas (60% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos) – o —saldo está no limite

Conclusão

Após o gasto dos créditos de execução, o limite de saldo de crédito é determinado pelo número de créditos que uma instância pode ganhar em 24 horas. Se a instância ganhar mais créditos do que gastar, os créditos recém-ganhos acima do limite serão descartados.

Período 5: 73 – 75 horas

Nas próximas três horas, o uso da CPU pela instância sobe para 20%. Isso requer 36 créditos. A instância ganha nove créditos nas mesmas três horas, resultando em uma diminuição do saldo líquido de 27 créditos. No final das três horas, o saldo é de 45 créditos ganhos.



Taxa de gasto de crédito	288 créditos por 24 horas (12 créditos por hora, 20% de utilização da CPU, 400% de taxa de ganhos de crédito) – 36— créditos em 3 horas
Taxa de ganhos de crédito	72 créditos por 24 horas (9 créditos em 3 horas)
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	45 créditos (saldo anterior (72) - créditos gastos (36) + créditos ganhos (9)) – o —saldo diminui a uma taxa de 216 créditos por 24 horas (taxa de gastos de 288/24 + taxa de

	ganhos de 72/24 = taxa de diminuição do saldo de 216/24)

Conclusão

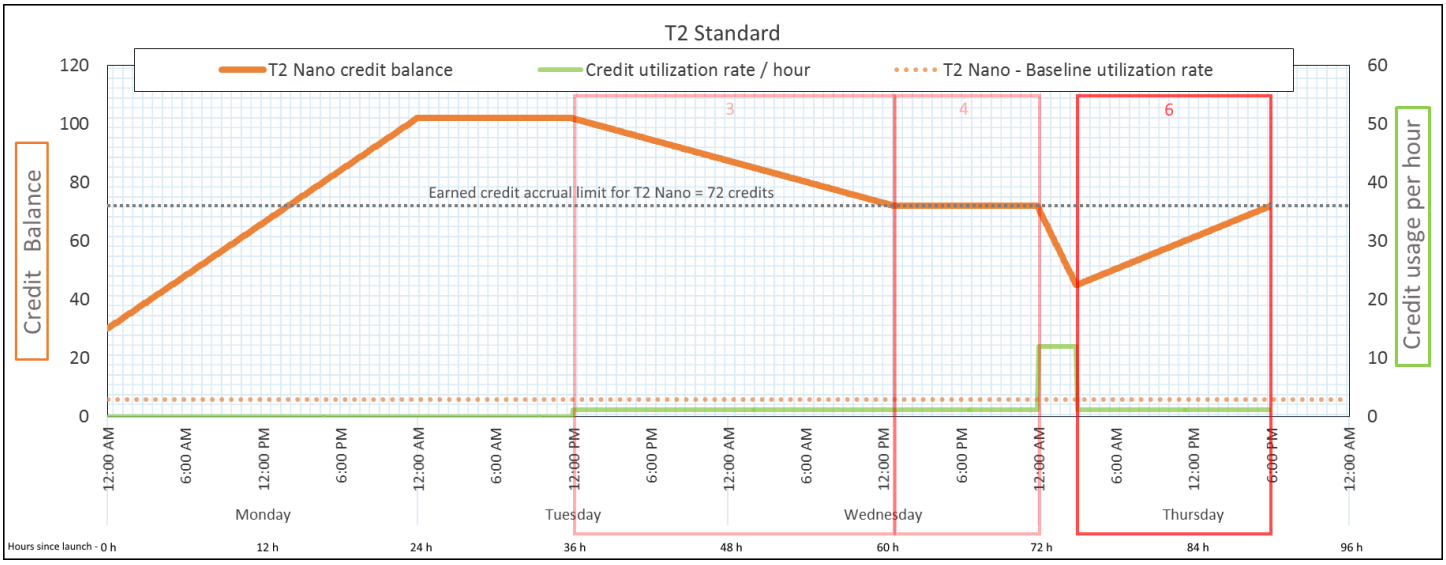
Se uma instância gastar mais créditos do que ganhar, seu balanço diminuirá.

Período 6: 76 a 90 horas

Nas próximas 15 horas, a instância usa 2% da CPU. Isso requer 18 créditos. Esta é a mesma utilização da CPU que nos períodos 3 e 4. No entanto, o saldo aumenta nesse período, embora tenha diminuído no Período 3 e estabilizado no Período 4.

No Período 3, os créditos de execução acumulados foram gastos. Todos os créditos ganhos que ultrapassaram o limite foram descartados, resultando em uma diminuição do saldo de crédito.
No Período 4, a instância gastou menos créditos do que ganhou. Todos os créditos ganhos que ultrapassaram o limite foram descartados. Portanto, o saldo se estabilizou no máximo de 72 créditos.

Nesse período, não há créditos de execução acumulados, e o número de créditos ganhos acumulados no saldo está abaixo do limite. Nenhum crédito ganho é descartado. Além disso, a instância ganha mais créditos do que gasta, resultando em um aumento do saldo de crédito.



Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 18— créditos em 15 horas

Taxa de ganhos de crédito	72 créditos por 24 horas (45 créditos em 15 horas)
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	72 créditos (o saldo aumenta a uma taxa de 43,2 créditos por 24 horas – taxa— de alterações = taxa de gastos de 28,8/24 + taxa de ganhos de 72/24)

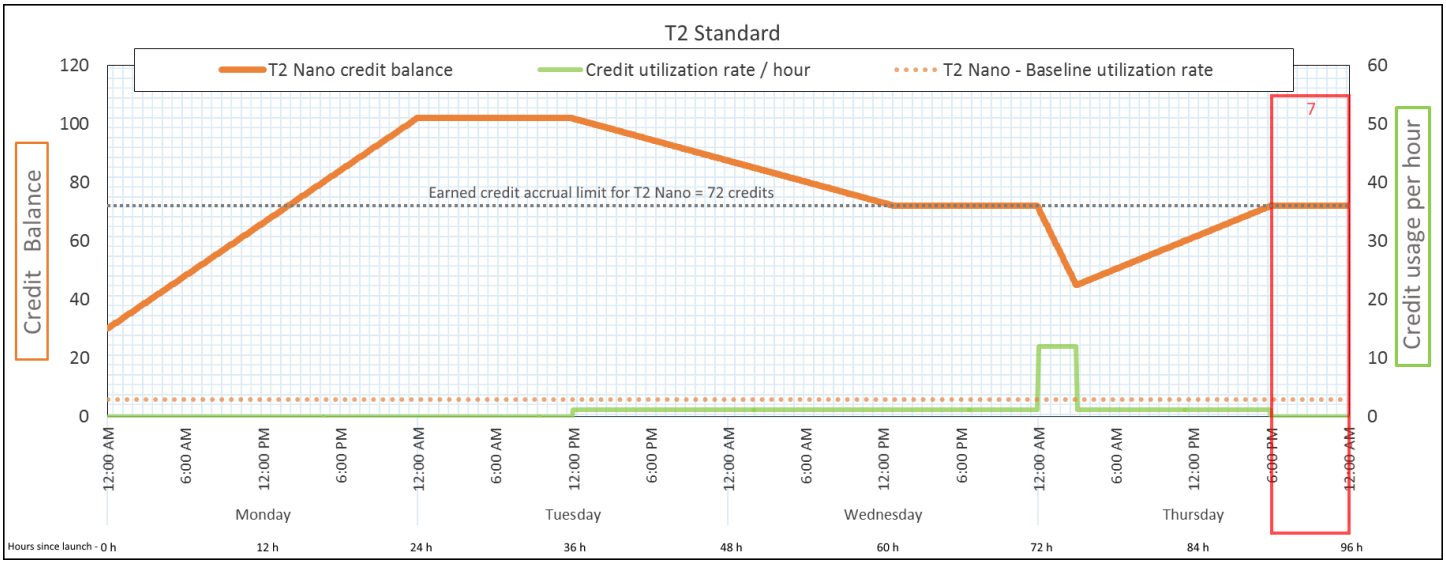
Conclusão

Se uma instância gastar menos créditos do que ganhar, seu saldo aumentará.

Período 7: 91 a 96 horas

Nas próximas seis horas, a instância permanecerá inativa —a utilização da CPU será de 0%— e nenhum crédito será gasto. Esse é o mesmo uso da CPU que no Período 2, mas o saldo não é estabilizado em 102 créditos. Ele se estabiliza em 72 créditos, —que é o limite para a instância.

No Período 2, o saldo incluiu 30 créditos de execução acumulados. OS créditos de execução foram gastos no Período 3. Uma instância em execução não pode obter mais créditos de execução. Quando o limite de saldo é atingido, os créditos ganhos ultrapassados são descartados.



Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)

Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos)

Conclusão

Uma instância ganha constantemente créditos, mas, se atingir o limite, não poderá acumular mais créditos. Assim que o limite é atingido, os créditos ganhos mais recentemente são descartados. O limite de saldo de crédito é determinado pelo número de créditos que uma instância pode ganhar em 24 horas. Para obter mais informações sobre os limites de saldo de crédito, consulte a Tabela de créditos.

Trabalhar com instâncias expansíveis

As etapas para a execução, monitoramento e modificação de instâncias de desempenho expansível (instâncias T) são semelhantes. A principal diferença é a especificação de crédito padrão na execução.

Cada família de instâncias T vem com a seguinte especificação de crédito padrão:

- As instâncias T4g, T3a e T3 são iniciadas como `unlimited`
- Instâncias T3 em um host dedicado são iniciadas como `standard`
- As instâncias T2 são executadas como `standard`

Você pode alterar a especificação de crédito padrão para a conta.

Conteúdo

- Iniciar uma instância expansível como ilimitada ou padrão
- Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada
- Exibir a especificação de crédito de uma instância expansível
- Modificar a especificação de crédito de uma instância expansível
- Definir a especificação de crédito padrão para a conta

- Visualizar a especificação de crédito padrão

Iniciar uma instância expansível como ilimitada ou padrão

É possível executar suas instâncias T como `unlimited` ou `standard` usando o console do Amazon EC2, um AWS SDK, uma ferramenta da linha de comando ou um grupo do Auto Scaling.

Os procedimentos a seguir descrevem como usar o console do EC2 ou a AWS CLI. Para obter informações sobre o uso de um grupo do Auto Scaling, consulte Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada.

Console

Para iniciar uma instância T como ilimitada ou padrão

1. Siga o procedimento para iniciar uma instância.
2. Em Instance type (Tipo de instância), selecione um tipo de instância T.
3. Expanda Advanced details (Detalhes avançados) e, em Credit specification (Especificação de crédito), selecione uma opção de crédito. Caso você não realize uma seleção, o padrão será aplicado. O padrão para a instância T2 é `standard`, e para as instâncias T4g, T3a e T3, é `unlimited`.
4. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

AWS CLI

Para iniciar uma instância T como ilimitada ou padrão

Use o comando run-instances para executar suas instâncias. Especifique a opção de crédito usando o parâmetro `--credit-specification CpuCredits=`. As opções de crédito válidas são `unlimited` e `standard`.

- Para as instâncias T4g, T3a e T3, se você não incluir o parâmetro `--credit-specification`, a instância será iniciada como `unlimited` por padrão.
- Para T2, se você não incluir o parâmetro `--credit-specification`, a instância será executada como `standard` por padrão.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada

Quando as instâncias T são executadas ou iniciadas, elas precisam de créditos de CPU para uma boa experiência de bootstrapping. Se você usar um grupo do Auto Scaling para executar suas instâncias, recomendamos configurar suas instâncias como `unlimited`. Caso faça isso, as instâncias usam créditos excedentes quando são automaticamente iniciadas ou reiniciadas pelo grupo do Auto Scaling. O uso de créditos excedentes impede restrições de performance.

Criar um modelo de execução

Use um modelo de execução para executar instâncias como `unlimited` em um grupo do Auto Scaling. Uma configuração de execução não oferece suporte à execução de instâncias como `unlimited`.

> **Note**
>
> O modo `unlimited` não é compatível com instâncias T3 que são iniciadas em um host dedicado.

Console

Para criar um modelo de inicialização que execute instâncias como ilimitadas

1. Siga o procedimento Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.
2. Em Launch template contents (Conteúdo do modelo de execução), para Instance type (Tipo de instância), escolha um tamanho de instância.
3. Para iniciar instâncias como `unlimited` em um grupo do Auto Scaling, em Advanced details (Detalhes avançados), para Credit specification (Especificação de crédito), escolha Unlimited (Ilimitado).

4. Ao terminar de definir os parâmetros do modelo de execução, escolha Create launch template (Criar modelo de execução).

AWS CLI

Para criar um modelo de inicialização que execute instâncias como ilimitadas

Use o comando create-launch-template e especifique `unlimited` como a opção de crédito.

- Para as instâncias T4g, T3a e T3, se você não incluir o valor `CreditSpecification={CpuCredits=unlimited}`, a instância será iniciada como `unlimited` por padrão.
- Em T2, se você não incluir o valor `CreditSpecification={CpuCredits=unlimited}`, a instância será executada como `standard` por padrão.

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
    --version-description FirstVersion \
    --launch-template-data
 ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Associar um grupo de Auto Scaling a um modelo de execução

Para associar o modelo de execução a um grupo do Auto Scaling, crie o grupo do Auto Scaling usando o modelo de execução ou adicione o modelo de execução a um grupo do Auto Scaling existente.

Console

Para criar um grupo do Auto Scaling usando um modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione a mesma região usada ao criar o modelo de execução.
3. No painel de navegação, escolha Auto Scaling Groups, Criar grupo do Auto Scaling.
4. Escolha Launch Template (Modelo de execução), selecione seu modelo de execução e, seguida, Next Step (Próxima etapa).

5. Preencha os campos para o grupo do Auto Scaling. Quando você terminar de revisar as definições de configuração na Review page (Página de revisão), selecione Create Auto Scaling group (Criar grupo do Auto Scaling). Para obter mais informações, consulte Criação de um grupo do Auto Scaling usando um modelo de execução no Guia do usuário do Amazon EC2 Auto Scaling.

AWS CLI

Para criar um grupo do Auto Scaling usando um modelo de inicialização

Use o comando create-auto-scaling-group da AWS CLI e especifique o parâmetro `--launch-template`.

Console

Para adicionar um modelo de inicialização a um grupo do Auto Scaling existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione a mesma região usada ao criar o modelo de execução.
3. No painel de navegação, escolha Groups Auto Scaling.
4. Na lista de grupos do Auto Scaling, selecione um grupo do Auto Scaling, Actions (Ações) e Edit (Editar).
5. Na guia Details (Detalhes), em Launch Template (Modelo de execução), selecione um modelo de execução e, em seguida, selecione Save (Salvar).

AWS CLI

Para adicionar um modelo de inicialização a um grupo do Auto Scaling existente

Use o comando update-auto-scaling-group da AWS CLI e especifique o parâmetro `--launch-template`.

Exibir a especificação de crédito de uma instância expansível

É possível visualizar a especificação de crédito (`unlimited` ou `standard`) de uma instância T em execução ou interrompida.

Console

Para visualizar a especificação de crédito de uma instância T

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Details (Detalhes) e exiba o campo Credit specification (Especificação de crédito). O valor é `unlimited` ou `standard`.

AWS CLI

Para descrever a especificação de crédito de uma instância T

Use o comando describe-instance-credit-specifications. Se você não especificar um ou mais IDs de instâncias, todas as instâncias com a especificação de crédito `unlimited` serão retornadas, bem como as instâncias que foram previamente configuradas com a especificação de crédito `unlimited`. Por exemplo, se você redimensionar uma instância T3 para uma instância M4, enquanto a mesma estiver configurada como `unlimited`, o Amazon EC2 retornará a instância M4.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Exemplo de saída

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

Modificar a especificação de crédito de uma instância expansível

É possível alterar a qualquer momento entre `unlimited` e `standard` a especificação de crédito de uma instância T interrompida ou em execução.

Observe que, no modo `unlimited`, uma instância pode gastar créditos excedentes, o que pode gerar uma cobrança adicional. Para ter mais informações, consulte Os créditos excedentes podem gerar cobranças.

Console

Para modificar a especificação de crédito de uma instância T

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância. Para modificar a especificação de crédito para várias instâncias de uma vez, selecione todas as instâncias aplicáveis.
4. Escolha Actions (Ações), Instance settings (Configurações de instância), Change credit specification (Alterar especificação de crédito). Essa opção só será ativada se você tiver selecionado uma instância T.
5. Para alterar a especificação de crédito para `unlimited`, marque a caixa de seleção ao lado do ID da instância. Para alterar a especificação de crédito para `standard`, desmarque a caixa de seleção ao lado do ID da instância.

AWS CLI

Para modificar a especificação de crédito de uma instância T

Use o comando modify-instance-credit-specification. Especifique a instância e sua opção de crédito usando o parâmetro `--instance-credit-specification`. As opções de crédito válidas são `unlimited` e `standard`.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Exemplo de saída

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
```

```
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Definir a especificação de crédito padrão para a conta

Cada família de instâncias T vem com uma especificação de crédito padrão. É possível alterar a especificação de crédito padrão por família de instâncias T no nível da conta por região da AWS.

Se você usar o assistente de inicialização de instância no console do EC2 para iniciar instâncias, o valor selecionado para a especificação de crédito substituirá a especificação de crédito padrão no nível da conta. Se você usar a AWS CLI para executar instâncias, todas as novas instâncias T na conta serão executadas usando a opção de crédito padrão. A especificação de crédito para instâncias existentes em execução ou interrompidas não é afetada.

Consideração

A especificação de crédito padrão para uma família de instâncias pode ser modificada apenas uma vez em um período contínuo de 5 minutos e até quatro vezes em um período contínuo de 24 horas.

Console

Para definir a especificação de crédito padrão no nível da conta por região

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
4. Em Account attributes (Atributos da conta), escolha Default credit specification (Especificação de crédito padrão).
5. Escolha Gerenciar.
6. Para cada família de instâncias, escolha Unlimited (Ilimitado) ou Standard (Padrão) e, em seguida, escolha Update (Atualizar).

AWS CLI

Como definir a especificação de crédito padrão no nível da conta (AWS CLI)

Use o comando modify-default-credit-specification. Especifique a região da AWS, a família de instâncias e a especificação de crédito padrão usando o parâmetro `--cpu-credits`. As especificações de crédito padrão válidas são `unlimited` e `standard`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

Visualizar a especificação de crédito padrão

É possível visualizar a especificação de crédito padrão de uma família de instâncias T no nível da conta por região da AWS.

Console

Para visualizar a especificação de crédito padrão no nível da conta

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
4. Em Account attributes (Atributos da conta), escolha Default credit specification (Especificação de crédito padrão).

AWS CLI

Para visualizar a especificação de crédito padrão no nível da conta

Use o comando get-default-credit-specification. Especifique a região da AWS e a família de instâncias.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Monitore seus créditos da CPU para instâncias expansíveis

O EC2 envia métricas para o Amazon CloudWatch. Você pode ver as métricas de crédito da CPU nas métricas do Amazon EC2 por instância do console do CloudWatch ou usando a AWS CLI para

listar as métricas de cada instância. Para ter mais informações, consulte Listar métricas usando o console e Listar métricas usando o AWS CLI.

Conteúdo

- Métricas adicionais do CloudWatch para instâncias expansíveis
- Calcular o uso de crédito da CPU

Métricas adicionais do CloudWatch para instâncias expansíveis

As instâncias expansíveis têm estas métricas adicionais do CloudWatch, que são atualizadas a cada cinco minutos:

- `CPUCreditUsage` – O número de créditos de CPU gastos durante o período de medição.
- `CPUCreditBalance` – o número de créditos de CPU que uma instância acumulou. Esse saldo é esgotado quando a CPU apresenta expansãos e os créditos de CPU são gastos com mais rapidez do que são ganhos.
- `CPUSurplusCreditBalance` – O número de créditos de CPU excedentes gastos para sustentar a utilização de CPU quando o valor de `CPUCreditBalance` for zero.
- `CPUSurplusCreditsCharged` – o número de créditos de CPU excedentes que ultrapassam o número máximo de créditos de CPU que podem ser ganhos em um período de 24 horas, resultando em uma cobrança adicional.

Essas duas últimas métricas aplicam-se somente a instâncias configuradas como `unlimited`.

A tabela a seguir descreve as métricas do CloudWatch para instâncias expansíveis. Para ter mais informações, consulte Listar as métricas disponíveis do CloudWatch para as instâncias.

Métrica	Descrição
`CPUCreditUsage`	O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos).

Métrica	Descrição
	As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística `Sum` em vez da estatística `Average`. Unidades: créditos (minutos de vCPU)
`CPUCreditBalance`	O número de créditos ganhos de CPU que uma instância acumulou desde que foi executada ou iniciada. Para a T2 Padrão, o `CPUCreditBalance` também inclui o número de créditos de execução que foram acumulados. Os créditos são acumulados no saldo de créditos após terem sido ganhos e são removidos do saldo de créditos quando são gastos. O saldo de crédito tem um limite máximo, determina do pelo tamanho da instância. Depois que o limite for atingido, todos os novos créditos ganhos serão descartados. Para a T2 Padrão, os créditos de execução não são contabilizados para o limite. Os créditos do `CPUCreditBalance` são disponibilizados para que a instância gaste e apresente intermitência com uma utilização de CPU acima da linha de base. Quando uma instância está em execução, os créditos do `CPUCreditBalance` não expiram. Quando uma instância T4g, T3a ou T3 é interrompida, o valor de `CPUCredit Balance` persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor `CPUCreditBalance` não persiste, e todos os créditos acumulados são perdidos. As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos. Unidades: créditos (minutos de vCPU)

Métrica	Descrição
`CPUSurplusCreditBalance`	O número de créditos excedentes gastos por uma instância `unlimited` quando seu valor `CPUCreditBalance` é zero. O valor `CPUSurplusCreditBalance` é pago pelos créditos de CPU ganhos. Se o número de créditos excedentes ultrapassar o número máximo de créditos que a instância pode ganhar em um período de 24 horas, os créditos excedentes gastos acima do limite máximo incorrerão em uma taxa adicional. Unidades: créditos (minutos de vCPU)
`CPUSurplusCreditsCharged`	O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional. Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre: • Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora. • A instância é interrompida ou encerrada. • A instância é alterada de `unlimited` para `standard`. Unidades: créditos (minutos de vCPU)

Calcular o uso de crédito da CPU

O uso de créditos de CPU de instâncias é calculado por meio das métricas de instância do CloudWatch descritas na tabela anterior.

O Amazon EC2 envia as métricas ao CloudWatch a cada cinco minutos. Uma referência ao valor anterior de uma métrica em qualquer momento implica o valor anterior da métrica, enviado cinco minutos atrás.

Calcular uso de créditos de CPU de instâncias padrão

- O saldo de crédito de CPU aumentará se a utilização de CPU ficar abaixo da linha de base, quando os créditos gastos forem inferiores aos créditos ganhos no intervalo anterior de cinco minutos.
- O saldo de crédito de CPU diminuirá se a utilização de CPU ficar acima da linha de base, quando os créditos gastos forem superiores aos créditos ganhos no intervalo anterior de cinco minutos.

Matematicamente, isso é capturado pela equação a seguir:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

O tamanho da instância determina o número de créditos que a instância pode ganhar por hora e o número de créditos ganhos que ela pode acumular no saldo de créditos. Para obter informações sobre o número de créditos ganhos por hora e o limite de saldo de créditos para cada tamanho de instância, consulte a Tabela de créditos.

Exemplo

Este exemplo usa uma instância `t3.nano`. Para calcular o valor `CPUCreditBalance` da instância, use a equação anterior, da seguinte maneira:

- `CPUCreditBalance` – O saldo de crédito atual a ser calculado.
- `prior CPUCreditBalance` – O saldo de crédito de cinco minutos atrás. Neste exemplo, a instância acumulou dois créditos.
- `Credits earned per hour` – A instância `t3.nano` ganha seis créditos por hora.
- `5/60` – Representa o intervalo de cinco minutos entre a publicação da métrica do CloudWatch. Multiplique os créditos ganhos a cada hora por 5/60 (cinco minutos) para obter o número de créditos que a instância ganhou nos últimos cinco minutos. A instância `t3.nano` ganha 0,5 crédito a cada cinco minutos.
- `CPUCreditUsage` – Quantos créditos a instância gastou nos últimos cinco minutos. Neste exemplo, a instância gastou um crédito nos últimos cinco minutos.

Com esses valores, é possível calcular o valor `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Cálculo de uso de créditos de CPU de instâncias ilimitadas

Quando uma instância expansível precisa ter uma expansão acima da linha de base, ela sempre gasta os créditos acumulados antes dos créditos excedentes. Quando ela esgotar o saldo de crédito de CPU acumulado, poderá gastar os créditos excedentes para expansão de CPU enquanto precisar. Quando a utilização de CPU ficar abaixo da linha de base, os créditos excedentes sempre serão pagos antes que a instância acumule créditos ganhos.

Usamos o termo `Adjusted balance` nas equações a seguir para refletir a atividade que ocorre nesse intervalo de cinco minutos. Usamos esse valor para atingir os valores das métricas do `CPUCreditBalance` de `CPUSurplusCreditBalance` e CloudWatch.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

O valor `0` em `Adjusted balance` indica que a instância gastou todos os créditos ganhos para expansão e nenhum crédito excedente foi gasto. Consequentemente, `CPUCreditBalance` e `CPUSurplusCreditBalance` são definidos como `0`.

Um valor `Adjusted balance` positivo indica que a instância acumulou créditos ganhos, e os créditos excedentes anteriores (se houver) foram pagos. Consequentemente, o valor de `Adjusted balance` é atribuído a `CPUCreditBalance`, e `CPUSurplusCreditBalance` é definido como `0`. O tamanho da instância determina o número máximo de créditos que ela pode acumular.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

O valor `Adjusted balance` negativo indica que a instância gastou todos os créditos ganhos acumulados e também os créditos excedentes gastos para expansão. Consequentemente, o valor de `Adjusted balance` é atribuído a `CPUSurplusCreditBalance`, e `CPUCreditBalance` é definido como `0`. Novamente, o tamanho da instância determina o número máximo de créditos que ela pode acumular.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Se os créditos excedentes gastos ultrapassarem o máximo de créditos que a instância pode acumular, o saldo de créditos excedentes será definido como o número máximo, conforme exibido na equação anterior. Os créditos excedentes restantes serão cobrados conforme representados pela métrica `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Por fim, quando a instância for encerrada, todos os créditos excedentes monitorados pelo `CPUSurplusCreditBalance` serão cobrados. Se a instância for alterada de `unlimited` para `standard`, todo o `CPUSurplusCreditBalance` restante também será cobrado.

Aceleração de desempenho com instâncias de GPU

As instâncias baseadas em GPU concedem acesso a GPUs NVIDIA com milhares de núcleos de computação. É possível essas instâncias para acelerar aplicações científicas, de engenharia e renderização utilizando as estruturas de computação paralela CUDA ou Open Computing Language (OpenCL). Também é possível usá-las para aplicações gráficas, incluindo transmissão de jogos, transmissão de aplicações 3-D e outras workloads gráficas.

Antes de ativar ou otimizar uma instância baseada em GPU, é necessário instalar os drivers apropriados, da seguinte forma:

- Para instalar drivers da NVIDIA em uma instância com uma GPU da NVIDIA conectada, como uma instância P3 ou G4dn, consulte Instalar drivers NVIDIA.
- Para instalar drivers da AMD em uma instância com uma GPU da AMD conectada, como uma instância G4ad, consulte Instalar drivers AMD.

Conteúdo

- Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2
- Otimização das configurações de GPU em instâncias do Amazon EC2

- Configuração de monitores Dual 4K em instâncias G4ad do Linux
- Como começar a usar instâncias P5 para o Linux

Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2

Para ativar as Aplicações GRID Virtual em instâncias baseadas em GPU que usam GPUs da NVIDIA (a NVIDIA GRID Virtual Workstation está habilitada por padrão), é necessário definir o tipo de produto para o driver, conforme apresentado a seguir.

Ativação de Aplicações GRID Virtual em instâncias do Linux

1. Crie o arquivo `/etc/nvidia/gridd.conf` a partir do arquivo de modelo fornecido.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Abra o arquivo `/etc/nvidia/gridd.conf` no editor de texto favorito.
3. Localize a linha `FeatureType` e defina-a como igual a `0`. Em seguida, adicione uma linha com `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Salve o arquivo e saia.
5. Reinicialize a instância para obter a nova configuração.

   ```
   [ec2-user ~]$ sudo reboot
   ```

Ativação de Aplicações GRID Virtual em instâncias do Windows

Ativação de Aplicações GRID Virtual em instâncias do Windows

1. Execute regedit.exe para abrir o editor do registro.
2. Navegue até `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
4. Em Nome, digite FeatureType e `Enter`.

5. Abra o menu de contexto (clique com o botão direito do mouse) em FeatureType e escolha Modify.
6. Para Dados de valor, insira `0` para NVIDIA Grid Virtual Applications e escolha OK.
7. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
8. Em Name, digite IgnoreSP e pressione `Enter`.
9. Abra o menu de contexto (clique com o botão direito do mouse) em IgnoreSP e escolha Modify.
10. Em Value data, digite 1 e escolha OK.
11. Feche o editor de Registro.

Otimização das configurações de GPU em instâncias do Amazon EC2

Há várias otimizações de configuração de GPU que é possível executar para obter a melhor performance nas instâncias GPU NIVIDIA. Com alguns desses tipos de instância, o driver NVIDIA usa um recurso de autoboost, que varia as velocidades de clock da GPU. Ao desativar o recurso de autoboost e definir as velocidades de clock de GPU como a frequência máxima, você pode atingir a performance máxima de forma consistente com suas instâncias de GPU.

Otimização das configurações de GPU no Linux

1. Defina as configurações de GPU para serem persistentes. Esse comando pode levar vários minutos para ser executado.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Somente para instâncias G3 e P2] Desabilite o recurso de autoboost para todas as GPUs na instância.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Defina todas as velocidades de relógio de GPU como a frequência máxima. Use a memória e as velocidades de relógio de placa gráfica especificadas nos seguintes comandos.

   Algumas versões do driver NVIDIA não suportam a configuração da velocidade de clock da aplicação e exibem o erro `"Setting applications clocks is not supported for GPU..."`, que é possível ignorar.

   - Instâncias G3:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

- Instâncias G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instâncias G5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instâncias G6 e Gr6:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- Instâncias P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- Instâncias P3 e P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Instâncias P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instâncias P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instâncias P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Otimização das configurações de GPU no Windows

1. Abra uma janela do PowerShell e navegue para a pasta de instalação NVIDIA.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\"
```

2. [Somente para instâncias G3 e P2] Desabilite o recurso de autoboost para todas as GPUs na instância.

```
.\nvidia-smi --auto-boost-default=0
```

3. Defina todas as velocidades de relógio de GPU como a frequência máxima. Use a memória e as velocidades de relógio de placa gráfica especificadas nos seguintes comandos.

   Algumas versões do driver NVIDIA não suportam a configuração da velocidade de clock da aplicação e exibem o erro `"Setting applications clocks is not supported for GPU..."`, que é possível ignorar.

   - Instâncias G3:

     ```
     .\nvidia-smi -ac "2505,1177"
     ```

   - Instâncias G4dn:

     ```
     .\nvidia-smi -ac "5001,1590"
     ```

   - Instâncias G5:

     ```
     .\nvidia-smi -ac "6250,1710"
     ```

   - Instâncias G6 e Gr6:

     ```
     .\nvidia-smi -ac "6251,2040"
     ```

   - Instâncias P2:

     ```
     .\nvidia-smi -ac "2505,875"
     ```

   - Instâncias P3 e P3dn:

     ```
     .\nvidia-smi -ac "877,1530"
     ```

   - Instâncias P4d:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
     ```

   - Instâncias P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instâncias P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Configuração de monitores Dual 4K em instâncias G4ad do Linux

Iniciar uma instância G4ad

1. Conecte-se à sua instância Linux para obter o endereço de barramento PCI da GPU a ser direcionado ao Dual 4K (2x4k):

   ```
   lspci -vv | grep -i amd
   ```

   Você terá um resultado semelhante ao seguinte:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. O endereço de barramento PCI é 00:1e.0 na saída acima. Crie um arquivo denominado `/etc/modprobe.d/amdgpu.conf` e adicione o seguinte:

   ```
   options amdgpu virtual_display=0000:00:1e.0,2
   ```

3. Para instalar drivers da AMD no Linux, consulte Instalação de drivers da AMD na instância do Amazon EC2. Se você já tiver o driver da GPU AMD instalado, precisará reconstruir os módulos do kernel amdgpu via dkms.

4. Utilize o arquivo xorg.conf abaixo para definir a topologia de tela dupla (2x4K) e salve o arquivo no `/etc/X11/xorg.conf:`

   ```
   ~$ cat /etc/X11/xorg.conf
   Section "ServerLayout"
       Identifier     "Layout0"
       Screen          0 "Screen0"
       Screen        1 "Screen1"
       InputDevice     "Keyboard0" "CoreKeyboard"
   ```

```
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
```

```
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Configure o DCV seguindo as instruções de configuração de um desktop interativo.
6. Quando a configuração do DCV terminar, reinicialize.
7. Verifique se o driver está funcional:

```
dmesg | grep amdgpu
```

A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

8. Você verá na saída de `DISPLAY=:0 xrandr -q` que existem dois monitores virtuais conectados:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
```

```
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Quando você se conectar ao DCV, altere a resolução para 2x4K, confirmando que o suporte de monitor duplo está registrado pelo DCV.

Como começar a usar instâncias P5 para o Linux

As instâncias P5 fornecem 8 GPUs NVIDIA H100 com 640 GB de memória de GPU com alta largura de banda. Elas oferecem processadores AMD EPYC de 3ª geração e fornecem 2 TB de memória de sistema, 30 TB de armazenamento de instância NVMe local, largura de banda da rede agregada de 3.200 Gbps e suporte a RDMA GPUDirect. As instâncias P5 também oferecem suporte à tecnologia Amazon EC2 UltraCluster, que fornece menor latência e melhor performance de rede usando o EFA.

A tabela a seguir fornece um resumo das especificações de `p5.48xlarge`.

vCPUs	Memória do sistema	GPUs	Memória da GPU	Largura de banda de rede	GPUDirect RDMA	GPU ponto a ponto	Armazenamento de instâncias
192	2 TiB	8 GPUs NVIDIA H100	HBM3 DE 640 GB	3200 Gbps com EFAv2	Compatível	Switch NV de 900 Gb/s	8 volumes SSD NVMe de 3.800 GB

Configuração de software

A maneira mais fácil de começar a usar instâncias P5 é iniciar uma instância usando um AWS Deep Learning AMI que está pré-configurado com todo o software necessário. Para o AWS Deep Learning AMI mais recente para uso com instâncias P5, consulte AWS Deep Learning Base GPU AMI (Ubuntu 20.04).

Se você precisar criar uma AMI personalizada para uso com instâncias P5, recomendamos instalar as seguintes versões mínimas de software:

- Driver NVIDIA 535.54.03 ou posterior
- CUDA 12.1 ou posterior
- NVIDIA GDRCopy 2.3 ou posterior
- Instalador EFA 1.24.1 ou posterior
- NCCL 2.18.3 ou posterior
- Plugin aws-ofi-nccl 1.7.2-aws ou posterior

Também recomendamos que você configure a instância para não usar estados C mais profundos. Para obter mais informações, consulte High performance and low latency by limiting deeper C-states no Amazon Linux 2 User Guide. A mais recente AMI de GPU básica de aprendizado profundo da AWS está pré-configurada para não usar estados C mais profundos.

Recomendações específicas do Ubuntu 20.04

As recomendações a seguir para o Ubuntu 20.04 ajudam a evitar a nomenclatura imprevisível da interface na inicialização.

- Verifique se você está executando `systemd 245.4-4ubuntu3.19` ou posterior com o seguinte comando:

```
systemd --version
```

- Verifique se você configurou o GRUB:
  - Abra o arquivo de configuração `/etc/default/grub` em um editor de texto.
  - Edite a entrada `GRUB_CMDLINE_LINUX_DEFAULT` para incluir `net.naming-scheme=v247`.
  - Reinicie sua instância executando `sudo update-grub`.

Configuração de rede e EFA

As instâncias P5 fornecem 3.200 Gbps de largura de banda de rede usando várias interfaces EFA. As instâncias P5 oferecem suporte a 32 placas de rede. Recomendamos que você defina uma única interface de rede EFA por placa de rede. Para configurar essas interfaces no lançamento, recomendamos as seguintes configurações:

- Para interface de rede `0`, especifique o índice de dispositivo `0`
- Para interface de rede `1` a `31`, especifique o índice de dispositivo `1`

Para obter mais informações sobre como configurar suas instâncias P5 para EFA, consulte Começar a usar instâncias P5 e EFA.

Instâncias Mac do Amazon EC2

As instâncias Mac do Amazon EC2 oferecem suporte nativo ao sistema operacional macOS.

- As instâncias Mac x86 do EC2 (`mac1.metal`) são criadas em hardware Mac mini 2018 baseado em processadores Intel de oitava geração (Coffee Lake) Core i7 de 3,2 GHz.
- As instâncias Mac M1 (`mac2.metal`) do EC2 são baseadas no hardware Mac mini 2020 e processadores Apple com chip M1.
- As instâncias Mac M1 Ultra (`mac2-m1ultra.metal`) do EC2 são baseadas no hardware Mac Studio 2022 e processadores Apple com chip M1 Ultra.

- As instâncias Mac M2 (`mac2-m2.metal`) do EC2 são baseadas no hardware Mac mini 2023 e processadores Apple com chip M2.
- As instâncias Mac M2 Pro (`mac2-m2pro.metal`) do EC2 são baseadas no hardware Mac mini 2023 e processadores Apple com chip M2 Pro.

As instâncias Mac do EC2 são ideais para desenvolver, criar, testar e assinar aplicações para plataformas Apple, como iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV e Safari. É possível se conectar à instância do Mac usando SSH ou Apple Remote Desktop (ARD).

> **Note**
>
> A unidade de faturamento é o host dedicado. As instâncias em execução nesse host não têm custo adicional.

Conteúdo

- Considerações
- Prontidão da instância
- AMIs do macOS do EC2
- EC2 MacOS Init
- Amazon EC2 System Monitor para macOS
- Recursos relacionados
- Iniciar uma instância Mac
- Conectar-se a instâncias Mac
- Atualizar o sistema operacional e o software em instâncias Mac
- Aumente o tamanho de um volume do EBS na instância do Mac
- Interromper e encerrar a instância do Mac
- Encontrar versões do macOS compatíveis para seu host dedicado Mac do Amazon EC2
- Assinar notificações de AMI do macOS
- Recuperar IDs de AMI do macOS usando a API do AWS Systems Manager Parameter Store
- Notas de lançamento das AMIs do Amazon EC2 para o macOS

Considerações

As seguintes considerações se aplicam às instâncias do Mac:

- As instâncias Mac só estão disponíveis como instâncias bare metal em hosts dedicados, com um período mínimo de alocação de 24 horas antes que seja possível liberar o host dedicado. É possível executar uma instância Mac por Host dedicado. É possível compartilhar o Host dedicado com as contas da AWS ou com unidades organizacionais na sua organização de AWS ou toda a organização da AWS.
- Instâncias Mac estão disponíveis em diferentes Regiões da AWS. Para obter uma lista da disponibilidade de instâncias Mac em cada uma das Regiões da AWS, consulte Tipos de instância do Amazon EC2 por região.
- As instâncias Mac estão disponíveis apenas como Instâncias on-demand. Elas não estão disponíveis como Instâncias spot ou Instâncias reservadas. É possível economizar dinheiro em instâncias Mac comprando um Savings Plan.
- As instâncias Mac podem executar um dos seguintes sistemas operacionais:
  - macOS Mojave (versão 10.14) (somente instâncias Mac x86)
  - macOS Catalina (versão 10.15) (somente instâncias Mac x86)
  - macOS Big Sur (versão 11) (instâncias Mac x86 e M1)
  - macOS Monterey (versão 12) (instâncias Mac x86 e M1)
  - macOS Ventura (versão 13) (todas as instâncias Mac M2 e M2 Pro Mac são compatíveis com o macOS Ventura versão 13.2 ou posterior)
  - macOS Sonoma (versão 14) (todas as instâncias do Mac)
- Há suporte para o hotplug do EBS.
- AWS não gerencia nem oferece suporte ao SSD interno no hardware Apple. Recomendamos enfaticamente usar os volumes do Amazon EBS em vez disso. Os volumes do EBS oferecem benefícios semelhantes de elasticidade, disponibilidade e durabilidade em instâncias Mac em comparação com qualquer outra instância do EC2.
- Recomendamos usar o SSD de uso geral (`gp2` e `gp3`) e o SSD de IOPS provisionadas (`io1` e `io2`) com instâncias Mac para obter a performance ideal para o EBS.
- Agora as instâncias Mac são compatíveis com o Amazon EC2 Auto Scaling.
- Em instâncias Mac x86, as atualizações automáticas de software estão desabilitadas. Recomendamos que você aplique as atualizações e as teste na sua instância antes de colocá-la

em produção. Para ter mais informações, consulte Atualizar o sistema operacional e o software em instâncias Mac.

- Quando você interrompe ou encerra uma instância do Mac, um fluxo de trabalho de depuração é executado no Host dedicado. Para ter mais informações, consulte Interromper e encerrar a instância do Mac.

> **Warning**
>
> Não use o FileVault. Ativar o FileVault fará com que o host não seja inicializado devido ao bloqueio das partições. Se houvere necessidade de criptografia de dados, use a criptografia do Amazon EBS para evitar problemas de inicialização e impacto na performance. Com a criptografia do Amazon EBS, as operações ocorrem nos servidores que hospedam instâncias, garantindo a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu armazenamento do EBS anexado. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS

Prontidão da instância

Depois de iniciar uma instância Mac, você precisará esperar até que a instância esteja pronta para se conectar a ela. Para uma AMI vendida pela AWS com uma instância Mac x86 ou uma instância Apple com chip Mac, o tempo de inicialização pode variar de 6 a 20 minutos aproximadamente. Dependendo dos tamanhos de volume escolhidos do Amazon EBS, da inclusão de scripts adicionais nos dados do usuário ou do software adicional carregado em uma AMI personalizada do macOS, o tempo de inicialização pode aumentar.

É possível usar um pequeno script de shell, como o abaixo, para pesquisar a API describe-instance-status para saber quando a instância está pronta para conexão. No comando a seguir, substitua o ID da instância do exemplo pelo ID da sua própria instância.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-0123456789example \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMIs do macOS do EC2

O macOS Amazon EC2 foi projetado para fornecer um ambiente estável, seguro e de alta performance para workloads de desenvolvedores executadas em instâncias Mac do Amazon EC2. As AMIs do macOS do EC2 também incluem vários pacotes que permitem a fácil integração com o AWS, incluindo ferramentas de configuração de execução bibliotecas e ferramentas populares do AWS .

Para obter mais informações sobre as AMIs do EC2 para o macOS, consulte Notas de lançamento das AMIs do Amazon EC2 para o macOS.

A AWS fornece AMIs do EC2 para o macOS atualizadas regularmente, as quais incluem atualizações para pacotes de propriedade da AWS e a versão mais recente do macOS totalmente testada. Além disso, o AWS fornece AMIs atualizadas com as atualizações mais recentes da versão secundária ou da versão principal assim que elas puderem ser totalmente testadas e aprovadas. Se você não precisar preservar dados ou personalizações das instâncias Mac, poderá obter as atualizações mais recentes ao executar uma nova instância usando a AMI atual e encerrando a instância anterior. Caso contrário, é possível escolher quais atualizações se aplicam às instâncias Mac.

Para obter informações sobre como se tornar assinante de notificações da AMI para o macOS, consulte Assinar notificações de AMI do macOS.

EC2 MacOS Init

O EC2 macOS Init é usado para inicializar instâncias Mac do EC2 na inicialização. Ele usa grupos prioritários para executar grupos lógicos de tarefas ao mesmo tempo.

O arquivo plist launchd é `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Os arquivos do EC2 macOS Init estão localizados no `/usr/local/aws/ec2-macos-init`.

Para obter mais informações, consulte https://github.com/aws/ec2-macos-init.

Amazon EC2 System Monitor para macOS

O Amazon EC2 System Monitor para macOS fornece métricas de utilização de CPU para o Amazon CloudWatch. Ele envia essas métricas para o CloudWatch por meio de um dispositivo serial personalizado em períodos de 1 minuto. É possível ativar ou desativar este agente da seguinte forma. Ele é habilitado por padrão.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> No momento, não há suporte para o Amazon EC2 System Monitor para macOS por parte de instâncias Mac que usam processadores Apple Silicon.

Recursos relacionados

Para obter mais informações sobre definição de preços, consulte Definição de preço do .

Para obter mais informações sobre instâncias Mac, consulte Instâncias Mac do Amazon EC2.

Para obter mais informações sobre especificações de hardware e desempenho de rede de instâncias Mac, consulte Instâncias de uso geral.

Iniciar uma instância Mac

As instâncias Mac do EC2 exigem um host dedicado. Primeiro, você precisa alocar um host para sua conta e depois iniciar a instância no host.

É possível iniciar uma instância usando o AWS Management Console ou a AWS CLI.

Executar uma instância do Mac usando o console

Para executar uma instância Mac em um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Aloque o host dedicado da seguinte forma:
   a. No painel de navegação, selecione Hosts dedicados.
   b. Escolha Allocate (Alocar) Host dedicado e, em seguida, faça o seguinte:
      i. Em Família de instâncias, escolha mac1, mac2, mac2-m2, mac2-m2pro ou mac2-m1ultra. Se a família de instâncias não aparecer na lista, significa que ela não é compatível com a região selecionada no momento.
      ii. Em Tipo de instância, escolha mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal ou mac2-m1ultra com base na família de instâncias escolhida.

iii. Em Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade do Host dedicado.

iv. Em Quantity (Quantidade), mantenha 1.

v. Escolha Allocate.

3. Inicie a instância no host da seguinte forma:

a. Selecione o Host dedicado que você criou e, em seguida, faça o seguinte:

i. Escolha Actions (Ações), Launch instances onto host (Iniciar instâncias no host).

ii. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI do macOS.

iii. Em Tipo de instância, selecione o tipo de instância apropriado (mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal ou mac2-m1ultra).

iv. Em Advanced details (Detalhes avançados), verifique se Tenancy (Locação), Tenancy host by (Host da locação até) e Tenancy host ID (ID do host da locação) estão pré-configurados com base no host dedicado que você criou. Atualize Tenancy affinity (Afinidade da locação) conforme necessário.

v. Conclua o assistente, especificando os volumes, grupos de segurança e pares de chaves do EBS conforme necessário.

vi. No painel Resumo painel, escolha Iniciar instância.

b. Uma página de confirmação informa que sua instância está sendo executada. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. O estado inicial de uma instância é `pending`. A instância está pronta quando seu estado muda para `running` e passa verificações de status.

Executar uma instância Mac usando o AWS CLI

Alocar o host dedicado

Use o comando allocate-hosts a seguir para alocar um host dedicado à instância Mac, substituindo o `instance-type` por `mac1.metal`, `mac2.metal`,`mac2-m2.metal` `mac2-m2pro.metal` ou `mac2-m1ultra.metal` e a `region` e a `availability-zone` pelas apropriadas para seu ambiente.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Iniciar a instância no host

Use o comando run-instances a seguir para iniciar uma instância Mac, substituindo novamente o `instance-type` por `mac1.metal`, `mac2.metal`, `mac2-m2.metal`, `mac2-m2pro.metal` ou `mac2-m1ultra.metal` e a `region` e a `availability-zone` pelas usadas anteriormente.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

O estado inicial de uma instância é `pending`. A instância está pronta quando seu estado muda para `running` e passa verificações de status. Use o comando describe-instance-status para exibir informações de status para a instância.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Veja a seguir um exemplo de saída para uma instância que está sendo executada e passou por verificações de status.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
```

```
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Conectar-se a instâncias Mac

Você pode se conectar à instância Mac usando o SSH ou uma interface gráfica do usuário.

Conectar a sua instância usando SSH

> **Important**
>
> Vários usuários podem acessar o sistema operacional simultaneamente. Normalmente, há uma sessão 1:1 de usuário:GUI devido ao serviço integrado de compartilhamento de tela na porta 5900. O uso do SSH no macOS é compatível com várias sessões até o limite de “Max Sessions” (Máximo de sessões) no arquivo sshd_config.

Por padrão, as instâncias Mac do Amazon EC2 não permitem SSH de raiz remota. A autenticação com senha é desabilitada para evitar ataques de força bruta em senhas. A conta ec2-user é configurada para login remoto usando SSH. A conta ec2-user também tem privilégios de sudo. Depois de se conectar à instância, é possível adicionar outros usuários.

Para oferecer suporte à conexão com a instância usando SSH, execute a instância usando um par de chaves e um grupo de segurança que permita acesso SSH e verifique se a instância tem conectividade com a Internet. Você fornece o arquivo `.pem` para o par de chaves quando se conecta à instância.

Use o procedimento a seguir para se conectar à instância MAC usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Para se conectar à sua instância usando SSH

1. Verifique se o computador local tem um cliente SSH instalado digitando ssh na linha de comando. Se o computador não reconhecer o comando, procure um cliente SSH para seu sistema operacional e instale-o.

2. Obtenha o nome público do DNS da sua instância. Usando o console do Amazon EC2, é possível encontrar o nome público do DNS nas guias Detalhes e Rede. Usando o AWS CLI, é possível encontrar o nome público do DNS usando o comando describe-instances.
3. Localize o arquivo `.pem` do par de chaves que você especificou quando executou a instância.
4. Conecte-se à instância usando o comando ssh, especificando o nome público do DNS da instância e do arquivo `.pem`.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Conecte-se à interface gráfica do usuário (GUI)

Use o procedimento a seguir para se conectar à instância usando o VNC, o Apple Remote Desktop (ARD) ou o aplicativo Apple Screen Sharing (incluído no macOS).

> **Note**
>
> O macOS 10.14 e posterior só permite o controle se o compartilhamento de tela estiver ativado por meio das Preferências do sistema.

Para se conectar à instância usando o cliente ARD ou o cliente VNC

1. Verifique se o computador local tem um cliente ARD ou um cliente VNC que suporte uma instalação do ARD. No macOS, é possível usar a aplicação de compartilhamento de tela integrado. Caso contrário, procure um cliente VNC para o sistema operacional e instale-o.
2. No computador local, conecte-se à instância usando SSH.
3. Defina uma senha para a conta ec2-user usando o comando passwd da seguinte forma.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Desconecte-se da sua instância digitando exit e pressionando Enter.

6. No computador, conecte-se à instância usando o comando ssh. Além das opções mostradas na seção anterior, use a opção -L para habilitar o encaminhamento de porta e encaminhar todo o tráfego na porta local 5900 para o servidor ARD na instância.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. No computador local, use o cliente ARD ou o cliente VNC com suporte a ARD para se conectar a `localhost:5900`. Por exemplo, use a aplicação de compartilhamento de tela no macOS da seguinte forma:

   a. Abra o Finder e selecione Ir.

   b. Selecione Conectar ao servidor.

   c. No campo Endereço do servidor, insira `vnc://localhost:5900`.

   d. Faça login conforme solicitado, usando **`ec2-user`** como nome de usuário e a senha que você criou para a conta ec2-user.

Modificar a resolução de tela do macOS em instâncias Mac

Depois de se conectar à instância Mac do EC2 usando ARD ou um cliente VNC compatível com ARD instalado, é possível modificar a resolução de tela do ambiente do macOS usando qualquer uma das ferramentas ou utilitários do macOS disponíveis publicamente, como o displayplacer.

Para modificar a resolução da tela usando o displayplacer

1. Instale o displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Mostre as informações atuais da tela e possíveis resoluções de tela.

```
[ec2-user ~]$ displayplacer list
```

3. Aplique a resolução de tela desejada.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

   Por exemplo:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Atualizar o sistema operacional e o software em instâncias Mac

> **Warning**
>
> A instalação das versões beta ou prévia do macOS está disponível somente nas instâncias Mac M1 do Amazon EC2. O Amazon EC2 não qualifica as versões beta ou prévia do macOS e não garante que as instâncias permaneçam funcionais após uma atualização para uma versão de pré-produção do macOS.
>
> A tentativa de instalação das versões beta ou prévia do macOS em instâncias do Mac x86 do Amazon EC2 levará à degradação do host dedicado do Mac do Amazon EC2 quando você interromper ou encerrar suas instâncias e impedirá que você inicie ou execute uma nova instância nesse host.

Etapas para atualizar o software em instâncias Mac do x86 e instâncias Apple com chip Mac.

- Atualizar o software em instâncias x86 do Mac
- Atualizar software em instâncias Mac com chip Apple

Atualizar o software em instâncias x86 do Mac

Em instâncias Mac x86, é possível instalar atualizações do sistema operacional da Apple usando o comando `softwareupdate`.

Para instalar atualizações do sistema operacional da Apple em instâncias Mac x86

1. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

```
[ec2-user ~]$ sudo softwareupdate --install label
```

Para instalar todas as atualizações, use o seguinte comando.

```
[ec2-user ~]$ sudo softwareupdate --install --all --restart
```

Os administradores de sistemas podem usar o AWS Systems Manager para implementar atualizações pré-aprovadas do sistema operacional em instâncias Mac x86. Para obter mais informações, consulte o Guia do usuário do AWS Systems Manager.

É possível usar o Homebrew para instalar atualizações em pacotes nas AMIs do EC2 para o macOS a fim de obter a versão mais recente desses pacotes nas instâncias. Também é possível usar o Homebrew para instalar e executar aplicações macOS comuns no macOS do Amazon EC2. Para obter mais informações, consulte a Documentação do Homebrew.

Para instalar atualizações usando o Homebrew

1. Atualize o Homebrew usando o seguinte comando.

```
[ec2-user ~]$ brew update
```

2. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

```
[ec2-user ~]$ brew outdated
```

3. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade package name
```

Para instalar todas as atualizações, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade
```

Atualizar software em instâncias Mac com chip Apple

Considerações

Driver do Adaptador de Rede Elástica (ENA)

Devido a uma atualização na configuração do driver de rede, a versão 1.0.2 do driver ENA não é compatível com o macOS 13.3 ou posterior. Se você quiser instalar qualquer versão macOS beta, prévia ou de produção 13.3 ou posterior e não tiver instalado o driver ENA mais recente, use o procedimento a seguir para instalar uma nova versão do driver.

Para instalar uma nova versão do driver ENA

1. Em uma janela do terminal, conecte-se à instância Mac com chip Apple usando SSH.
2. Baixe a aplicação ENA no arquivo `Applications` usando o comando a seguir.

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

> **Dica de solução de problemas**
>
> Se você receber o aviso `No available formula with the name amazon-ena-ethernet-dext`, execute o comando a seguir.
>
> ```
> [ec2-user ~]$ brew update
> ```

3. Desconecte-se da sua instância digitando exit e pressionando return.
4. Use o cliente VNC para ativar a aplicação ENA.
   a. Configure o cliente VNC usando Conecte-se à interface gráfica do usuário (GUI).
   b. Depois de se conectar à sua instância usando a aplicação de compartilhamento de tela, acesse a pasta Aplicações e abra a aplicação ENA.
   c. Selecione Ativar
   d. Para confirmar que o driver foi ativado corretamente, execute o comando a seguir na janela do terminal. A saída do comando mostra que o driver antigo está no estado de encerramento e o novo driver está no estado ativado.

```
systemextensionsctl list;
```

e. Depois de reiniciar a instância, somente o novo driver estará presente.

Atualização de software em instâncias Mac com chip Apple

Nas instâncias Mac com chip Apple, você deve concluir várias etapas para realizar uma atualização do sistema operacional no local. Primeiro, acesse o disco interno da instância usando a GUI com um cliente VNC (Virtual Network Computing). Esse procedimento usa o compartilhamento de tela do macOS, o cliente VNC integrado. Em seguida, delegue a propriedade ao usuário administrativo (`ec2-user`) fazendo login como`aws-managed-user` no volume do Amazon EBS.

Ao executar esse procedimento, você cria duas senhas. Uma senha é para o usuário administrativo (`ec2-user`) e a outra senha é para um usuário administrativo especial (`aws-managed-user`). Lembre-se dessas senhas, pois você as usará enquanto executar o procedimento.

> **Note**
>
> Com esse procedimento no macOS Big Sur, só é possível realizar pequenas atualizações, como a atualização do macOS Big Sur 11.7.3 para o macOS Big Sur 11.7.4. Para o macOS Monterey ou superior, é possível realizar grandes atualizações de software.

Para acessar o disco interno

1. No computador local, no terminal, conecte-se à instância Mac com chip Apple usando SSH com o comando a seguir. Para ter mais informações, consulte Conectar a sua instância usando SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

3. Defina uma senha para `ec2-user` com o comando a seguir. Lembre-se da senha, pois você a usará mais tarde.

   ```
   [ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

4. Desconecte-se da instância digitando exit e pressionando return.

5. No seu computador local, no terminal, reconecte-se à sua instância com um túnel SSH para a porta VNC usando o comando a seguir.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
```

> **Note**
>
> Não saia dessa sessão SSH até que as seguintes etapas de conexão VNC e GUI sejam concluídas. Quando a instância for reiniciada, a conexão se fechará automaticamente.

6. No computador local, conecte-se a `localhost:5900` usando as etapas a seguir:

   a. Abra o Finder e selecione Ir.

   b. Selecione Conectar ao servidor.

   c. No campo Endereço do servidor, insira `vnc://localhost:5900`.

7. Na janela do macOS, conecte-se à sessão remota da instância Mac com chip Apple como `ec2-user` com a senha que você criou na etapa 3.

8. Acesse o disco interno, chamado InternalDisk, usando uma das opções a seguir.

   a. Para macOS Ventura ou superior: abra as Configurações do sistema, selecione Geral no painel esquerdo e depois Disco de startup no canto inferior direito do painel.

   b. Para macOS Monterey ou inferior: abra as Preferências do sistema, selecione Disco de startup e desbloqueie o painel escolhendo o ícone de cadeado no canto inferior esquerdo da janela.

> **Dica de solução de problemas**
>
> Se você precisar montar o disco interno, execute o comando a seguir no terminal.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Escolha o disco interno, chamado InternalDisk, e selecione Reiniciar. Selecione Reiniciar novamente quando solicitado.

> **Important**
>
> Se o disco interno for denominado Macintosh HD em vez de InternalDisk, sua instância precisará ser interrompida e reiniciada para que o host dedicado possa ser atualizado. Para ter mais informações, consulte Interromper e encerrar a instância do Mac.

Use o procedimento a seguir para delegar a propriedade ao usuário administrativo. Ao se reconectar à sua instância com SSH, você fará a inicialização a partir do disco interno usando o usuário administrativo especial (`aws-managed-user`). A senha inicial de `aws-managed-user` é em branco, então você precisa sobrescrevê-la em sua primeira conexão. Em seguida, você precisará repetir as etapas para instalar e iniciar o compartilhamento de tela do macOS, pois o volume de inicialização foi alterado.

Para delegar a propriedade ao administrador de um volume do Amazon EBS

1. No seu computador local, no terminal, conecte-se à sua instância Mac com chip Apple usando o comando a seguir.

   ```
   ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
   ```

2. Ao receber o aviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, use um dos comandos a seguir para resolver esse problema.

   a. Limpe os hosts conhecidos usando o comando a seguir. Em seguida, repita a etapa anterior.

      ```
      rm ~/.ssh/known_hosts
      ```

   b. Adicione o seguinte ao comando SSH na etapa anterior.

      ```
      -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
      ```

3. Defina a senha do `aws-managed-user` com o comando a seguir. A senha inicial de `aws-managed-user` é em branco, então você precisa sobrescrevê-la em sua primeira conexão.

a.
```
[aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
```

b. Ao receber o aviso `Permission denied. Please enter user's old password:`, pressione enter.

> **Dica de solução de problemas**
>
> Se você receber o erro `passwd: DS error: eDSAuthFailed`, use o comando a seguir.
>
> ```
> [aws-managed-user ~]$ sudo passwd aws-managed-user
> ```

4. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Desconecte-se da instância digitando exit e pressionando return.

6. No seu computador local, no terminal, reconecte-se à sua instância com um túnel SSH para a porta VNC usando o comando a seguir.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
```

7. No computador local, conecte-se a `localhost:5900` usando as etapas a seguir:

   a. Abra o Finder e selecione Ir.

   b. Selecione Conectar ao servidor.

   c. No campo Endereço do servidor, insira `vnc://localhost:5900`.

8. Na janela do macOS, conecte-se à sessão remota da instância Mac com chip Apple como `aws-managed-user` com a senha que você criou na etapa 3.

> **Note**
>
> Quando solicitado a fazer login com seu Apple ID, selecione Configurar mais tarde.

9. Acesse o volume do Amazon EBS usando uma das opções a seguir.

   a. Para macOS Ventura ou superior: abra as Configurações do sistema, selecione Geral no painel esquerdo e depois Disco de startup no canto inferior direito do painel.

   b. Para macOS Monterey ou inferior: abra as Preferências do sistema, selecione Disco de startup e desbloqueie o painel escolhendo o ícone de cadeado no canto inferior esquerdo da janela.

   > **Note**
   >
   > Até que a reinicialização ocorra, quando for solicitada uma senha de administrador, use a senha que você definiu acima para `aws-managed-user`. Essa senha pode ser diferente da que você definiu para o `ec2-user` ou a conta de administrador padrão em sua instância. As instruções a seguir especificam quando usar a senha de administrador da sua instância.

10. Selecione o volume Amazon EBS (o volume não denominado InternalDisk na janela Disco de startup) e escolha Reiniciar.

    > **Note**
    >
    > Se você tiver vários volumes inicializáveis do Amazon EBS anexados à instância Mac com chip Apple, certifique-se de usar um nome exclusivo para cada volume.

11. Confirme a reinicialização e escolha Autorizar usuários quando solicitado.
12. No painel Autorizar usuário neste volume, verifique se o usuário administrativo (`ec2-user`, por padrão) está selecionado e selecione Autorizar.
13. Digite a senha do `ec2-user` que você criou na Etapa 3 do procedimento anterior e selecione Continuar.
14. Digite a senha do usuário administrativo especial (`aws-managed-user`) quando solicitado.
15. No computador local, no terminal, reconecte-se à instância usando SSH com o nome de usuário `ec2-user`.

> **Dica de solução de problemas**
>
> Se você receber o aviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, execute o comando a seguir e reconecte-se à sua instância usando SSH.
>
> ```
> rm ~/.ssh/known_hosts
> ```

16. Para realizar a atualização do software, use os comandos em Atualizar o software em instâncias x86 do Mac.

Aumente o tamanho de um volume do EBS na instância do Mac

É possível aumentar o tamanho dos volumes do Amazon EBS na sua instância do Mac. Para obter mais informações, consulte Volumes Elásticos do Amazon EBS no Guia do usuário do Amazon EBS.

Depois de aumentar o tamanho do volume, é necessário aumentar o tamanho do contêiner APFS da forma a seguir.

Disponibilizar maior espaço em disco para uso

1. Determine se uma reinicialização é necessária. Se você redimensionou um volume do EBS existente em uma instância Mac em execução, será necessário reinicializar a instância para disponibilizar o novo tamanho. Se a modificação do espaço em disco tiver sido feita durante o tempo de lançamento, não será necessária uma reinicialização.

   Exibir o status atual dos tamanhos de disco:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme           *322.1 GB     disk0
      1:                 EFI EFI                          209.7 MB     disk0s1
      2:                 Apple_APFS Container disk2       321.9 GB     disk0s2
   ```

2. Copie e cole o seguinte comando.

   ```
   [ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
   APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
   d" " -f8)
   ```

```
yes | sudo diskutil repairDisk $PDISK
```

3. Copie e cole o seguinte comando.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Interromper e encerrar a instância do Mac

Quando você interrompe uma instância do Mac, ela permanece no estado `stopping` por cerca de 15 minutos antes de entrar no estado `stopped`.

Quando uma instância do Mac é interrompida ou encerrada, o Amazon EC2 executa um fluxo de trabalho de depuração no host dedicado subjacente para apagar o SSD interno, limpar as variáveis NVRAM persistentes e, se necessário, atualizar o firmware do dispositivo para a versão mais recente. Isso garante que as instâncias Mac forneçam segurança e privacidade de dados semelhantes quando comparadas com outras instâncias do EC2 no Nitro. Isso também permite que você execute as AMIs mais recentes do macOS. Durante o fluxo de trabalho de depuração, o host dedicado entra temporariamente no estado de pendente. Em instâncias Mac x86, o fluxo de trabalho de limpeza pode levar até 50 minutos. Em instâncias Mac com chip Apple, o fluxo de trabalho de limpeza pode levar até 110 minutos. Além disso, nas instâncias Mac x86, se o firmware do dispositivo precisar ser atualizado, o fluxo de trabalho de limpeza poderá demorar até 3 horas.

Não é possível iniciar a instância do Mac interrompida ou iniciar uma nova instância do Mac até que o fluxo de trabalho de depuração seja concluído, momento no qual o estado Host dedicado entra no estado `available`.

A medição e o faturamento são pausados quando o host dedicado entra no estado `pending`. Você não será cobrado pela duração do fluxo de trabalho de depuração.

Libere o Host dedicado para a sua instância do Mac

Quando você terminar de usar a instância Mac, poderá liberar o Host dedicado. Antes de liberar o Host dedicado, é necessário interromper ou encerrar a instância Mac. Você não pode liberar o host até que o período de alocação exceda o mínimo de 24 horas.

Para liberar o Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância) ou Terminate instance (Encerrar instância).
4. No painel de navegação, selecione Hosts dedicados.
5. Selecione o Host dedicado e escolha Actions (Ações), Release host (Liberar host).
6. Quando for solicitada a confirmação, escolha Release (Liberar).

Encontrar versões do macOS compatíveis para seu host dedicado Mac do Amazon EC2

É possível ver as versões mais recentes do macOS compatíveis com seu host dedicado Mac do Amazon EC2. Com essa funcionalidade, você poderá validar a compatibilidade do seu host dedicado com execuções de instância com suas versões preferenciais do macOS.

Cada versão do macOS requer uma versão mínima de firmware no Apple Mac subjacente para uma execução bem-sucedida. A versão de firmware do Apple Mac pode ficar desatualizada se um host dedicado do Mac alocado tiver ficado inativo por um longo período de tempo ou tiver uma instância em execução há muito tempo.

Para garantir a compatibilidade com as versões mais recentes do macOS, você pode interromper ou encerrar instâncias no host dedicado Mac alocado. Isso vai acionar o fluxo de trabalho de limpeza de host e atualizar o firmware no respectivo Apple Mac para compatibilidade com as versões mais recentes do macOS. Um host dedicado com uma instância em execução há muito tempo será atualizado automaticamente quando você interromper ou encerrar uma instância em execução.

Para obter mais informações sobre o fluxo de trabalho de limpeza, consulte Interromper e encerrar a instância do Mac.

Para obter mais informações sobre como executar instâncias Mac, consulte Iniciar uma instância Mac.

É possível visualizar informações sobre as versões compatíveis mais recentes do macOS em seu host dedicado alocado usando o console do Amazon EC2 ou a AWS CLI.

Console

Para ver as informações do firmware do host dedicado usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Hosts dedicados.
3. Na página de Detalhes de hosts dedicados, em Versões mais recentes compatíveis do macOS, você poderá ver as versões mais recentes do macOS compatíveis com o host.

AWS CLI

Para ver as informações do firmware do host dedicado usando a AWS CLI

Use o comando `describe-mac-hosts`, substituindo `region` pela Região da AWS adequada.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

Assinar notificações de AMI do macOS

Para ser notificado sobre o lançamento de novas AMIs ou atualizações do bridgeOS, inscreva-se em notificações usando o Amazon SNS.

Para obter mais informações sobre as AMIs do macOS para EC2, consulte Notas de lançamento das AMIs do Amazon EC2 para o macOS.

Para assinar notificações de AMI do macOS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Use essa região porque as notificações do SNS nas quais está se inscrevendo foram criadas nessa região.
3. No painel de navegação, escolha Subscriptions.

4. Selecione Create subscription.
5. Na caixa de diálogo Create subscription, faça o seguinte:

   a. Em Topic ARN, copie e cole um dos seguintes nomes de recursos da Amazon (ARNs):

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Em Protocolo, escolha uma das seguinte opções:

      - E-mail:

        Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações. Após criar a assinatura, você receberá uma mensagem de confirmação com a linha de assunto `AWS Notification - Subscription Confirmation`. Abra o e-mail e escolha Confirm subscription (Confirmar assinatura) para concluir a assinatura

      - SMS:

        Em Endpoint, digite um número de telefone que é possível usar para receber as notificações.

      - AWS Lambda, Amazon SQS, Amazon Data Firehose (as notificações são recebidas no formato JSON):

        Em Endpoint, insira o ARN da função Lambda, fila SQS ou transmissão do Firehose que é possível usar para receber notificações.

   c. Selecione Criar assinatura.

Sempre que AMIs do macOS forem lançadas, enviaremos notificações aos assinantes do tópico `amazon-ec2-macos-ami-updates`. Sempre que houver uma atualização do bridgeOS , enviaremos notificações aos assinantes do tópico `amazon-ec2-bridgeos-updates`. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações de AMIs do macOS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Use essa região porque as notificações do SNS foram criada nessa região.
3. No painel de navegação, escolha Subscriptions.

4. Selecione as assinaturas e escolha Actions e Delete subscriptions. Quando solicitado a confirmar, escolha Delete.

Recuperar IDs de AMI do macOS usando a API do AWS Systems Manager Parameter Store

Você pode visualizar todas as AMIs do macOS em uma Região da AWS e recuperar a AMI mais recente do macOS consultando a API do AWS Systems Manager Parameter Store. Ao usar esses parâmetros públicos, não será necessário pesquisar manualmente IDs de AMI para o macOS. Os parâmetros públicos estão disponíveis para as AMIs do macOS x86 e ARM64 e podem ser integrados aos modelos do AWS CloudFormation existentes.

Permissões

A entidade principal do IAM que você usar deverá ter a permissão do IAM `ssm:GetParameter`.

Para visualizar uma lista de todas as AMIs do macOS na Região da AWS atual usando a AWS CLI

Use o comando get-parameters-by-path para visualizar uma lista de todas as AMIs do macOS na região atual.

```
aws ssm get-parameters-by-path --–path /aws/service/ec2-macos --–query
 "Parameters[].Name"
```

Para recuperar o ID da AMI principal mais recente do macOS usando a AWS CLI

Use o seguinte comando get-parameter com o subparâmetro `image_id`. No exemplo a seguir, substitua `sonoma` por uma versão principal compatível do macOS, `x86_64_mac` pelo processador e `region-code` por uma Região da AWS compatível para a qual você deseja o ID de AMI mais recente do macOS.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Para obter mais informações, consulte Chamar parâmetros públicos da AMI para macOS no Guia do usuário do AWS Systems Manager.

Notas de lançamento das AMIs do Amazon EC2 para o macOS

As informações apresentadas a seguir fornecem detalhes sobre os pacotes incluídos por padrão nas AMIs do EC2 para o macOS e resumem as alterações para cada lançamento da AMI do EC2 para o macOS.

Para obter informações sobre como se tornar assinante de notificações da AMI para o macOS, consulte Assinar notificações de AMI do macOS.

Pacotes padrão incluídos nas AMIs do Amazon EC2 para o macOS

A tabela apresentada a seguir descreve os pacotes incluídos por padrão nas AMIs do EC2 para o macOS.

Pacotes	Notas de release
EC2 macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2 macOS Utils	https://github.com/aws/ec2-macos-utils/tags
Amazon SSM Agent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) versão 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Ferramentas da linha de comando para Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Atualizações da AMI do Amazon EC2 para o macOS

A tabela apresentada a seguir descreve as alterações incluídas nos lançamentos da AMI do EC2 para o macOS. Observe que algumas alterações são aplicáveis a todas as AMIs do EC2 para o macOS, enquanto outras se aplicam apenas a um subconjunto dessas AMIs.

Atualizações da AMI do EC2 para o macOS

Versão	Alterações

2024.06.07	Todas as AMIs
	• Atualização do Homebrew para a versão 4.3.1-1
	• Atualização da `aws-cli` para a versão 2.15.56
	• Atualização do `amazon-ssm-agent` para a versão 3.3.380.0-1
	
	Lançamento do macOS Sonoma 14.5 (para todas as instâncias do Mac)
	• Conteúdo de segurança do macOS Sonoma 14.5
	
	Lançamento do macOS Ventura 13.6.7 (para todas as instâncias do Mac)
	• Conteúdo de segurança do macOS Ventura 13.6.7
	• Atualização do Safari para a versão 17.5
	  • Conteúdo de segurança do Safari 17.5
	
	Lançamento do macOS Monterey 12.7.5 (para todas as instâncias do Mac)
	• Conteúdo de segurança do macOS Monterey 12.7.5
	• Atualização do Safari para a versão 17.5
	  • Conteúdo de segurança do Safari 17.5

2024.04.12	Todas as AMIs • Atualização do Homebrew para a versão 4.2.16-1 • Atualização da `aws-cli` para a versão 2.15.36

Versão	Alterações

	Lançamento do macOS Sonoma 14.4.1 (para todas as instâncias Mac)
	• Conteúdo de segurança do macOS Sonoma 14.4.1
	
	Lançamento do macOS Ventura 13.6.6 (para todas as instâncias Mac)
	• Conteúdo de segurança do macOS Ventura 13.6.6
	• Atualização do Safari para a versão 17.4.1
	  • Conteúdo de segurança do Safari 17.4.1
	
	Para macOS Monterey (todas as instâncias Mac)
	• Atualização do Safari para a versão 17.4.1
	  • Conteúdo de segurança do Safari 17.4.1

Instâncias otimizadas para Amazon EBS

Uma instância otimizada para o Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade adicional dedicada para E/S do Amazon EBS. Essa otimização proporciona a melhor performance para seus volumes do EBS ao minimizar a contenção entre a E/S do Amazon EBS e outro tráfego de sua instância.

Instâncias otimizadas para o EBS oferecem largura de banda dedicada para o Amazon EBS. Quando anexados a uma instância otimizada para EBS, os volumes de SSD de uso geral (`gp2` e `gp3`) fornecem ao menos 90% de sua performance de IOPS provisionada, 99% do tempo em um determinado ano, e os volumes de SSD com IOPS provisionadas (`io1` e `io2`) fornecem ao menos 90% de sua performance de IOPS provisionadas, 99,9% do tempo em um determinado ano. HDD otimizado para throughput (`st1`) e HDD frio (`sc1`) fornecem ao menos 90% da performance esperada de throughput, 99% do tempo em um determinado ano. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da throughput total esperada a cada hora. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.

> **Important**
>
> A performance do EBS de uma instância é limitada pelos limites de performance da instância ou pela performance agregada dos seus volumes anexados, a que for menor. Para alcançar a performance máxima do EBS, uma instância deve ter volumes anexados que forneçam uma performance combinada igual ou superior à performance máxima da instância.
> Por exemplo, para obter `80,000` IOPS para`r6i.16xlarge`, a instância deve ter pelo menos 5 volumes `gp3` provisionados com `16,000` IOPS cada (5 volumes x `16,000` IOPS = `80,000` IOPS).

Escolha uma instância otimizada para EBS que forneça uma throughput do Amazon EBS mais dedicada do que o necessário para sua aplicação. Caso contrário, a conexão entre o Amazon EBS e o Amazon EC2 pode se tornar um gargalo de performance.

Há tipos de instância que são otimizados para EBS por padrão e tipos de instância que habilitam a otimização do EBS.

Conteúdo

- Otimizados para EBS por padrão
- Suporte à otimização do EBS
- Obtenha a máxima performance
- Exibir tipos de instâncias compatíveis com a otimização do EBS
- Habilitação da otimização do EBS na execução
- Habilitar a otimização do EBS para uma instância existente

Otimizados para EBS por padrão

Os tipos de instância a seguir são otimizados para EBS por padrão. Não é necessário habilitar a otimização para EBS, e nada ocorrerá se você desabilitá-la.

A tabela descreve a performance do EBS, incluindo a largura de banda dedicada ao Amazon EBS, o throughput máximo normal agregado que pode ser atingido nessa conexão com uma workload de leitura de transmissão e tamanho de E/S de 128 KiB, além de número máximo de IOPS para o qual a instância oferece suporte se você estiver usando um tamanho de E/S de 16 KiB.

Também é possível visualizar essas informações de maneira programática usando a AWS CLI. Para ter mais informações, consulte Exibir tipos de instâncias compatíveis com a otimização do EBS.

Performance do EBS

- Instâncias de uso geral
- Otimizadas para computação
- Otimizado para memória
- Otimizada para armazenamento
- Computação acelerada
- Computação de alta performance

Instâncias de uso geral

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
a1.medium [1]	300	3500	37,50	437,50	2500	20000
a1.large [1]	525	3500	65,62	437,50	4000	20000
a1.xlarge [1]	800	3500	100,00	437,50	6000	20000
a1.2xlarge [1]	1750	3500	218,75	437,50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	
a1.metal [2]	3500		437,5		20000	
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m4.2xlarge [2]	1000		125,0		8000	
m4.4xlarge [2]	2000		250,0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10000		1250,0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850,0		30000	
m5.12xlarge [2]	9500		1187,5		40000	
m5.16xlarge [2]	13600		1700,0		60000	
m5.24xlarge [2]	19000		2375,0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5.metal [2]	19000		2375,0		80000	
m5a.large [1]	650	2.880	81,25	360,00	3600	16000
m5a.xlarge [1]	1085	2.880	135,62	360,00	6000	16000
m5a.2xlarge [1]	1580	2.880	197,50	360,00	8333	16000
m5a.4xlarge [2]	2.880		360,0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187,5		40000	
m5a.24xlarge [2]	13750		1718,75		60000	
m5ad.large [1]	650	2.880	81,25	360,00	3600	16000
m5ad.xlarge [1]	1085	2.880	135,62	360,00	6000	16000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5ad.2xlarge [1]	1580	2.880	197,50	360,00	8333	16000
m5ad.4xlarge [2]	2.880		360,0		16000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187,5		40000	
m5ad.24xlarge [2]	13750		1718,75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	
m5d.8xlarge [2]	6800		850,0		30000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5d.12xlarge [2]	9500		1187,5		40000	
m5d.16xlarge [2]	13600		1700,0		60000	
m5d.24xlarge [2]	19000		2375,0		80000	
m5d.metal [2]	19000		2375,0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850,0		30000	
m5dn.12xlarge [2]	9500		1187,5		40000	
m5dn.16xlarge [2]	13600		1700,0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5dn.24xlarge [2]	19000		2375,0		80000	
m5dn.metal [2]	19000		2375,0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850,0		30000	
m5n.12xlarge [2]	9500		1187,5		40000	
m5n.16xlarge [2]	13600		1700,0		60000	
m5n.24xlarge [2]	19000		2375,0		80000	
m5n.metal [2]	19000		2375,0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5zn.large [1]	800	3170	100,00	396,25	3333	13333
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13333
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187,5		40000	
m5zn.12xlarge [2]	19000		2375,0		80000	
m5zn.metal [2]	19000		2375,0		80000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6a.8xlarge [2]	10000		1250,0		40000	
m6a.12xlarge [2]	15000		1875,0		60000	
m6a.16xlarge [2]	20000		2500,0		80000	
m6a.24xlarge [2]	30000		3750,0		120000	
m6a.32xlarge [2]	40000		5000,0		160000	
m6a.48xlarge [2]	40000		5000,0		240000	
m6a.metal [2]	40000		5000,0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187,5		40000	
m6g.12xlarge [2]	14250		1781,25		50000	
m6g.16xlarge [2]	19000		2375,0		80000	
m6g.metal [2]	19000		2375,0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	
m6gd.8xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6gd.12xlarge [2]	14250		1781,25		50000	
m6gd.16xlarge [2]	19000		2375,0		80000	
m6gd.metal [2]	19000		2375,0		80000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250,0		40000	
m6i.12xlarge [2]	15000		1875,0		60000	
m6i.16xlarge [2]	20000		2500,0		80000	
m6i.24xlarge [2]	30000		3750,0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6i.32xlarge [2]	40000		5000,0		160000	
m6i.metal [2]	40000		5000,0		160000	
m6id.large [1]	650	10000	81,25	1250,00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250,0		40000	
m6id.12xlarge [2]	15000		1875,0		60000	
m6id.16xlarge [2]	20000		2500,0		80000	
m6id.24xlarge [2]	30000		3750,0		120000	
m6id.32xlarge [2]	40000		5000,0		160000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6id.metal [2]	40000		5000,0		160000	
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6idn.8xlarge [2]	25000		3125,0		100000	
m6idn.12xlarge [2]	37500		4687,5		150000	
m6idn.16xlarge [2]	50000		6250,0		200000	
m6idn.24xlarge [2]	75000		9375,0		300000	
m6idn.32xlarge [2]	100000		12500,0		400000	
m6idn.metal [2]	100000		12500,0		400000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6in.large [1]	1562	25000	195,31	3125,00	6250	100000
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6in.8xlarge [2]	25000		3125,0		100000	
m6in.12xlarge [2]	37500		4687,5		150000	
m6in.16xlarge [2]	50000		6250,0		200000	
m6in.24xlarge [2]	75000		9375,0		300000	
m6in.32xlarge [2]	100000		12500,0		400000	
m6in.metal [2]	100000		12500,0		400000	
m7a.medium [1]	325	10000	40,62	1250,00	2500	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7a.large [1]	650	10000	81,25	1250,00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250,0		40000	
m7a.12xlarge [2]	15000		1875,0		60000	
m7a.16xlarge [2]	20000		2500,0		80000	
m7a.24xlarge [2]	30000		3750,0		120000	
m7a.32xlarge [2]	40000		5000,0		160000	
m7a.48xlarge [2]	40000		5000,0		240000	
m7a.metal-48xl [2]	40000		5000,0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7g.medium [1]	315	10000	39,38	1250,00	2500	40000
m7g.large [1]	630	10000	78,75	1250,00	3600	40000
m7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7g.8xlarge [2]	10000		1250,0		40000	
m7g.12xlarge [2]	15000		1875,0		60000	
m7g.16xlarge [2]	20000		2500,0		80000	
m7g.metal [2]	20000		2500,0		80000	
m7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
m7gd.large [1]	630	10000	78,75	1250,00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7gd.8xlarge [2]	10000		1250,0		40000	
m7gd.12xlarge [2]	15000		1875,0		60000	
m7gd.16xlarge [2]	20000		2500,0		80000	
m7gd.metal [2]	20000		2500,0		80000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7i.8xlarge [2]	10000		1250,0		40000	
m7i.12xlarge [2]	15000		1875,0		60000	
m7i.16xlarge [2]	20000		2500,0		80000	
m7i.24xlarge [2]	30000		3750,0		120000	
m7i.48xlarge [2]	40000		5000,0		240000	
m7i.metal-24xl [2]	30000		3750,0		120000	
m7i.metal-48xl [2]	40000		5000,0		240000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
m7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
mac1.metal [2]	14000		1750,0		80000	
mac2.metal [2]	10000		1250,0		55000	
mac2-m1ultra.metal 2	10000		1250,0		55000	
mac2-m2.metal [2]	8000		1000,0		55000	
mac2-m2pro.metal [2]	8000		1000,0		55000	
t3.nano [1]	43	2085	5,38	260,62	250	11800
t3.micro [1]	87	2085	10,88	260,62	500	11800
t3.small [1]	174	2085	21,75	260,62	1000	11800
t3.medium [1]	347	2085	43,38	260,62	2000	11800
t3.large [1]	695	2780	86,88	347,50	4000	15700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.nano [1]	45	2085	5,62	260,62	250	11800

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
t3a.micro [1]	90	2085	11,25	260,62	500	11800
t3a.small [1]	175	2085	21,88	260,62	1000	11800
t3a.medium [1]	350	2085	43,75	260,62	2000	11800
t3a.large [1]	695	2780	86,88	347,50	4000	15700
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.nano [1]	43	2085	5,38	260,62	250	11800
t4g.micro [1]	87	2085	10,88	260,62	500	11800
t4g.small [1]	174	2085	21,75	260,62	1000	11800
t4g.medium [1]	347	2085	43,38	260,62	2000	11800
t4g.large [1]	695	2780	86,88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15700

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizadas para computação

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c4.large [2]	500		62.5		4000	
c4.xlarge [2]	750		93,75		6000	
c4.2xlarge [2]	1000		125,0		8000	
c4.4xlarge [2]	2000		250,0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	
c5.9xlarge [2]	9500		1187,5		40000	
c5.12xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5.18xlarge [2]	19000		2375,0		80000	
c5.24xlarge [2]	19000		2375,0		80000	
c5.metal [2]	19000		2375,0		80000	
c5a.large [1]	200	3170	25,00	396,25	800	13300
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787.5		26700	
c5a.24xlarge [2]	9500		1187,5		40000	
c5ad.large [1]	200	3170	25,00	396,25	800	13300

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787.5		26700	
c5ad.24xlarge [2]	9500		1187,5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5d.4xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5d.9xlarge [2]	9500		1187,5		40000	
c5d.12xlarge [2]	9500		1187,5		40000	
c5d.18xlarge [2]	19000		2375,0		80000	
c5d.24xlarge [2]	19000		2375,0		80000	
c5d.metal [2]	19000		2375,0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5n.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187,5		40000	
c5n.18xlarge [2]	19000		2375,0		80000	
c5n.metal [2]	19000		2375,0		80000	
c6a.large [1]	650	10000	81,25	1250,00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6a.8xlarge [2]	10000		1250,0		40000	
c6a.12xlarge [2]	15000		1875,0		60000	
c6a.16xlarge [2]	20000		2500,0		80000	
c6a.24xlarge [2]	30000		3750,0		120000	
c6a.32xlarge [2]	40000		5000,0		160000	
c6a.48xlarge [2]	40000		5000,0		240000	
c6a.metal [2]	40000		5000,0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187,5		40000	
c6g.12xlarge [2]	14250		1781,25		50000	
c6g.16xlarge [2]	19000		2375,0		80000	
c6g.metal [2]	19000		2375,0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6gd.4xlarge [2]	4750		593,75		20000	
c6gd.8xlarge [2]	9500		1187,5		40000	
c6gd.12xlarge [2]	14250		1781,25		50000	
c6gd.16xlarge [2]	19000		2375,0		80000	
c6gd.metal [2]	19000		2375,0		80000	
c6gn.medium [1]	760	9500	95,00	1187,50	2500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187,5		40000	
c6gn.8xlarge [2]	19000		2375,0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6gn.12xlarge [2]	28500		3562,5		120000	
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6i.8xlarge [2]	10000		1250,0		40000	
c6i.12xlarge [2]	15000		1875,0		60000	
c6i.16xlarge [2]	20000		2500,0		80000	
c6i.24xlarge [2]	30000		3750,0		120000	
c6i.32xlarge [2]	40000		5000,0		160000	
c6i.metal [2]	40000		5000,0		160000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250,0		40000	
c6id.12xlarge [2]	15000		1875,0		60000	
c6id.16xlarge [2]	20000		2500,0		80000	
c6id.24xlarge [2]	30000		3750,0		120000	
c6id.32xlarge [2]	40000		5000,0		160000	
c6id.metal [2]	40000		5000,0		160000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
c6in.8xlarge [2]	25000		3125,0		100000	
c6in.12xlarge [2]	37500		4687,5		150000	
c6in.16xlarge [2]	50000		6250,0		200000	
c6in.24xlarge [2]	75000		9375,0		300000	
c6in.32xlarge [2]	100000		12500,0		400000	
c6in.metal [2]	100000		12500,0		400000	
c7a.medium [1]	325	10000	40,62	1250,00	2500	40000
c7a.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250,0		40000	
c7a.12xlarge [2]	15000		1875,0		60000	
c7a.16xlarge [2]	20000		2500,0		80000	
c7a.24xlarge [2]	30000		3750,0		120000	
c7a.32xlarge [2]	40000		5000,0		160000	
c7a.48xlarge [2]	40000		5000,0		240000	
c7a.metal-48xl [2]	40000		5000,0		240000	
c7g.medium [1]	315	10000	39,38	1250,00	2500	40000
c7g.large [1]	630	10000	78,75	1250,00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250,0		40000	
c7g.12xlarge [2]	15000		1875,0		60000	
c7g.16xlarge [2]	20000		2500,0		80000	
c7g.metal [2]	20000		2500,0		80000	
c7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c7gd.large [1]	630	10000	78,75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7gd.8xlarge [2]	10000		1250,0		40000	
c7gd.12xlarge [2]	15000		1875,0		60000	
c7gd.16xlarge [2]	20000		2500,0		80000	
c7gd.metal 2	20000		2500,0		80000	
c7gn.medium [1]	521	10000	65,12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000
c7gn.xlarge [1]	2083	10000	260,38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520,88	1250,00	16667	40000
c7gn.4xlarge [1]	8333	10000	1041,62	1250,00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083,38	2500,00	66667	80000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7gn.12xlarge [1]	25000	30000	3125,00	3750,00	100000	120000
c7gn.16xlarge [1]	33333	40000	4166,62	5000,00	133333	160000
c7gn.metal [1]	33333	40000	4166,62	5000,00	133333	160000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i.8xlarge [2]	10000		1250,0		40000	
c7i.12xlarge [2]	15000		1875,0		60000	
c7i.16xlarge [2]	20000		2500,0		80000	
c7i.24xlarge [2]	30000		3750,0		120000	
c7i.48xlarge [2]	40000		5000,0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7i.metal-24xl [2]	30000		3750,0		120000	
c7i.metal-48xl [2]	40000		5000,0		240000	
c7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
c7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
c7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizado para memória

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r4.large [2]	425		53.125		3000	
r4.xlarge [2]	850		106,25		6000	
r4.2xlarge [2]	1700		212,5		12000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875,0		37500	
r4.16xlarge [2]	14000		1750,0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850,0		30000	
r5.12xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5.16xlarge [2]	13600		1700,0		60000	
r5.24xlarge [2]	19000		2375,0		80000	
r5.metal [2]	19000		2375,0		80000	
r5a.large [1]	650	2.880	81,25	360,00	3600	16000
r5a.xlarge [1]	1085	2.880	135,62	360,00	6000	16000
r5a.2xlarge [1]	1580	2.880	197,50	360,00	8333	16000
r5a.4xlarge [2]	2.880		360,0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187,5		40000	
r5a.24xlarge [2]	13570		1696,25		60000	
r5ad.large [1]	650	2.880	81,25	360,00	3600	16000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5ad.xlarge [1]	1085	2.880	135,62	360,00	6000	16000
r5ad.2xlarge [1]	1580	2.880	197,50	360,00	8333	16000
r5ad.4xlarge [2]	2.880		360,0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187,5		40000	
r5ad.24xlarge [2]	13570		1696,25		60000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10000	312,50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10000	625,00	1250,00	21667	43333
r5b.4xlarge [2]	10000		1250,0		43333	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5b.8xlarge [2]	20000		2500,0		86667	
r5b.12xlarge [2]	30000		3750,0		130000	
r5b.16xlarge [2]	40000		5000,0		173333	
r5b.24xlarge [2]	60000		7500,0		260000	
r5b.metal [2]	60000		7500,0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850,0		30000	
r5d.12xlarge [2]	9500		1187,5		40000	
r5d.16xlarge [2]	13600		1700,0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5d.24xlarge [2]	19000		2375,0		80000	
r5d.metal [2]	19000		2375,0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850,0		30000	
r5dn.12xlarge [2]	9500		1187,5		40000	
r5dn.16xlarge [2]	13600		1700,0		60000	
r5dn.24xlarge [2]	19000		2375,0		80000	
r5dn.metal [2]	19000		2375,0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	
r5n.8xlarge [2]	6800		850,0		30000	
r5n.12xlarge [2]	9500		1187,5		40000	
r5n.16xlarge [2]	13600		1700,0		60000	
r5n.24xlarge [2]	19000		2375,0		80000	
r5n.metal [2]	19000		2375,0		80000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6a.8xlarge [2]	10000		1250,0		40000	
r6a.12xlarge [2]	15000		1875,0		60000	
r6a.16xlarge [2]	20000		2500,0		80000	
r6a.24xlarge [2]	30000		3750,0		120000	
r6a.32xlarge [2]	40000		5000,0		160000	
r6a.48xlarge [2]	40000		5000,0		240000	
r6a.metal [2]	40000		5000,0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6g.8xlarge [2]	9500		1187,5		40000	
r6g.12xlarge [2]	14250		1781,25		50000	
r6g.16xlarge [2]	19000		2375,0		80000	
r6g.metal [2]	19000		2375,0		80000	
r6gd.medium [1]	315	4750	39,38	593,75	2500	20000
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187,5		40000	
r6gd.12xlarge [2]	14250		1781,25		50000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6gd.16xlarge [2]	19000		2375,0		80000	
r6gd.metal [2]	19000		2375,0		80000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6i.8xlarge [2]	10000		1250,0		40000	
r6i.12xlarge [2]	15000		1875,0		60000	
r6i.16xlarge [2]	20000		2500,0		80000	
r6i.24xlarge [2]	30000		3750,0		120000	
r6i.32xlarge [2]	40000		5000,0		160000	
r6i.metal [2]	40000		5000,0		160000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6idn.8xlarge [2]	25000		3125,0		100000	
r6idn.12xlarge [2]	37500		4687,5		150000	
r6idn.16xlarge [2]	50000		6250,0		200000	
r6idn.24xlarge [2]	75000		9375,0		300000	
r6idn.32xlarge [2]	100000		12500,0		400000	
r6idn.metal [2]	100000		12500,0		400000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6in.8xlarge [2]	25000		3125,0		100000	
r6in.12xlarge [2]	37500		4687,5		150000	
r6in.16xlarge [2]	50000		6250,0		200000	
r6in.24xlarge [2]	75000		9375,0		300000	
r6in.32xlarge [2]	100000		12500,0		400000	
r6in.metal [2]	100000		12500,0		400000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250,0		40000	
r6id.12xlarge [2]	15000		1875,0		60000	
r6id.16xlarge [2]	20000		2500,0		80000	
r6id.24xlarge [2]	30000		3750,0		120000	
r6id.32xlarge [2]	40000		5000,0		160000	
r6id.metal [2]	40000		5000,0		160000	
r7a.medium [1]	325	10000	40,62	1250,00	2500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7a.8xlarge [2]	10000		1250,0		40000	
r7a.12xlarge [2]	15000		1875,0		60000	
r7a.16xlarge [2]	20000		2500,0		80000	
r7a.24xlarge [2]	30000		3750,0		120000	
r7a.32xlarge [2]	40000		5000,0		160000	
r7a.48xlarge [2]	40000		5000,0		240000	
r7a.metal-48xl [2]	40000		5000,0		240000	
r7g.medium [1]	315	10000	39,38	1250,00	2500	40000
r7g.large [1]	630	10000	78,75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250,0		40000	
r7g.12xlarge [2]	15000		1875,0		60000	
r7g.16xlarge [2]	20000		2500,0		80000	
r7g.metal [2]	20000		2500,0		80000	
r7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r7gd.large [1]	630	10000	78,75	1250,00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250,0		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7gd.12xlarge [2]	15000		1875,0		60000	
r7gd.16xlarge [2]	20000		2500,0		80000	
r7gd.metal [2]	20000		2500,0		80000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250,0		40000	
r7i.12xlarge [2]	15000		1875,0		60000	
r7i.16xlarge [2]	20000		2500,0		80000	
r7i.24xlarge [2]	30000		3750,0		120000	
r7i.48xlarge [2]	40000		5000,0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7i.metal-24xl [2]	30000		3750,0		120000	
r7i.metal-48xl [2]	40000		5000,0		240000	
r7iz.large [1]	792	10000	99,00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198,00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396,00	1250,00	13333	40000
r7iz.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7iz.8xlarge [2]	10000		1250,0		40000	
r7iz.12xlarge [2]	19000		2375,0		76000	
r7iz.16xlarge [2]	20000		2500,0		80000	
r7iz.32xlarge [2]	40000		5000,0		160000	
r7iz.metal-16xl [2]	20000		2500,0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7iz.metal-32xl [2]	40000		5000,0		160000	
u-3tb1.56xlarge [2]	19000		2375,0		80000	
u-6tb1.56xlarge [2]	38000		4750,0		160000	
u-6tb1.112xlarge [2]	38000		4750,0		160000	
u-6tb1.metal [2]	38000		4750,0		160000	
u-9tb1.112xlarge [2]	38000		4750,0		160000	
u-9tb1.metal [2]	38000		4750,0		160000	
u-12tb1.112xlarge [2]	38000		4750,0		160000	
u-12tb1.metal [2]	38000		4750,0		160000	
u-18tb1.112xlarge [2]	38000		4750,0		160000	
u-18tb1.metal [2]	38000		4750,0		160000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-12tb.224xlarge [2]	60000		7500,0		420000	
u7in-16tb.224xlarge [2]	100000		12500,0		420000	
u7in-24tb.224xlarge [2]	100000		12500,0		420000	
u7in-32tb.224xlarge [2]	100000		12500,0		420000	
x1.16xlarge [2]	7000		875,0		40000	
x1.32xlarge [2]	14000		1750,0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20000
x2gd.large [1]	630	4750	78,75	593,75	3600	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x2gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187,5		40000	
x2gd.12xlarge [2]	14250		1781,25		60000	
x2gd.16xlarge [2]	19000		2375,0		80000	
x2gd.metal [2]	19000		2375,0		80000	
x2idn.16xlarge [2]	40000		5000,0		173333	
x2idn.24xlarge [2]	60000		7500,0		260000	
x2idn.32xlarge [2]	80000		10000,0		260000	
x2idn.metal [2]	80000		10000,0		260000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x2iedn.xlarge [1]	2500	20000	312,50	2500,00	8125	65000
x2iedn.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500,00	32500	65000
x2iedn.8xlarge [2]	20000		2500,0		65000	
x2iedn.16xlarge [2]	40000		5000,0		130000	
x2iedn.24xlarge [2]	60000		7500,0		195000	
x2iedn.32xlarge [2]	80000		10000,0		260000	
x2iedn.metal [2]	80000		10000,0		260000	
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x2iezn.8xlarge [2]	12000		1500,0		55000	
x2iezn.12xlarge [2]	19000		2375,0		80000	
x2iezn.metal [2]	19000		2375,0		80000	
x1e.xlarge [2]	500		62.5		3700	
x1e.2xlarge [2]	1000		125,0		7400	
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875,0		40000	
x1e.32xlarge [2]	14000		1750,0		80000	
z1d.large [1]	800	3170	100,00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13333

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
z1d.2xlarge [2]	3170		396,25		13333	
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187,5		40000	
z1d.12xlarge [2]	19000		2375,0		80000	
z1d.metal [2]	19000		2375,0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizada para armazenamento

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
d2.xlarge [2]	750		93,75		6000	
d2.2xlarge [2]	1000		125,0		8000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
d2.4xlarge [2]	2000		250,0		16000	
d2.8xlarge [2]	4000		500,0		32000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	
d3en.8xlarge [2]	5000		625,0		30000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
d3en.12xlarge [2]	7000		875,0		40000	
h1.2xlarge [2]	1750		218,75		12000	
h1.4xlarge [2]	3500		437,5		20000	
h1.8xlarge [2]	7000		875,0		40000	
h1.16xlarge [2]	14000		1750,0		80000	
i3.large [2]	425		53.125		3000	
i3.xlarge 2	850		106,25		6000	
i3.2xlarge [2]	1700		212,5		12000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875,0		32500	
i3.16xlarge [2]	14000		1750,0		65000	
i3.metal [2]	19000		2375,0		80000	
i3en.large [1]	576	4750	72,10	593,75	3000	20000
i3en.xlarge [1]	1153	4750	144,20	593,75	6000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i3en.2xlarge [1]	2307	4750	288,39	593,75	12000	20000
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	
i3en.12xlarge [2]	9500		1187,5		40000	
i3en.24xlarge [2]	19000		2375,0		80000	
i3en.metal [2]	19000		2375,0		80000	
i4g.large [1]	625	10000	78,12	1250,00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250,0		40000	
i4g.16xlarge [2]	20000		2500,0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i4i.large [1]	625	10000	78,12	1250,00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4i.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4i.8xlarge [2]	10000		1250,0		40000	
i4i.12xlarge [2]	15000		1875,0		60000	
i4i.16xlarge [2]	20000		2500,0		80000	
i4i.24xlarge [2]	30000		3750,0		120000	
i4i.32xlarge [2]	40000		5000,0		160000	
i4i.metal [2]	40000		5000,0		160000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000
im4gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
im4gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250,0		40000	
im4gn.8xlarge [2]	20000		2500,0		80000	
im4gn.16xlarge [2]	40000		5000,0		160000	
is4gen.medium [1]	625	10000	78,12	1250,00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
is4gen.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250,0		40000	
is4gen.8xlarge [2]	20000		2500,0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Computação acelerada

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
dl1.24xlarge [2]	19000		2375,0		80000	
dl2q.24xlarge [2]	19000		2375,0		80000	
f1.2xlarge [2]	1700		212,5		12000	
f1.4xlarge [2]	3500		437,5		44000	
f1.16xlarge [2]	14000		1750,0		75000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875,0		40000	
g3.16xlarge [2]	14000		1750,0		80000	
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13333

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13333
g4ad.8xlarge [2]	3170		396,25		13333	
g4ad.16xlarge [2]	6300		787.5		26667	
g4dn.xlarge [1]	950	3500	118,75	437,50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187,5		40000	
g4dn.12xlarge [2]	9500		1187,5		40000	
g4dn.16xlarge [2]	9500		1187,5		40000	
g4dn.metal [2]	19000		2375,0		80000	
g5.xlarge [1]	700	3500	87,50	437,50	3000	15000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000,0		65000	
g5.12xlarge [2]	16000		2000,0		65000	
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375,0		80000	
g5.48xlarge [2]	19000		2375,0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g5g.16xlarge [2]	19000		2375,0		80000	
g5g.metal [2]	19000		2375,0		80000	
g6.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6.4xlarge [2]	8000		1000,0		32000	
g6.8xlarge [2]	16000		2000,0		64000	
g6.12xlarge [2]	20000		2500,0		80000	
g6.16xlarge [2]	20000		2500,0		80000	
g6.24xlarge [2]	30000		3750,0		120000	
g6.48xlarge [2]	60000		7500,0		240000	
gr6.4xlarge [2]	8000		1000,0		32000	
gr6.8xlarge [2]	16000		2000,0		64000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6000	20000
inf1.6xlarge [2]	4750		593,75		20000	
inf1.24xlarge [2]	19000		2375,0		80000	
inf2.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
inf2.8xlarge [2]	10000		1250,0		40000	
inf2.24xlarge [2]	30000		3750,0		120000	
inf2.48xlarge [2]	60000		7500,0		240000	
p2.xlarge [2]	750		93,75		6000	
p2.8xlarge [2]	5000		625,0		32500	
p2.16xlarge [2]	10000		1250,0		65000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875,0		40000	
p3.16xlarge [2]	14000		1750,0		80000	
p3dn.24xlarge [2]	19000		2375,0		80000	
p4d.24xlarge [2]	19000		2375,0		80000	
p4de.24xlarge [2]	19000		2375,0		80000	
p5.48xlarge [2]	80000		10000,0		260000	
trn1.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
trn1.32xlarge [2]	80000		10000,0		260000	
trn1n.32xlarge [2]	80000		10000,0		260000	
vt1.3xlarge [1]	2375	4750	296,88	593,75	10000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19000		2375,0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Computação de alta performance

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11000

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter o desempenho declarado indefinidamente. Se a sua workload exigir desempenho máximo sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Suporte à otimização do EBS

Os tipos de instância a seguir oferecem suporte à otimização do EBS, mas essa otimização não está habilitada por padrão. É possível habilitar a otimização do EBS ao executar essas instâncias ou após elas estarem em execução. É necessário habilitar a otimização do EBS para alcançar o nível de performance descrito. Ao habilitar a otimização de EBS, você paga uma taxa adicional por hora pela capacidade dedicada. Para obter informações sobre preços, consulte Instâncias otimizadas para EBS em Instâncias da geração anterior.

Tamanho da instância	Largura de banda máxima (Mbps)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
c1.xlarge	1000	125,0	8000
c3.xlarge	500	62.5	4000
c3.2xlarge	1000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62.5	4000
i2.2xlarge	1000	125,0	8000
i2.4xlarge	2000	250,0	16000
m1.large	500	62.5	4000
m1.xlarge	1000	125,0	8000
m2.2xlarge	500	62.5	4000
m2.4xlarge	1000	125,0	8000
m3.xlarge	500	62.5	4000
m3.2xlarge	1000	125,0	8000
r3.xlarge	500	62.5	4000
r3.2xlarge	1000	125,0	8000
r3.4xlarge	2000	250,0	16000

As instâncias `i2.8xlarge`, `c3.8xlarge` e `r3.8xlarge` não possuem largura de banda EBS dedicada e, portanto, não oferecem otimização de EBS. Nessas instâncias, o tráfego de rede e o trafego de Amazon EBS compartilham a mesma interface de rede de 10 gigabits.

Obtenha a máxima performance

É possível usar as métricas `EBSIOBalance%` e `EBSByteBalance%` para ajudá-lo a determinar se as instâncias estão dimensionadas corretamente. É possível visualizar essas métricas no console do CloudWatch e definir um alarme que é acionado com base nos limites especificados por você. Essas métricas são expressadas como uma porcentagem. As instâncias com uma porcentagem de equilíbrio consistentemente baixa são candidatas à ampliação. As instâncias nas quais a porcentagem de equilíbrio jamais fica abaixo de 100% são candidatas à redução. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.

As instâncias com mais memória foram projetadas para executar grandes bancos de dados na memória, incluindo implantações de produção do banco de dados na memória SAP HANA na nuvem. Para maximizar a performance do EBS, use instâncias com mais memória com um número par de volumes de `io1` ou `io2` com performance provisionada idêntica. Por exemplo, para workloads pesadas com relação às IOPS, use quatro volumes de `io1` ou `io2` com 40.000 IOPS provisionadas para obter o máximo de 160.000 IOPS de instância. Da mesma forma, para workloads pesadas com relação à throughput, use seis volumes de `io1` ou `io2` com 48.000 IOPS provisionadas para obter o máximo de 4.750 MB/s de throughput. Para obter recomendações adicionais, consulte Configuração de armazenamento para SAP HANA.

Considerações

- As instâncias G4dn, I3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a e Z1d lançadas após 26 de fevereiro de 2020 fornecem a performance máxima listada na tabela acima. Para obter a máxima performance de uma instância lançada antes de 26 de fevereiro de 2020, interrompa-a e inicie-a.
- As instâncias C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn e P3dn lançadas após 3 de dezembro de 2019 fornecem a performance máxima listada na tabela acima. Para obter a performance máxima de uma instância lançada antes de 3 de dezembro de 2019, interrompa-a e inicie-a.
- As instâncias `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` lançadas após 12 de março de 2020 fornecem a performance indicada na tabela acima. As instâncias desses tipos lançadas antes de 12 de março de 2020 podem fornecer performance menor. Para obter a performance máxima de uma instância lançada antes de 12 de março de 2020, entre em contato com a equipe de conta para atualizar a instância sem custo adicional.

Exibir tipos de instâncias compatíveis com a otimização do EBS

Use a AWS CLI para visualizar os tipos de instâncias na região atual que são compatíveis com a otimização do EBS.

Para visualizar os tipos de instância que oferecem suporte à otimização do EBS e que estão ativados por padrão

Use o comando describe-instance-types a seguir. Se estiver realizando a execução deste comando em um prompt de comando do Windows, substitua os caracteres de continuação de linha \ pelo caractere ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Exemplos de resultado para `eu-west-1`:

```
-------------------------------------------------------------------------------
|                            DescribeInstanceTypes                            |
+------------------+---------------------+-----------+-----------------------+
|   InstanceType   | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/s)  |
+------------------+---------------------+-----------+-----------------------+
|  m5dn.8xlarge    |  6800               |  30000    |  850.0                |
|  m6gd.xlarge     |  4750               |  20000    |  593.75               |
|  c4.4xlarge      |  2000               |  16000    |  250.0                |
|  r4.16xlarge     |  14000              |  75000    |  1750.0               |
|  m5ad.large      |  2880               |  16000    |  360.0                |
...
```

Para visualizar os tipos de instância compatíveis com a otimização do EBS e que estão ativados por padrão

Use o comando describe-instance-types a seguir.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
```

```
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Exemplos de resultado para `eu-west-1`:

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+-----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+-----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

Habilitação da otimização do EBS na execução

É possível habilitar a otimização para uma instância definindo o atributo para otimização de EBS.

Para ativar a otimização de Amazon EBS ao executar uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Launch Instance (Executar instância).
3. Em []Step 1: Choose an Amazon Machine Image (AMI [] (Etapa 1: escolher uma imagem de máquina da Amazon [AMI]), selecione uma AMI.
4. Em Step 2: Choose an Instance Type (Etapa 2: Escolher um tipo de instância), selecione um tipo de instância que esteja listada como compatível com a otimização para Amazon EBS.

5. Em Step 3: Configure Instance Details (Etapa 3: Configurar detalhes da instância), preencha os campos necessários e escolha Launch as EBS-optimized instance (Executar como instância otimizada para EBS). Se o tipo de instância que você selecionou na etapa anterior não oferecer suporte à otimização para Amazon EBS, essa opção não estará presente. Se o tipo de instância selecionado for otimizado para Amazon EBS por padrão, essa opção estará selecionada e você não poderá cancelar a seleção.
6. Siga as instruções para concluir o assistente e executar sua instância.

Para habilitar a otimização para EBS ao executar uma instância usando a linha de comando

É possível usar um dos seguintes comandos com a opção correspondente. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- run-instances com `--ebs-optimized` (AWS CLI)
- New-EC2Instance com `-EbsOptimized` (AWS Tools for Windows PowerShell)

Habilitar a otimização do EBS para uma instância existente

É possível ativar ou desativar a otimização para uma instância existente modificando o atributo de instância otimizada para Amazon EBS. Se a instância estiver em execução, é necessário interrompê-la primeiro.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Como habilitar a otimização de EBS para uma instância existente usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Para interromper a instância, escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância). Pode demorar alguns minutos para que a instância pare.
4. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância).

5. Em Change Instance Type (Alterar tipo de instância), execute um dos seguintes procedimentos:

   - Se o tipo de sua instância for otimizado para Amazon EBS por padrão, a opção EBS-optimized (Otimizada para EBS) será selecionada e você não poderá alterar a seleção. É possível escolher Cancel (Cancelar), pois a otimização para Amazon EBS já está ativada para a instância.
   - Se o tipo de instância for compatível com a otimização para Amazon EBS, escolha EBS-optimized (Otimizada para EBS) e escolha Apply (Aplicar).
   - Se o tipo de instância não oferecer suporte à otimização de Amazon EBS, você não poderá escolher EBS-optimized (Otimizada para EBS). É possível selecionar um tipo de instância em Instance type (Tipo de instância) que seja compatível com a otimização para Amazon EBS, escolher EBS-optimized (Otimizada para EBS) e Apply (Aplicar).
6. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

Como habilitar a otimização de EBS para uma instância existente usando a linha de comando

1. Se a instância estiver em execução, use um dos seguintes comandos para interrompê-la:

   - stop-instances (AWS CLI)
   - Stop-EC2Instance (AWS Tools for Windows PowerShell)
2. Para habilitar a otimização do EBS, use um dos seguintes comandos com a opção correspondente:

   - modify-instance-attribute com `--ebs-optimized` (AWS CLI)
   - Edit-EC2InstanceAttribute com `-EbsOptimized` (AWS Tools for Windows PowerShell)

Opções de compra de instância

O Amazon EC2 fornece as seguintes opções de compra para permitir otimizar os custos com base em suas necessidades:

- Instâncias sob demanda: pague pelas instâncias que você iniciar
- Savings Plans: reduza os custos do Amazon EC2 se comprometendo com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos.

- Reserved Instances (Instâncias reservadas): reduza os custos do Amazon EC2 se comprometendo com uma configuração consistente de instância, incluindo o tipo de instância e a região, por um período de vigência de um ou de três anos.
- Spot Instances (Instâncias spot): solicite instâncias do EC2 não utilizadas, o que pode reduzir os custos do Amazon EC2 significativamente.
- Dedicated Hosts (Hosts dedicados): pague por um host físico que seja totalmente dedicado à execução de suas instâncias e traga suas licenças de software existentes por soquete, por núcleo ou por VM para reduzir custos.
- Dedicated Instances (Instâncias dedicadas): pague por hora pelas instâncias que são executadas no hardware de um ocupante único.
- Reservas de capacidade: reserve capacidade para as instâncias do EC2 em uma zona de disponibilidade específica.

Se você não puder se comprometer com uma configuração de instância específica, mas puder se comprometer com uma quantidade de uso, adquira Savings Plans para reduzir seus custos de instâncias sob demanda.Se você precisar de uma reserva de capacidade, compre instâncias reservadas ou Reservas de Capacidade para uma zona de disponibilidade específica. Os blocos de capacidade podem ser usados para reservar um cluster de instâncias de GPU. As instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executados e se poderão ser interrompidas. Os hosts dedicados ou as instâncias dedicadas podem ajudar você a atender aos requisitos de conformidade e reduzir custos usando as licenças de software associadas ao servidor. Para obter mais informações, consulte Definição de preço Amazon EC2.

Para obter mais informações sobre Savings Plans, consulte o Savings Plans User Guide (Guia do usuário de Savings Plans).

Tópicos

- Determinar o ciclo de vida da instância
- Instâncias sob demanda
- Reserved Instances
- Instâncias spot
- Dedicated Hosts
- Dedicated Instances

- Reservas de capacidade

Determinar o ciclo de vida da instância

O ciclo de vida de uma instância começa quando ela é executada e termina quando é encerrada. A opção de compra escolhida afeta o ciclo de vida da instância. Por exemplo, uma instância sob demanda é executada quando você a inicia e é encerrada quando você a encerra. Uma instância spot é executada contanto que sua capacidade esteja disponível e sua sugestão de preço máximo seja superior ao preço spot.

Use um dos métodos a seguir para determinar o ciclo de vida de uma instância.

Para determinar o ciclo de vida da instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Details (Detalhes), em Instance details (Detalhes da instância), localize Lifecycle (Ciclo de vida). Se o valor for `spot`, a instância será uma instância spot. Se o valor for `normal`, a instância será uma instância sob demanda ou uma Instância reservada.
5. Na guia Details (Detalhes), em Host and placement group (Host e placement group), localize Tenancy (Locação). Se o valor for `host`, a instância estará em execução em um Host dedicado. Se o valor for `dedicated`, a instância será uma Instâncias dedicadas.

Para determinar o ciclo de vida da instância usando a AWS CLI

Use o seguinte comando describe-instances:

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Se a instância estiver em execução em um Host dedicado, o resultado conterá as seguintes informações:

```
"Tenancy": "host"
```

Se a instância for uma Instâncias dedicadas, o resultado conterá as seguintes informações:

```
"Tenancy": "dedicated"
```

Se a instância for uma instância spot, o resultado conterá as seguintes informações:

```
"InstanceLifecycle": "spot"
```

Caso contrário, o resultado não conterá `InstanceLifecycle`.

Instâncias sob demanda

Com instâncias sob demanda, você paga pela capacidade computacional por segundo, sem qualquer compromisso de longo prazo. Você tem pleno controle sobre o ciclo de vida da instância: você decide quando executar, interromper, hibernar, iniciar, reiniciar ou encerrá-la.

Não há compromisso de longo prazo ao comprar Instâncias on-demand. Você paga apenas pelos segundos em que suas instâncias sob demanda estiverem no estado `running`, com um mínimo de 60 segundos. O preço por segundo para uma instância sob demanda em execução é fixo e está listado na página de preços sob demanda, preços do Amazon EC2.

Recomendamos o uso de Instâncias on-demand para aplicações com workloads de curto prazo e irregulares que não podem ser interrompidas.

Para economias significativas com relação a instâncias sob demanda, use AWS Savings Plans, Instâncias spot ou Reserved Instances.

Sumário

- Cotas de instância sob demanda
  - Monitorar cotas e uso de instância sob demanda
  - Solicitar um aumento da cota
- Consulte os preços das instâncias sob demanda

Cotas de instância sob demanda

Há cotas para o número de instâncias sob demanda em execução por Conta da AWS por região. As cotas de instância sob demanda são gerenciadas em termos do número de unidades de processamento central virtual (vCPUs) que as instâncias sob demanda em execução estão usando, independentemente do tipo de instância. Cada tipo de cota especifica o número máximo de vCPUs para uma ou mais famílias de instâncias.

Sua conta inclui as cotas apresentadas a seguir para as instâncias sob demanda. As cotas se aplicam somente às instâncias em execução. Se a instância estiver pendente, sendo interrompida, interrompida ou hibernada, ela não será contabilizada em suas cotas.

Nome	Padrão	Ajustável
Execução de instâncias DL sob demanda	0	Sim
Execução de instâncias F sob demanda	0	Sim
Execução de instâncias G e VT sob demanda	0	Sim
Executar todas as instâncias HPC sob demanda	0	Sim
Executar instâncias com mais memória sob demanda	0	Sim
Execução de instâncias Inf sob demanda	0	Sim
Execução de instâncias P sob demanda	0	Sim
Execução de instâncias padrão sob demanda (A, C, D, H, I, M, R, T, Z)	5	Sim
Executar instâncias Trn sob demanda	0	Sim
Execução de instâncias X sob demanda	0	Sim

Para obter informações sobre as diferentes famílias, gerações e tamanhos de instâncias, consulte o Guia de tipos de instância do Amazon EC2.

É possível executar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação, desde que o número de vCPUs não exceda a cota da sua conta. Por exemplo: com uma cota de instância padrão de 256 vCPUs, é possível iniciar 32 instâncias `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias `c5.4xlarge` (16 x 16 vCPUs). Para mais informações, consulte Limites de instância sob demanda do EC2.

Tarefas

- Monitorar cotas e uso de instância sob demanda

- Solicitar um aumento da cota

Monitorar cotas e uso de instância sob demanda

É possível visualizar e gerenciar suas cotas de instância sob demanda usando os métodos a seguir.

Para visualizar as cotas atuais usando o console do Service Quotas

1. Abra o console do Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação, selecione uma região.
3. No campo de filtro, insira **`On-Demand`**.
4. A coluna Valor da cota aplicada exibe o número máximo de vCPUs para cada tipo de cota de instância sob demanda da sua conta.

Para visualizar as cotas atuais usando o console do AWS Trusted Advisor

Abra a página Limites do serviço no console do AWS Trusted Advisor.

Para configurar os alarmes do CloudWatch

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em relação às cotas. Também é possível configurar alarmes para alertar quando estiver chegando próximo da cota. Para obter mais informações, consulte Alarmes do Service Quotas e do Amazon Cloudwatch no Guia do usuário do Service Quotas.

Solicitar um aumento da cota

Mesmo que o Amazon EC2 aumente automaticamente suas cotas de instância sob demanda com base em seu uso, é possível solicitar um aumento de cota, se for o caso. Por exemplo, se você pretender iniciar mais instâncias do que o permitido por sua cota atual, é possível solicitar um aumento de cota usando console do Service Quotas, descrito em Service Quotas do Amazon EC2.

Consulte os preços das instâncias sob demanda

É possível usar a API do serviço de lista de preços ou a API da lista de preços da AWS para consultar os preços de instâncias sob demanda. Para obter mais informações, consulte Uso da API da lista de preços da AWS no Guia do usuário do AWS Billing.

Reserved Instances

> **Important**
>
> Recomendamos utilizar Savings Plans em vez de instâncias reservadas. Os Savings Plans são a maneira mais fácil e flexível de economizar dinheiro em seus custos de computação da AWS e oferecem preços mais baixos (até 72% de desconto sobre os preços sob demanda), assim como as instâncias reservadas. No entanto, os Savings Plans são diferentes das instâncias reservadas. Com as instâncias reservadas, você se compromete com uma configuração de instância específica, enquanto que com Savings Plans você tem a flexibilidade de usar as configurações de instância que melhor atendam às suas necessidades. Para usar o Savings Plans, você se compromete com uma quantidade consistente de uso, medida em USD por hora. Para obter mais informações, consulte o Guia do usuário do AWS Savings Plans.

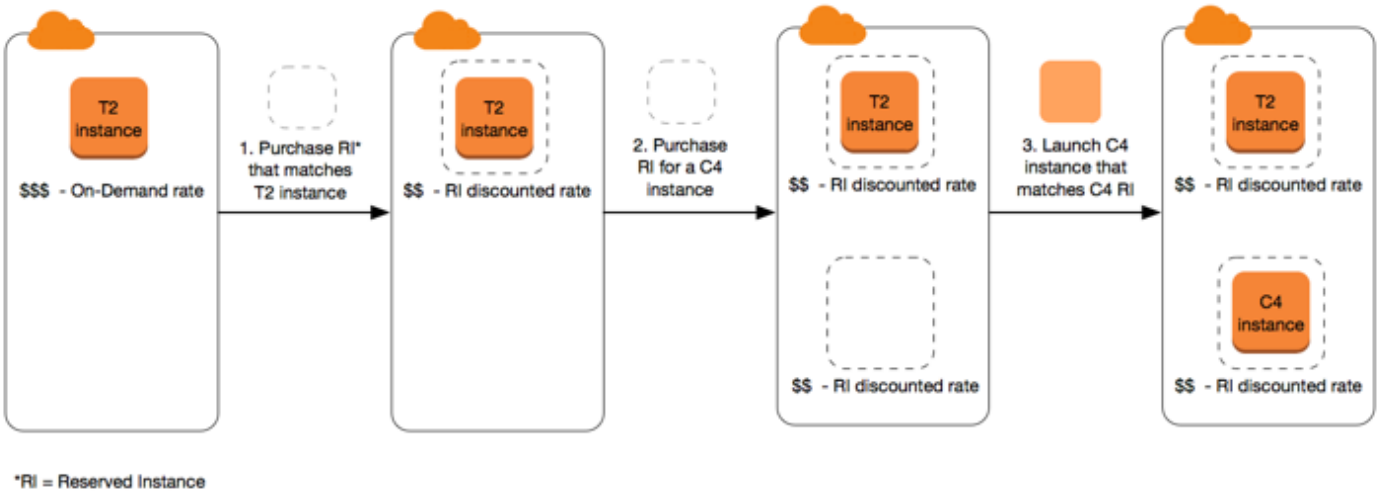
As instâncias reservadas proporcionam economia significativa em seus custos do Amazon EC2 em comparação com os preços de instâncias sob demanda. As instâncias reservadas não são instâncias físicas, mas um desconto na fatura aplicado na sua conta pelo uso de instâncias sob demanda. Essas Instâncias on-demand devem corresponder a determinados atributos, como o tipo de instância e a região, para que você possa aproveitar os benefícios do desconto de faturamento.

Tópicos de Instâncias reservadas

- Visão geral da Instância reservada
- Principais variáveis que determinam a definição de preço da Instância reservada
- Instâncias reservadas regionais e zonais (escopo)
- Tipos de Instâncias reservadas (classes de oferta)
- Como as Instâncias reservadas são aplicadas
- Use as suas Instâncias reservadas
- Como você é cobrado
- Comprar instâncias reservadas
- Vender no Marketplace de instâncias reservadas
- Modificar a Instâncias reservadas
- Trocar Instâncias reservadas conversíveis
- Cotas de instâncias reservadas

Visão geral da Instância reservada

O diagrama a seguir mostra uma visão geral básica da compra e do uso das Instâncias reservadas.



Neste cenário, você tem uma instância sob demanda (T2) em execução na sua conta, pela qual paga atualmente as tarifas sob demanda. Você compra uma Instância reservada que corresponde aos atributos da instância em execução, e o benefício do faturamento é aplicado imediatamente. Em seguida, você compra uma Instância reservada para uma instância C4. Você não tem nenhuma instância em execução na conta que corresponda aos atributos dessa Instância reservada. Na etapa final, execute uma instância que corresponda aos atributos da Instância reservada C4 para que o benefício do faturamento seja aplicado imediatamente.

Principais variáveis que determinam a definição de preço da Instância reservada

A definição de preço de Instância reservada é determinada pelas principais variáveis a seguir.

Atributos da instância

Uma instância reservada tem quatro atributos de instância que determinam seu preço.

- Tipo de instância: Por exemplo, `m4.large`. Isso é composto pela família de instâncias (por exemplo, `m4`) e pelo tamanho da instância (por exemplo, `large`).
- Região: a região na qual a Instância reservada é comprada.
- Locação: Se sua instância é executada em hardware compartilhado (padrão) ou com grupo de usuários único (dedicado). Para ter mais informações, consulte Dedicated Instances.
- Plataforma: O sistema operacional; por exemplo, Windows ou Linux/Unix. Para ter mais informações, consulte Escolher uma plataforma.

Compromisso com o período de vigência

É possível comprar uma Instância reservada para um compromisso de um ou três anos, sendo que há um grande desconto para o compromisso de três anos.

- Um ano: o compromisso de um ano é definido como 31536000 segundos (365 dias).
- Três anos: o compromisso de três anos é definido como 94608000 segundos (1095 dias).

As Instâncias reservadas não são renovadas automaticamente; quando elas expiram, é possível continuar usando a instância do EC2 sem interrupções, mas serão cobradas taxas sob demanda. No exemplo acima, quando as Instâncias reservadas que cobrem as instâncias T2 e C4 expirarem, você voltará a pagar as taxas sob demanda até encerrar as instâncias ou comprar novas Instâncias reservadas que correspondam aos atributos de instância.

> **Important**
>
> Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, será possível modificar, trocar ou vender a Instância reservada caso suas necessidades mudem.

Opções de pagamento

As seguintes opções de pagamento estão disponíveis para Instâncias reservadas:

- Pagamento adiantado integral: o pagamento integral é feito no início do período de vigência, sem outros custos ou cobranças por hora incorridos pelo restante do período, independentemente das horas usadas.
- Adiantamento parcial: uma parte do custo deve ser paga adiantada, e as horas restantes do período de vigência são faturadas em uma taxa por hora com desconto, independentemente de a Instância reservada estar ou não sendo usada.
- Sem pagamento adiantado: é cobrada a tarifa por hora com desconto para cada hora do período de vigência, independentemente de a Instância reservada estar ou não sendo usada. Nenhum pagamento adiantado é necessário.

> **Note**
>
> As Instâncias reservadas sem pagamento adiantado têm como base uma obrigação contratual de pagamento mensal pelo período de vigência da reserva. Por esse motivo,

é necessário ter um histórico de faturamento de sucesso para que seja possível comprar Instâncias reservadas sem pagamento adiantado.

Em linhas gerais, é possível economizar mais ao fazer um pagamento adiantado maior pelas Instâncias reservadas. Também é possível encontrar instâncias reservadas oferecidas por vendedores terceirizados a preços menores e períodos de vigência mais curtos no Marketplace de instâncias reservadas. Para ter mais informações, consulte Vender no Marketplace de instâncias reservadas.

Classe de oferta

Se sua computação precisar de uma mudança, você talvez consiga modificar ou trocar a Instância reservada, dependendo da classe de oferta.

- Padrão: fornece o desconto mais significativo, mas só pode ser modificada. As Instâncias reservadas não podem ser alteradas.
- Conversível: fornece um desconto menor que o das Instâncias reservadas padrão, mas pode ser trocada por outra Instância reservada conversível com atributos de instância diferentes. As Instâncias reservadas conversíveis também podem ser modificadas.

Para ter mais informações, consulte Tipos de Instâncias reservadas (classes de oferta).

Important

Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, será possível modificar, trocar ou vender a Instância reservada caso suas necessidades mudem.

Para obter mais informações, consulte a página Definição de preço de instâncias reservadas do Amazon EC2.

Instâncias reservadas regionais e zonais (escopo)

Ao comprar uma Instância reservada, você determina o escopo da Instância reservada. O escopo pode ser regional ou zonal.

- Regional: quando você compra uma Instância reservada para uma região, ela é chamada de Instância reservada regional.

- Zonal: quando você compra uma Instância reservada para uma zona de disponibilidade específica, ela é chamada de Instância reservada zonal.

O escopo não afeta o preço. Você paga o mesmo preço por um Instância reservada regional ou zonal. Para obter mais informações sobre Instância reserva da definição de preço, consulte Principais variáveis que determinam a definição de preço da Instância reservada and Definição de preço de instâncias reservadas do Amazon EC2.

Para saber mais sobre como especificar o escopo de uma instância reservada, consulte Atributos da RI, especificamente o marcador Zona de disponibilidade.

Diferenças entre Instâncias reservadas regionais e zonais

A tabela a seguir destaca algumas das principais diferenças entre regionais Instâncias reservadas e zonais Instâncias reservadas:

	Instâncias reservadas regionais	Instâncias reservadas zonais
Capacidade de reservar capacidade	Uma Instância reservada regional não reserva capacidade.	Uma Instância reservada zonal reserva capacidade na zona de disponibilidade especificada.
Flexibilidade da zona de disponibilidade	O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade na região especificada.	Sem flexibilidade da zona de disponibilidade — o desconto da Instância reservada se aplica ao uso da instância somente na zona de disponibilidade especificada.
Flexibilidade de tamanho da instância	O desconto da Instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho.	Sem flexibilidade de tamanho da instância — o desconto da Instância reservada se aplica ao uso da instância somente

	Instâncias reservadas regionais	Instâncias reservadas zonais
	Compatível somente com Instâncias reservadas de Linux/Unix da Amazon com locação padrão. Para ter mais informações, consulte Flexibilidade de tamanho da instância determinada pelo fator de normalização.	para o tamanho e o tipo de instância especificados.
Enfileiramento de uma compra	É possível enfileirar compras para instâncias reservadas regionais.	Você não pode enfileirar compras para instâncias reservadas zonais.

Para ter mais informações e exemplos, consulte Como as Instâncias reservadas são aplicadas.

Tipos de Instâncias reservadas (classes de oferta)

A classe de oferta de uma Instância reservada é padrão ou conversível. Uma Instância reservada padrão oferece um desconto mais significativo do que uma Instância reservada conversível, mas você não pode trocar uma Instância reservada padrão. É possível trocar Instâncias reservadas conversíveis. É possível modificar Instâncias reservadas padrão e conversíveis.

A configuração de uma Instância reservada compreende um único tipo de instância, plataforma, escopo e locação ao longo de um termo. Se as suas necessidades de computação mudarem, talvez seja possível modificar ou trocar a sua Instância reservada.

Diferenças entre Instâncias reservadas padrão e conversível

A seguir estão as diferenças entre as classes de oferta da Instâncias reservadas padrão e conversível.

	Instância reservada padrão	Convertible Reserved Instance
Modificar a Instâncias reservadas	Alguns atributos podem ser modificados. Para ter	Alguns atributos podem ser modificados. Para ter

	Instância reservada padrão	Convertible Reserved Instance
	mais informações, consulte Modificar a Instâncias reservadas.	mais informações, consulte Modificar a Instâncias reservadas.
Trocar instâncias reservadas	Não pode ser trocada.	Pode ser trocada durante o período de vigência por outra Instância reservada convertível com novos atributos, incluindo a família de instâncias, o tipo de instância, a plataforma, o escopo ou a locação. Para ter mais informações, consulte Trocar Instâncias reservadas conversíveis.
Vender no Marketplace de instâncias reservadas	Pode ser vendida no Marketplace de instâncias reservadas.	Não pode ser vendida no Marketplace de instâncias reservadas.
Comprar no marketplace de instâncias reservadas	Pode ser comprada no Marketplace de instâncias reservadas.	Não pode ser comprada no Marketplace de instâncias reservadas.

Como as Instâncias reservadas são aplicadas

As instâncias reservadas não são instâncias físicas, mas um desconto na fatura aplicado às instâncias sob demanda em execução em sua conta. As instâncias sob demanda devem atendem a determinadas especificações de instâncias reservadas para que possam se beneficiar do desconto na fatura.

Se você adquirir uma instância reservada e já tiver uma instância sob demanda em execução que atenda às especificações e instância reservada, o desconto na fatura será aplicado automaticamente. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância sob demanda qualificada em execução, inicie uma instância sob demanda com as mesmas

especificações da instância reservada Para ter mais informações, consulte Use as suas Instâncias reservadas.

A classe de oferta (padrão ou conversível) da instância reservada não afeta a forma como o desconto da fatura é aplicado.

Tópicos

- Como as Instâncias reservadas zonais são aplicadas
- Como as Instâncias reservadas regionais são aplicadas
- Flexibilidade de tamanho da instância
- Exemplos de aplicação da Instâncias reservadas

Como as Instâncias reservadas zonais são aplicadas

Uma instância reservada que é comprada para reservar capacidade em uma zona de disponibilidade específica é denominada instância reservada zonal.

- O desconto de instância reservada se aplica ao uso correspondente da instância nessa zona de disponibilidade.
- Os atributos (locação, plataforma, zona de disponibilidade, tipo de instância e tamanho de instância) das instâncias em execução devem corresponder aos atributos das Instâncias reservadas.

Por exemplo, se você tiver adquirido duas instâncias reservadas de locação padrão `c4.xlarge` na zona de disponibilidade us-east-1a, até duas instâncias do Linux/Unix `c4.xlarge` de locação padrão em execução na zona de disponibilidade us-east-1a poderão se beneficiar com o desconto da instância reservada.

Como as Instâncias reservadas regionais são aplicadas

Uma instâncias reservada comprada para uma região é denominada instância reservada regional e fornece flexibilidade de zona de disponibilidade e tamanho de instância.

- O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade nessa região.
- O desconto da instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho; isso é conhecido como flexibilidade de tamanho de instância.

Flexibilidade de tamanho da instância

Com a flexibilidade de tamanho da instância, o desconto de instância reservada aplica-se ao uso de instâncias que têm a mesma família, geração e atributo. A instância reservada é aplicada do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização. Para obter um exemplo de como o desconto de instância reservada é aplicado, consulte Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização.

Limitações

- Com suporte: só há suporte para a flexibilidade do tamanho da instância para instâncias reservadas regionais.
- Sem suporte: a flexibilidade do tamanho da instância não tem suporte nas seguintes instâncias reservadas:
  - Instâncias reservadas compradas para uma zona de disponibilidade específica (Instâncias reservadas zonal)
  - Instâncias reservadas para instâncias G4ad, G4dn, G5, G5g, Inf1 e Inf2
  - Instâncias reservadas para Windows Server, Windows Server com SQL Standard, Windows Server com SQL Server Enterprise, Windows Server com SQL Server Web, RHEL e SUSE Linux Enterprise Server
  - Instâncias reservadas com locação dedicada

Flexibilidade de tamanho da instância determinada pelo fator de normalização

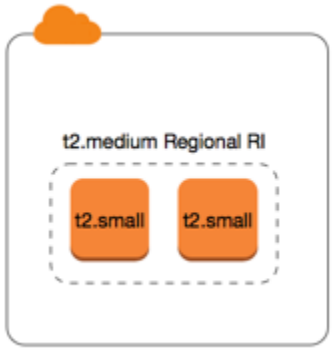
A flexibilidade de tamanho da instância é determinada pelo fator de normalização do tamanho da instância. O desconto se aplica total ou parcialmente às instâncias em execução da mesma família de instâncias, dependendo do tamanho da instância da reserva, em qualquer zona de disponibilidade na região. Os únicos atributos que devem ser correspondentes são a locação, a plataforma e a família de instâncias.

A tabela a seguir descreve os diferentes tamanhos em uma família de instâncias e o fator de normalização correspondente. Essa escala é usada para aplicar a taxa de desconto de Instâncias reservadas ao uso normalizado da família de instâncias.

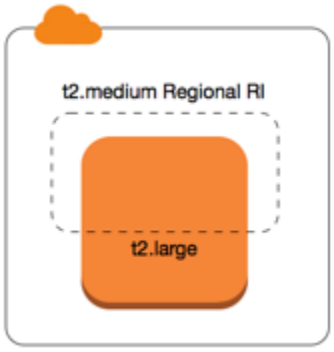
Tamanho da instância	Fator de normalização
nano	0.25

Tamanho da instância	Fator de normalização
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Por exemplo, uma instância `t2.medium` tem um fator de normalização de 2. Se você tiver adquirido uma Instância reservada `t2.medium` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver duas instâncias `t2.small` em execução em sua conta nessa região, o benefício de faturamento será aplicado integralmente às duas instâncias.



Ou, se você tiver uma instância `t2.large` em execução em sua conta na região US East (N. Virginia) o benefício de faturamento será aplicado a 50% do uso da instância.



O fator de normalização é aplicado também ao modificar Instâncias reservadas. Para ter mais informações, consulte Modificar a Instâncias reservadas.

Fator de normalização para instâncias bare metal

A flexibilidade de tamanho da instância também se aplica a instâncias bare metal na família de instâncias. Se você tem Instâncias reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias bare metal, é possível se beneficiar das economias de Instância reservada na mesma família de instâncias. O inverso também é verdadeiro: se você tem Instâncias reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias na mesma família que uma instância bare metal, é possível se beneficiar das economias de Instância reservada na instância bare metal.

O tamanho da instância `metal` não tem um único fator de normalização. Uma instância bare metal tem o mesmo fator de normalização que o tamanho de instância virtualizada equivalente na mesma família de instâncias. Por exemplo, uma instância `i3.metal` tem o mesmo fator de normalização que uma instância `i3.16xlarge`.

Tamanho da instância	Fator de normalização
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Por exemplo, uma instância `i3.metal` tem um fator de normalização de 128. Se você comprar uma Instância reservada `i3.metal` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia), o benefício de faturamento poderá ser aplicado da seguinte maneira:

- Se você tem uma instância `i3.16xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente à instância `i3.16xlarge` (fator de normalização da `i3.16xlarge` = 128).
- Ou, se você tem duas instâncias `i3.8xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a ambas as instâncias `i3.8xlarge` (fator de normalização da `i3.8xlarge` = 64).

- Ou, se você tem quatro instâncias `i3.4xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a todas as quatro instâncias `i3.4xlarge` (fator de normalização da `i3.4xlarge` = 32).

O inverso também é verdadeiro. Por exemplo, se você comprar duas Instâncias reservadas `i3.8xlarge` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver uma instância `i3.metal` em execução nessa região, o benefício de faturamento será aplicado integralmente à instância `i3.metal`.

Exemplos de aplicação da Instâncias reservadas

Os cenários a seguir abrangem as maneiras como as Instâncias reservadas são aplicadas.

- Cenário 1: Instâncias reservadas em uma única conta
- Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização
- Cenário 3: Instâncias reservadas regionais em contas vinculadas
- Cenário 4: Instâncias reservadas zonais em uma conta vinculada

Cenário 1: Instâncias reservadas em uma única conta

Você está executando as seguintes Instâncias on-demand na conta A:

- 4 x instâncias do Linux `m3.large` de locação padrão na zona de disponibilidade us-east-1a
- 2 x instâncias do Amazon Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1b
- 1 x instâncias do Amazon Linux `c4.xlarge` de locação padrão na zona de disponibilidade us-east-1c

Você adquire as seguintes Instâncias reservadas na conta A:

- 4 Instâncias reservadas Linux `m3.large` de locação padrão na zona de disponibilidade us-east-1a (a capacidade é reservada)
- 4 x Instâncias reservadas `m4.large` de locação padrão do Amazon Linux na região us-east-1
- 1 x Instâncias reservadas `c4.large` de locação padrão do Amazon Linux na região us-east-1

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- O desconto e a reserva de capacidade das quatro Instâncias reservadas `m3.large` zonais são usados pelas quatro instâncias `m3.large`, pois os atributos (tamanho da instância, região, plataforma, locação) entre elas são correspondentes.
- As `m4.large` Instâncias reservadas regionais fornecem flexibilidade de zona de disponibilidade e de tamanho de instância, pois são Instâncias reservadas Amazon Linux regionais com locação padrão.

  `m4.large` é equivalente a 4 unidades normalizadas/hora.

  Você adquiriu quatro Instâncias reservadas `m4.large` regionais e, no total, elas equivalem a 16 unidades normalizadas/hora (4x4). A conta A tem duas instâncias `m4.xlarge` em execução, equivalente a 16 unidades normalizadas/hora (2x8). Nesse caso, as quatro Instâncias reservadas `m4.large` regionais fornecem o benefício completo de faturamento de uso das duas instâncias `m4.xlarge`.
- A Instância reservada `c4.large` regional em us-east-1 fornece flexibilidade de zona de disponibilidade e de tamanho da instância, pois é uma Instância reservada Amazon Linux regional com locação padrão e se aplica à instância `c4.xlarge`. Uma instância `c4.large` é equivalente a 4 unidades normalizadas/hora e a uma `c4.xlarge` é equivalente a 8 unidades normalizadas/hora.

  Nesse caso, a `c4.large` Instância reservada regional fornece benefício parcial para uso de `c4.xlarge`. Isso ocorre porque a Instância reservada `c4.large` equivale a 4 unidades normalizadas/hora de uso, mas a instância `c4.xlarge` requer 8 unidades normalizadas/hora. Portanto, o desconto de faturamento da Instância reservada `c4.large` aplica-se a 50% do uso de `c4.xlarge`. O uso `c4.xlarge` restante é cobrado na tarifa sob demanda.

Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização

Você está executando as seguintes Instâncias on-demand na conta A:

- 2 x instâncias do Amazon Linux `m3.xlarge` de locação padrão na zona de disponibilidade us-east-1b
- 2 x instâncias do Amazon Linux `m3.large` de locação padrão na zona de disponibilidade us-east-1b

Você adquire as seguintes Instâncias reservadas na conta A:

- 1 x Instância reservada `m3.2xlarge` de locação padrão do Amazon Linux na região us-east-1

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- A Instância reservada regional `m3.2xlarge` em us-east-1 fornece flexibilidade de zona de disponibilidade e de tamanho da instância, pois é uma Instância reservada Amazon Linux regional com locação padrão e se aplica à instância . Ele se aplica primeiro às instâncias `m3.large` e, em seguida, às instâncias `m3.xlarge`, porque a aplicação é do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização.

  Uma instância `m3.large` é equivalente a 4 unidades normalizadas/hora.

  Uma instância `m3.xlarge` é equivalente a 8 unidades normalizadas/hora.

  Uma instância `m3.2xlarge` é equivalente a 16 unidades normalizadas/hora.

  O benefício é aplicado da seguinte forma:

  A instância reservada regional `m3.2xlarge` oferece total benefício para uso de 2 x `m3.large`, porque juntas essas instâncias representam 8 unidades normalizadas/hora. Isso deixa 8 unidades normalizadas/hora para serem aplicadas às instâncias `m3.xlarge`.

  Com as restantes 8 unidades/hora normalizadas, a instância reservada regional `m3.2xlarge` oferece total benefício para uso de 1 x `m3.xlarge`, porque cada instância `m3.xlarge` é equivalente a 8 unidades normalizadas/hora. O uso `m3.xlarge` restante é cobrado na tarifa sob demanda.

Cenário 3: Instâncias reservadas regionais em contas vinculadas

As Instâncias reservadas são aplicadas primeiro ao uso na conta de compra, seguida pelo uso de qualificação em qualquer outra conta da organização. Para ter mais informações, consulte Instâncias reservadas e faturamento consolidado. Para Instâncias reservadas regionais que oferecem flexibilidade de tamanho de instância, o benefício é aplicado do menor para o maior tamanho de instância na família de instâncias.

Você está executando a seguinte Instâncias on-demand na conta A (a conta de compra):

- 2 x instâncias do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1a
- 1 x instâncias do Linux `m4.2xlarge` de locação padrão na zona de disponibilidade us-east-1b
- 2 x instâncias do Linux `c4.xlarge` de locação padrão na zona de disponibilidade us-east-1a
- 1 x instâncias do Linux `c4.2xlarge` de locação padrão na zona de disponibilidade us-east-1b

Outro cliente está executando as seguintes Instâncias on-demand na conta B — uma conta vinculada:

- 2 x instâncias do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1a

Você adquire as seguintes Instâncias reservadas regionais na conta A:

- 4 x Instâncias reservadas `m4.xlarge` de locação padrão do Linux na região us-east-1
- 2 x Instâncias reservadas `c4.xlarge` de locação padrão do Linux na região us-east-1

Os benefícios da Instância reservada regional são aplicados da seguinte maneira:

- O desconto das quatro Instâncias reservadas `m4.xlarge` é usado pelas duas instâncias `m4.xlarge` e pela única instância `m4.2xlarge` na conta A (conta de compra). Todas as três instâncias têm atributos correspondentes (locação, plataforma região e família de instâncias). O desconto é aplicado às instâncias da conta de compra (conta A) primeiro, mesmo que a conta B (conta vinculada) tenha duas `m4.xlarge` que também correspondam às Instâncias reservadas. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.
- O desconto das duas Instâncias reservadas `c4.xlarge` se aplica às duas instâncias `c4.xlarge`, porque eles são um tamanho de instância menor que a instância `c4.2xlarge`. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.

Cenário 4: Instâncias reservadas zonais em uma conta vinculada

Geralmente, as Instâncias reservadas pertencentes a uma conta são aplicadas primeiro ao uso nessa conta. Contudo, se houver Instâncias reservadas qualificadas e não utilizadas para uma zona de disponibilidade específica (Instâncias reservadas zonais) em outras contas da organização, elas serão aplicadas à conta antes das Instâncias reservadas regionais pertencentes à conta. Isso é feito para garantir a utilização máxima da Instância reservada e uma fatura menor. Para fins de faturamento, todas as contas da organização são tratadas como se fossem uma só. O exemplo a seguir pode ajudar a explicar isso.

Você está executando a seguinte instância sob demanda na conta A (a conta de compra):

- 1 x instância do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1a

Um cliente está executando a seguinte instância sob demanda na conta vinculada B:

- 1 x instância do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1b

Você adquire as seguintes Instâncias reservadas regionais na conta A:

- 1 x Instância reservada `m4.xlarge` de locação padrão do Linux na região us-east-1

Um cliente também compra as seguintes Instâncias reservadas de zona na conta C vinculada:

- 1 `m4.xlarge` Linux Instâncias reservadas de locação padrão na zona de disponibilidade us-east-1a

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- O desconto da Instância reservada `m4.xlarge` de zona pertencente à conta C é aplicado ao uso de `m4.xlarge` na conta A.
- O desconto da Instância reservada `m4.xlarge` regional pertencente à conta A é aplicado ao uso de `m4.xlarge` na conta B.
- Se a Instância reservada regional pertencente à conta A tiver sido aplicada primeiro ao uso na conta A, a Instância reservada de zona pertencente à conta C permanecerá não utilizada, e o uso na conta B será cobrado nas taxas sob demanda.

Para obter mais informações, consulte Instâncias reservadas no relatório do Billing and Cost Management.

> **Note**
>
> As instâncias reservadas de zona reservam capacidade somente para a conta proprietária e não podem ser compartilhadas com outras Contas da AWS. Se você precisar compartilhar a capacidade com outras Contas da AWS, use On-Demand Capacity Reservations.

Use as suas Instâncias reservadas

As Instâncias reservadas são aplicadas automaticamente às Instâncias on-demand em execução, desde que as especificações sejam correspondentes. Se você não tiver nenhuma Instâncias on-demand que corresponda às especificações de sua Instância reservada, a Instância reservada não será utilizada até que você execute uma instância com as especificações necessárias.

Se você estiver iniciando uma instância para aproveitar o benefício de fatura de uma instância reservada, especifique as informações a seguir quando configurar a instância sob demanda:

Plataforma

Especifique uma imagem de máquina da Amazon (AMI) que corresponda à plataforma (descrição de produtos) da instância reservada. Por exemplo, se você tiver especificado `Linux/UNIX` para a instância reservada, pode iniciar uma instância de uma AMI do Amazon Linux AMI ou do Ubuntu.

Tipo de instância

Se você comprou uma instância reservada zonal, especifique o mesmo tipo de instância da instância reservada; por exemplo, `t3.large`. Para ter mais informações, consulte Como as Instâncias reservadas zonais são aplicadas.

Se você comprou uma instância reservada regional, deverá especificar um tipo de instância da mesma família de instâncias que o tipo de instância da instância reservada. Por exemplo, se você tiver especificado `t3.xlarge` para a instância reservada, deverá iniciar a instância na família T3, mas poderá especificar qualquer tamanho, por exemplo, `t3.medium`. Para ter mais informações, consulte Como as Instâncias reservadas regionais são aplicadas.

Zona de disponibilidade

Se você adquiriu uma instância reservada para uma zona de disponibilidade específica, deve iniciar a instância na mesma zona de disponibilidade.

Se adquiriu uma instância reservada regional, pode iniciar a instância em qualquer zona de disponibilidade da região que especificou para a instância reservada.

Locação

A locação (`dedicated` ou `shared`) da instância deve corresponder à locação da instância reservada. Para ter mais informações, consulte Dedicated Instances.

Para obter exemplos de como as instâncias reservadas são aplicadas às instâncias sob demanda em execução, consulte Como as Instâncias reservadas são aplicadas. Para obter mais informações, consulte Por que minhas instâncias reservadas do Amazon EC2 não estão sendo aplicadas à minha fatura da AWS da forma que eu esperava?

É possível usar vários métodos para iniciar as instâncias sob demanda que usem o desconto de instância reservada. Para obter informações sobre os diferentes métodos de lançamento,

consulte Executar sua instância. É possível usar o Amazon EC2 Auto Scaling para iniciar instâncias dedicadas. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Como você é cobrado

Todas as Instâncias reservadas fornecem um desconto em comparação à definição de preço sob demanda. Com as Instâncias reservadas, você paga por todo o período de vigência, e não pelo uso real. É possível optar por pagar pela Instância reservada adiantado, parcialmente adiantado ou mensalmente, dependendo da opção de pagamento especificada para a Instância reservada.

Quando as Instâncias reservadas expirarem, serão cobradas taxas sob demanda pelo uso da instância do EC2. É possível colocar uma Instância reservada em uma fila para compra por até três anos de maneira antecipada. Isso pode ajudar a garantir que você tenha cobertura ininterrupta. Para ter mais informações, consulte Enfileirar sua compra.

O nível gratuito da AWS está disponível para novas contas da AWS. Se você estiver usando o nível gratuito da AWS para executar instâncias do Amazon EC2 e adquirir uma instância reservada, será cobrado de acordo com as diretrizes padrão de definição de preço. Para obter informações, consulte Nível gratuito da AWS.

Tópicos

- Faturamento do uso
- Visualizar sua fatura
- Instâncias reservadas e faturamento consolidado
- Níveis de definição de preço com desconto da Instância reservada

Faturamento do uso

As Instâncias reservadas são cobradas a cada hora fechada durante o período de vigência selecionado, independentemente de uma instância estar sendo executada ou não. Cada hora fechada começa na hora (zero minutos e zero segundos após a hora) de um relógio padrão de 24 horas. Por exemplo, 1:00:00 a 1:59:59 é uma hora fechada. Para obter mais informações sobre os estados da instância, consulte Ciclo de vida da instância.

Um benefício do faturamento de Instância reservada pode ser aplicado a uma instância em execução com base em uma taxa por segundo. O faturamento por segundo está disponível para instâncias que usam uma distribuição de código aberto do Linux, como o Amazon Linux e o Ubuntu. O faturamento

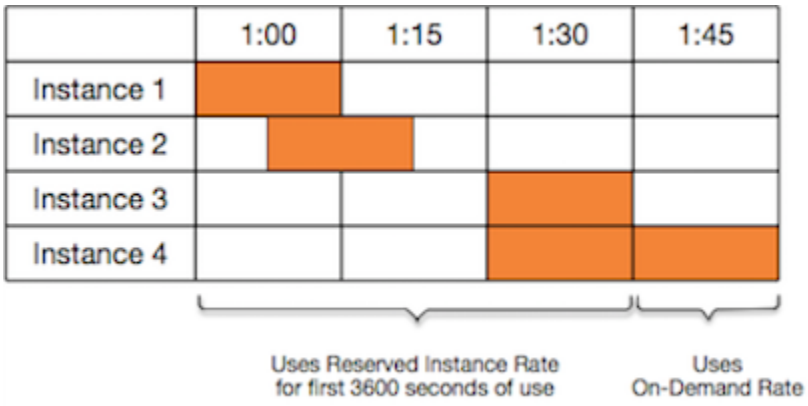
por hora é usado para distribuições comerciais do Linux, como o Red Hat Enterprise Linux e o SUSE Linux Enterprise Server.

Um dos benefícios de faturamento da Instância reservada pode ser aplicado a um máximo de 3600 segundos (uma hora) de uso de instância por hora fechada. É possível executar várias instâncias simultaneamente, mas só pode receber o benefício do desconto de Instância reservada por um total de 3600 segundos por hora. O uso de instância que ultrapassar 3600 segundos em uma hora será faturado com base na taxa sob demanda.

Por exemplo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` simultaneamente por uma hora, uma instância será cobrada em uma hora de uso de Instância reservada, enquanto as outras três instâncias serão cobradas em três horas de uso sob demanda.

Contudo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` por 15 minutos (900 segundos) cada uma na mesma hora, o tempo total de execução das instâncias será uma hora, o que resultará em uma hora de uso de Instância reservada e 0 hora de uso sob demanda.

Se várias instâncias qualificadas estiverem sendo executadas simultaneamente, o benefício de faturamento de Instância reservada será aplicado a todas as instâncias ao mesmo tempo até um máximo de 3600 segundos em uma hora. Depois disso, serão cobradas taxas sob demanda.



O Cost Explorer no console do Billing and Cost Management permite que você analise as economias com base nas Instâncias on-demand em execução. As perguntas frequentes sobre Instâncias reservadas incluem um exemplo de um cálculo de valor de tabela.

Se você fechar sua conta na AWS, o faturamento sob demanda dos seus recursos será interrompido. Contudo, se você tiver Instâncias reservadas na conta, continuará recebendo a fatura delas até que elas expirem.

Visualizar sua fatura

Você encontrará mais informações sobre as cobranças e as taxas da sua conta ao visualizar o console do AWS Billing and Cost Management.

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Instâncias reservadas.

É possível visualizar as cobranças online ou baixar um arquivo CSV.

Também é possível monitorar a utilização da instância reservada usando o Relatório de uso e de custos da AWS. Para obter mais informações, consulte Instâncias reservadas em Relatório de custo e uso no Guia do usuário do AWS Billing.

Instâncias reservadas e faturamento consolidado

Os benefícios da definição de preços das Instâncias reservadas são compartilhados quando a conta que faz a compra é parte de um conjunto de contas faturadas sob uma conta pagante de faturamento consolidado. O uso da instância em todas as contas-membro é agregada na conta pagante todos os meses. Em geral, isso é útil para empresas em que há equipes ou grupos funcionais diferentes; dessa forma, a lógica usual da Instância reservada é aplicada para calcular a conta. Para obter mais informações, consulte Faturamento consolidado para o AWS Organizations.

Se você fechar a conta que comprou a Instância reservada, a conta pagante será cobrada pela Instância reservada até que a instância reservada expire. Depois que a conta encerrada for excluída permanentemente em 90 dias, as contas de membro não se beneficiarão mais do desconto de faturamento da instância reservada.

> **Note**
>
> As instâncias reservadas de zona reservam capacidade somente para a conta proprietária e não podem ser compartilhadas com outras Contas da AWS. Se você precisar compartilhar a capacidade com outras Contas da AWS, use On-Demand Capacity Reservations.

Níveis de definição de preço com desconto da Instância reservada

Se sua conta se qualificar para uma camada de preços com desconto, ela receberá automaticamente descontos nas taxas de uso de instância e com pagamento adiantado nas compras de Instância reservada que você fizer nessa camada, desse ponto em diante. Para se qualificar para um desconto, o valor de tabela das Instâncias reservadas na região deverá ser de 500.000 USD ou mais.

As seguintes regras se aplicam:

- As camadas de preços e descontos relacionados aplicam-se somente às compras das Amazon EC2 padrão do Instâncias reservadas.
- As camadas de preços não se aplicam às Instâncias reservadas para Windows com SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- As camadas de preços não se aplicam às Instâncias reservadas para Linux com SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- Os descontos do nível de preços aplicam-se somente às compras feitas pela AWS. Eles não se aplicam a compras de Instâncias reservadas de terceiros.
- As camadas de preços com desconto atualmente não são aplicáveis a compras de Instância reservada convertível.

Tópicos

- Calcular descontos de preço de Instância reservada
- Comprar com nível de desconto
- Cruzamento de níveis de definição de preço
- Faturamento consolidado para níveis de definição de preço

Calcular descontos de preço de Instância reservada

É possível determinar a camada da definição de preço de sua conta ao calcular o valor de tabela de todas as Instâncias reservadas em uma região. Multiplique o preço recorrente por hora de cada reserva pelo número total de horas do período de vigência e adicione o preço adiantado sem desconto (conhecido também como preço fixo) no momento da compra. Como o valor de tabela se no preço sem desconto (público), ele não será afetado se você se qualificar para um desconto por volume ou se o preço cair depois de você comprar suas Instâncias reservadas.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Por exemplo, para uma `t2.small` Instância reservada com adiantamento parcial de 1 ano, supõe-se que o preço inicial seja 60,00 USD e a taxa por hora seja 0,007 USD. Isso fornece um valor de tabela de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Para ver os valores de preço fixo das Instâncias reservadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Para exibir a coluna Preço para pagamento adiantado, selecione o ícone de configurações () no canto superior direito, ative Preço para pagamento adiantado e escolha Confirmar.

Old console

Para ver os valores de preço fixo das Instâncias reservadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Para exibir a coluna Preço para pagamento adiantado, selecione o ícone de configurações () no canto superior direito, clique em Preço para pagamento adiantado e escolha Fechar.

Para ver os valores de preço fixo das Instâncias reservadas usando a linha de comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)
- DescribeReservedInstances (API do Amazon EC2)

Comprar com nível de desconto

Quando você comprar Instâncias reservadas, o Amazon EC2 aplicará automaticamente todos os descontos à parte da sua compra que estiver dentro do nível de preço com desconto. Você não precisará fazer nada diferente e poderá comprar as Instâncias reservadas usando qualquer ferramenta do Amazon EC2. Para ter mais informações, consulte Comprar instâncias reservadas.

Depois que o valor de tabela das Instâncias reservadas ativas em uma região ultrapassar um nível de definição de preço com desconto, qualquer compra futura de Instâncias reservadas nessa região será cobrada com uma taxa com desconto. Se com uma única compra de Instâncias reservadas em uma região você ultrapassar o limite de uma camada com desconto, a parte da compra que estiver acima do limite de preço será cobrada com a taxa com desconto. Para obter mais informações sobre os IDs de Instância reservada temporária criados durante o processo de compra, consulte Cruzamento de níveis de definição de preço.

Se o valor de tabela ficar abaixo do ponto de preço desse nível de definição de preço com desconto — por exemplo, se algumas das Instâncias reservadas expirarem — as futuras compras de Instâncias reservadas na região não receberão desconto. Contudo, você continua a receber o desconto aplicado em todas as Instâncias reservadas originalmente compradas no nível de preço com desconto.

Estes são os quatros cenários possíveis durante a compra de Instâncias reservadas:

- Sem desconto — sua compra em uma região ainda está abaixo do limite para desconto.
- Desconto parcial — sua compra em uma região ultrapassa o limite do primeiro nível de desconto. Nenhum desconto é aplicado a uma ou mais reservas e a taxa com desconto é aplicada nas reservas restantes.
- Desconto total — sua compra inteira em uma região cai em um nível de desconto e recebe o desconto apropriado.
- Duas taxas com desconto — sua compra em uma região ultrapassa um nível inferior de desconto para um nível superior de desconto. Serão cobradas duas taxas diferentes: uma ou mais reservas na taxa desconto inferior e as reservas restantes com a taxa desconto maior.

Cruzamento de níveis de definição de preço

Se sua compra cruzar um nível de preços com desconto, você verá múltiplas entradas para essa compra: uma para a parte da compra cobrada em preço normal e outra para essa a parte da compra cobrada na taxa de desconto aplicável.

O serviço Instância reservada gera vários IDs de Instância reservada porque sua compra passou de um nível sem desconto ou de um nível com desconto para outro. Há um ID para cada conjunto de reservas em um nível. Portanto, o ID retornado pelo comando de compra da CLI ou pela ação da API é diferente do ID real das novas Instâncias reservadas.

Faturamento consolidado para níveis de definição de preço

Uma conta de faturamento consolidado agrega o valor de tabela das contas-membro em uma região. Quando o valor de tabela de todas as Instâncias reservadas ativas para a conta de faturamento consolidado atingir uma camada de preços com desconto, todas as Instâncias reservadas compradas depois desse ponto por qualquer membro da conta de faturamento consolidado serão cobradas com o desconto (desde que o valor de tabela para essa conta consolidada fique acima de limite de camada de preços com desconto). Para ter mais informações, consulte Instâncias reservadas e faturamento consolidado.

Comprar instâncias reservadas

Para comprar uma instância reservada, pesquise por ofertas de instância reservada na AWS e em vendedores terceirizados, ajustando os parâmetros de pesquisa até encontrar a correspondência exata que está procurando.

Quando você procurar Instâncias reservadas para comprar, receberá um orçamento do custo das ofertas apresentadas. Ao dar continuidade à compra, a AWS colocará automaticamente um preço-limite sobre o preço de compra. O custo total das suas Instâncias reservadas não excederá o valor orçado.

Se o preço aumentar ou mudar por algum motivo, a compra não será concluída. Quando você realiza a aquisição de uma instância reservada de um vendedor terceirizado no Marketplace de instâncias reservadas do EC2, se houver ofertas semelhantes à sua escolha, mas com um preço inicial mais baixo, a AWS venderá as ofertas a preços iniciais mais baixos.

Antes de confirmar sua compra, analise os detalhes da Instância reservada que planeja comprar e verifique se todos os parâmetros são precisos. Após adquirir uma instância reservada (do vendedor terceirizado no Marketplace de instâncias reservadas ou da AWS), você não poderá cancelar sua compra.

Para comprar e modificar instâncias reservadas, certifique-se de que seu usuário tenha as permissões apropriadas, como a capacidade de descrever zonas de disponibilidade. Para obter informações, consulte the section called “Trabalhar com Instâncias reservadas” (API) ou the section called “Trabalhar com Instâncias reservadas” (console).

Tópicos

- Escolher uma plataforma
- Enfileirar sua compra
- Comprar Instâncias reservadas padrão
- Comprar Instâncias reservadas conversíveis
- Comprar do Marketplace da Instância reservada
- Como visualizar o Instâncias reservadas
- Como cancelar uma compra colocada na fila
- Renovar uma Instância reservada

Escolher uma plataforma

O Amazon EC2 é compatível com as seguintes plataformas para as instâncias reservadas:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux com HA
- Windows
- Windows com SQL Server Standard
- Windows com SQL Server Web
- Windows com SQL Server Enterprise

Quando adquire uma Instância reservada, escolha uma oferta para uma plataforma que represente o sistema operacional da sua instância.

Instâncias do Linux

- Para as distribuições do SUSE Linux e do RHEL, é necessário escolher ofertas para essas plataformas específicas, ou seja, para as plataformas SUSE Linux ou Red Hat Enterprise Linux.
- Para todas as demais distribuições do Linux (incluindo Ubuntu), escolha uma oferta para a plataforma Linux/UNIX.
- Se você trouxer sua assinatura de RHEL existente, será necessário escolher uma oferta para a plataforma Linux/UNIX, não uma oferta para a plataforma Red Hat Enterprise Linux.

Instâncias do Windows

- Para Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web, escolha ofertas específicas para essas plataformas.
- Para todas as demais versões do Windows, escolha uma oferta para a plataforma Windows.

> **Note**
>
> O Ubuntu Pro não está disponível como uma instância reservada. Para obter economias significativas em comparação com os preços de instâncias sob demanda, recomendamos usar o Ubuntu Pro com Savings Plans. Para obter mais informações, consulte o Guia do usuário do Savings Plans.

> **Important**
>
> Se você planeja comprar uma instância reservada para aplicar a uma instância sob demanda iniciada em uma AMI do AWS Marketplace, primeiro verifique o campo `PlatformDetails` da AMI. O campo `PlatformDetails` indica qual Instância reservada comprar. Os detalhes da plataforma da AMI devem corresponder à plataforma do Instância reservada, caso contrário, o Instância reservada não será aplicado ao instância sob demanda. Para obter informações sobre como visualizar os detalhes da plataforma da AMI, consulte Noções básicas sobre as informações de faturamento da AMI.

Enfileirar sua compra

Por padrão, quando você compra uma Instância reservada, a compra é feita imediatamente. Se preferir, será possível colocar as compras na fila para uma data e hora futura. Por exemplo, é possível colocar uma compra na fila para o momento próximo da expiração de uma Instância reservada existente. Isso pode ajudar a garantir que você tenha cobertura ininterrupta.

É possível colocar compras na fila para uma Instâncias reservadas regional, mas não para uma Instâncias reservadas zonal ou uma Instâncias reservadas de outros vendedores. É possível colocar uma compra na fila por até três anos de maneira antecipada. Na data e hora programadas, a compra será executada usando a forma de pagamento padrão. Após o pagamento ser feito com êxito, os benefícios de faturamento serão aplicados.

É possível visualizar as compras colocadas na fila no console do Amazon EC2. O status de uma compra na fila é queued (na fila). É possível cancelar uma compra na fila a qualquer momento antes da hora programada. Para obter detalhes, consulte Como cancelar uma compra colocada na fila.

Comprar Instâncias reservadas padrão

É possível comprar as Instâncias reservadas padrão em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, é possível abandonar a reserva de capacidade e comprar uma Instância reservada padrão regional;.

New console

Para comprar Instâncias reservadas padrão usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).
3. Para Offering class (Classe da oferta), escolha Standard (Padrão) para exibir as Instâncias reservadas padrão.
4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra. Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

   Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.

5. Selecione outras configurações conforme necessário e escolha Search (Pesquisar).
6. Para cada Instância reservada que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).

   Para comprar uma instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party (terceiros) na coluna Seller (Vendedor) dos resultados de pesquisa. A coluna Termo exibe os termos não padrão. Para ter mais informações, consulte Comprar do Marketplace da Instância reservada.
7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order all (Pedir tudo).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `Payment-pending` para `Active`. Quando a Instância reservada for `Active`, ela estará pronta para ser usada.

> **Note**
>
> Se o status mudar para `Retired`, a AWS pode não ter recebido seu pagamento.

Old console

Para comprar Instâncias reservadas padrão usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).

3. Para Offering class (Classe da oferta), escolha Standard (Padrão) para exibir as Instâncias reservadas padrão.
4. Para comprar uma reserva de capacidade, escolha Mostrar apenas ofertas que reservam capacidade no canto superior direito da tela de compra. Para comprar uma Instância reservada regional, deixe a caixa de seleção desmarcada.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.

   Para comprar uma instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party (terceiros) na coluna Seller (Vendedor) dos resultados de pesquisa. A coluna Termo exibe os termos não padrão.
6. Para cada Instância reservada que você deseja comprar, insira a quantidade e escolha Add to Cart (Adicionar ao carrinho).
7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View cart (Visualizar carrinho).
8. Se Order On (Pedir em) for Now (Agora), a compra será concluída imediatamente. Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order (Fazer pedido).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `payment-pending` para `active`. Quando a Instância reservada for `active`, ela estará pronta para ser usada.

> **Note**
>
> Se o status mudar para `retired`, a AWS pode não ter recebido seu pagamento.

Para comprar uma instância reservada padrão usando a AWS CLI

1. Localize as Instâncias reservadas disponíveis usando o comando describe-reserved-instances-offerings. Especifique `standard` para o parâmetro `--offering-class` apresentar somente Instâncias reservadas padrão. É possível aplicar parâmetros adicionais para restringir os resultados. Por exemplo, se você quiser comprar uma Instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX` durante um período de vigência de somente 1 ano:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

   Para localizar as instâncias reservadas somente no Marketplace de instâncias reservadas, use o filtro `marketplace` e não especifique uma duração na solicitação, pois o período de vigência pode ser mais curto que o período de 1 ou 3 anos.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

   Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando purchase-reserved-instances-offering para comprar sua Instância reservada. Especifique o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando describe-reserved-instances para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances
```

Como alternativa, use os seguintes comandos do AWS Tools for Windows PowerShell:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Após concluir a compra, se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será aplicado imediatamente. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução adequada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para ter mais informações, consulte Use as suas Instâncias reservadas.

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte Como as Instâncias reservadas são aplicadas.

Comprar Instâncias reservadas conversíveis

É possível comprar Instâncias reservadas conversíveis em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, é possível abandonar a reserva de capacidade e comprar uma Instância reservada convertível regional.

New console

Para comprar Instâncias reservadas conversíveis usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).

3. Em Offering class (Classe da oferta), escolha Convertible (Conversível) para exibir as Instâncias reservadas conversíveis.
4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra. Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

   Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.
6. Para cada Instância reservada convertível que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).
7. Para ver um resumo da sua seleção, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order all (Pedir tudo).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `Payment-pending` para `Active`. Quando a Instância reservada for `Active`, ela estará pronta para ser usada.

> **Note**
>
> Se o status mudar para `Retired`, a AWS pode não ter recebido seu pagamento.

Old console

Para comprar Instâncias reservadas conversíveis usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).
3. Em Offering class (Classe da oferta), escolha Convertible (Conversível) para exibir as Instâncias reservadas conversíveis.
4. Para comprar uma reserva de capacidade, escolha Mostrar apenas ofertas que reservam capacidade no canto superior direito da tela de compra. Para comprar uma Instância reservada regional, deixe a caixa de seleção desmarcada.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.
6. Para cada Instância reservada convertível que você deseja comprar, insira a quantidade e escolha Add to Cart (Adicionar ao carrinho).
7. Para ver um resumo da sua seleção, escolha View cart (Visualizar carrinho).
8. Se Order On (Pedir em) for Now (Agora), a compra será concluída imediatamente. Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order (Fazer pedido).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `payment-pending` para `active`. Quando a Instância reservada for `active`, ela estará pronta para ser usada.

> **Note**
>
> Se o status mudar para `retired`, a AWS pode não ter recebido seu pagamento.

Para comprar uma instância reservada conversível usando a AWS CLI

1. Localize as Instâncias reservadas disponíveis usando o comando describe-reserved-instances-offerings. Especifique `convertible` para o parâmetro `--offering-class` apresentar somente Instâncias reservadas conversíveis. É possível aplicar parâmetros adicionais para

estreitar seus resultados; por exemplo, se você quiser comprar uma Instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX`:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando purchase-reserved-instances-offering para comprar sua Instância reservada. Especifique o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando describe-reserved-instances para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances
```

Como alternativa, use os seguintes comandos do AWS Tools for Windows PowerShell:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será imediatamente aplicado. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução adequada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para ter mais informações, consulte Use as suas Instâncias reservadas.

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte Como as Instâncias reservadas são aplicadas.

Comprar do Marketplace da Instância reservada

É possível adquirir instâncias reservadas de vendedores terceiros que tenham instâncias reservadas de que não precisam mais do Marketplace de instâncias reservadas. É possível fazer isso usando o console do Amazon EC2 ou a ferramenta da linha de comando. O processo é semelhante à compra de instâncias reservadas da AWS. Para ter mais informações, consulte Comprar Instâncias reservadas padrão.

Existem poucas diferenças entre instâncias reservadas adquiridas no Marketplace de instâncias reservadas e adquiridas diretamente da AWS:

- Período de vigência: as instâncias reservadas que você compra de terceiros têm menos que um período de vigência padrão completo restante. Os períodos de vigência completos da AWS são de um ano ou três anos.
- Preço adiantado: as instâncias reservadas de terceiros podem ser vendidas em preços adiantados diferentes. As taxas de uso ou recorrentes são as mesmas que as taxas definidas quando as instâncias reservadas foram adquiridas originalmente da AWS.
- Tipos de instâncias reservadas: somente instâncias reservadas padrão do Amazon EC2 podem ser adquiridas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis, Amazon RDS e Amazon ElastiCache não estão disponíveis para compra no Marketplace de instâncias reservadas.

Informações básicas sobre você são compartilhadas com o vendedor – por exemplo, seu código postal e as informações do país.

Essas informações permitem que os vendedores calculem os impostos de transação necessários que precisam remeter ao governo (como impostos sobre vendas ou imposto sobre valor agregado) e são fornecidas na forma de um relatório de desembolso. Em raras circunstâncias, a AWS pode ter

de fornecer ao vendedor seu endereço de e-mail, de forma que possam entrar em contato com você sobre as perguntas relacionadas à venda (por exemplo, dúvidas sobre impostos).

Por motivos semelhantes, a AWS compartilha a razão social do vendedor na fatura de compra do comprador. Se você precisar de mais informações sobre o vendedor para fins de impostos ou algo relacionado, entre em contato com o AWS Support.

Como visualizar o Instâncias reservadas

É possível visualizar as Instâncias reservadas adquiridas usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Para visualizar as Instâncias reservadas no console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Seus Instâncias reservadas em fila, ativos e retirados estarão listados. A coluna Estado exibe o estado.
4. Se você for um vendedor no Marketplace de instâncias reservadas, a aba My Listings (Minhas ofertas) exibirá o status de uma reserva listada no Marketplace de instâncias reservadas. Para obter mais informações, consulte Estados de listagem da Instância reservada.

Para visualizar as Instâncias reservadas usando a linha de comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (Tools for Windows PowerShell)

Como cancelar uma compra colocada na fila

É possível colocar uma compra na fila por até três anos de maneira antecipada. É possível cancelar uma compra na fila a qualquer momento antes da hora programada.

New console

Como cancelar uma compra colocada na fila

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.

3. Selecione uma ou mais Instâncias reservadas.
4. Selecione Actions (Ações), Delete Queued Reserved Instances (Excluir instâncias reservadas na fila).
5. Quando a confirmação for solicitada, insira Delete (Excluir) e escolha Close (Fechar).

Old console

Como cancelar uma compra colocada na fila

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Selecione Actions (Ações), Delete Queued Reserved Instances (Excluir instâncias reservadas na fila).
5. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).

Como cancelar uma compra na fila usando a linha de comando

- delete-queued-reserved-instances (AWS CLI)
- Remove-EC2QueuedReservedInstance (Tools for Windows PowerShell)

Renovar uma Instância reservada

É possível renovar uma Instância reservada antes que ela esteja programada para expirar. Renovar uma Instância reservada coloca a compra de uma Instância reservada na fila com a mesma configuração até que a Instância reservada atual expire.

New console

Para renovar uma instância reservada usando uma compra em fila

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione a instância reservada para renovar.
4. Escolha Actions (Ações), Renew Reserved Instances (Renovar instâncias reservadas).
5. Para concluir o pedido, escolha Order all (Pedir tudo) e, em seguida, Close (Fechar).

Old console

Para renovar uma instância reservada usando uma compra em fila

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione a instância reservada para renovar.
4. Escolha Actions (Ações), Renew Reserved Instances (Renovar instâncias reservadas).
5. Para concluir o pedido, selecione Order (Fazer pedido).

Vender no Marketplace de instâncias reservadas

O Marketplace de instâncias reservadas é uma plataforma compatível com a venda padrão de instâncias reservadas padrão não utilizadas de clientes da AWS e de terceiros, que variam em termos de duração e opções de preço. Por exemplo, é possível querer vender as instâncias reservadas depois de mover instâncias para uma nova região da AWS, alterar para um novo tipo de instância, concluir projetos antes da expiração do prazo, quando suas necessidades de negócio mudarem ou quando tiver capacidade desnecessária.

Assim que você oferecer suas instâncias reservadas no Marketplace de instâncias reservadas, elas serão disponibilizadas para que possíveis compradores as encontrem. Todas as Instâncias reservadas são agrupadas de acordo com a duração do período de vigência restante e do preço por hora.

Para atender à solicitação de um comprador que deseja realizar a aquisição de uma instância reservada de um vendedor terceirizado por meio do Marketplace de instâncias reservadas do EC2, primeiro a AWS vende a instância reservada com o preço inicial mais baixo no agrupamento especificado. Em seguida, a AWS vende a instância reservada com o menor preço até que o pedido inteiro do comprador seja cumprido. A AWS então processa as transações e transfere a propriedade das instâncias reservadas ao comprador.

Você manterá a propriedade da Instância reservada até ela ser vendida. Após venda, você abre mão da reserva de capacidade e das taxas recorrentes com desconto. Se você continuar a usar sua instância, a AWS cobrará de você o preço sob demanda, a partir do momento em que sua instância reservada foi vendida.

Se você quiser vender suas instâncias reservadas não utilizadas no Marketplace de instâncias reservadas, deverá atender a determinados critérios de elegibilidade.

Para obter mais informações sobre como comprar instâncias reservadas no Marketplace de instâncias reservadas, consulte Comprar do Marketplace da Instância reservada.

Tópicos

- Restrições e limitações
- Registre-se como vendedor
- Conta de banco para desembolso
- Informações fiscais
- Precificar suas Instâncias reservadas
- Liste as suas Instâncias reservadas
- Estados de listagem da Instância reservada
- Ciclo de vida de uma lista
- Depois que a Instância reservada é vendida
- Recebimentos
- Informações compartilhadas com o comprador

Restrições e limitações

Antes que você possa vender suas reservas não utilizadas, é necessário registrar-se como vendedor no Marketplace de instâncias reservadas. Para ter mais informações, consulte Registre-se como vendedor.

As seguintes limitações e restrições são aplicáveis na venda da Instâncias reservadas:

- Somente as instâncias regional padrão e reservada zonal do Amazon EC2 podem ser vendidas no Marketplace de instâncias reservadas.
- Instâncias reservadas conversíveis do Amazon EC2 não podem ser vendidas no Marketplace de instâncias reservadas.
- Instâncias reservadas de outros serviços da AWS, como o Amazon RDS e o Amazon ElastiCache, não podem ser vendidas no Marketplace de instâncias reservadas.
- Deve haver pelo menos um mês restante no período de vigência da Instância reservada padrão.
- Não é possível vender uma Instância reservada standard em uma região que é desativada por padrão.
- O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.

- É possível vender instâncias reservadas sem adiantamento, com adiantamento parcial ou adiantamento integral no Marketplace de instâncias reservadas, desde que estejam ativas em sua conta há pelo menos 30 dias. Além disso, se houver um pagamento antecipado em uma instância reservada, ela só poderá ser vendida após a AWS ter recebido o pagamento adiantado.
- Você não pode modificar diretamente sua oferta no Marketplace de instâncias reservadas. No entanto, é possível alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos. Para ter mais informações, consulte Precificar suas Instâncias reservadas. Também é possível modificar as Instâncias reservadas antes de listá-las. Para obter mais informações, consulte Modificar a Instâncias reservadas.
- A AWS cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada padrão que você vender no Marketplace de instâncias reservadas. O preço inicial é aquele que o vendedor está cobrando pela Instância reservada padrão;.
- Quando você se registra como vendedor, o banco especificado deve ter um endereço nos EUA. Para obter mais informações, consulte Requisitos adicionais do vendedor para produtos pagos no Guia do vendedor do AWS Marketplace.
- Os clientes do Amazon Web Services India Private Limited (AWS India) não podem vender instâncias reservadas no Reserved Instance Marketplace mesmo que tenham uma conta bancária nos EUA. Para obter mais informações, consulte Quais são as diferenças entre as Contas da AWS e as contas da AWS India?

Registre-se como vendedor

> **Note**
>
> Somente o Usuário raiz da conta da AWS pode registrar uma conta como vendedor.

Para vender no Marketplace de instâncias reservadas, é necessário se registrar como vendedor. Durante o registro, você fornecerá as seguintes informações:

- Informações bancárias: a AWS deve ter suas informações bancárias para desembolsar os fundos recolhidos da venda das suas reservas. O banco que você especificar deverá ter um endereço nos EUA. Para ter mais informações, consulte Conta de banco para desembolso.
- Informação sobre impostos — todos os vendedores precisam concluir uma entrevista sobre informações de impostos para determinar qualquer obrigação de declaração de impostos necessária. Para ter mais informações, consulte Informações fiscais.

Depois que a AWS receber o registro preenchido do vendedor, você receberá um e-mail confirmando seu registro e informando que é possível começar a vender no Marketplace de instâncias reservadas.

Conta de banco para desembolso

A AWS deverá ter suas informações bancárias para pagar os fundos recolhidos quando você vender a instância reservada. O banco que você especificar deverá ter um endereço nos EUA. Para obter mais informações, consulte Requisitos adicionais do vendedor para produtos pagos no Guia do vendedor do AWS Marketplace.

Para registrar uma conta de banco padrão para desembolsos

1. Abra a página Reserved Instance Marketplace Seller Registration (Registro do vendedor do Marketplace de instâncias reservadas) e faça login usando as credenciais da AWS.
2. Na página Gerenciar conta bancária, forneça as informações a seguir sobre o banco para receber o pagamento:

   - Nome do titular da conta
   - Número de roteamento
   - Número da conta
   - Tipo de conta bancária

   > **Note**
   >
   > Se você estiver usando uma conta bancária corporativa, será solicitado que envie as informações sobre a conta bancária via fax (1-206-765-3424).

Após o registro, a conta bancária fornecida é definida como padrão, ficando pendente a verificação com o banco. Pode demorar até duas semanas para verificar uma conta bancária nova, e durante esse tempo você não poderá receber desembolsos. Para uma conta estabelecida, geralmente leva cerca de dois dias para os desembolsos serem concluídos.

Para alterar a conta de banco padrão para o desembolso

1. Na página Reserved Instance Marketplace Seller Registration (Registro do vendedor do Marketplace de instâncias reservadas), faça login na conta que você usou ao se registrar.

2. Na página Gerenciar conta bancária, adicione uma conta bancária nova ou modifique a conta bancária padrão conforme necessário.

Informações fiscais

A venda de Instâncias reservadas pode estar sujeita a um imposto baseado em transação, como imposto sobre vendas ou imposto sobre valor agregado. É necessário verificar com os departamentos fiscal, jurídico, financeiro ou contábil da sua empresa para determinar a aplicabilidade dos impostos de transação. Você é responsável para coletar e enviar impostos de transação para a devida autoridade fiscal.

Como parte do processo de registro do vendedor, é necessário completar uma entrevista sobre impostos no Portal de registro do vendedor. O entrevista coleta suas informações sobre impostos e preenche um formulário W-9, W-8BEN ou W-8BEN-E de IRS, que é usado para determinar todas as obrigações de declaração de impostos necessárias.

As informações sobre impostos inseridas como parte da entrevista sobre impostos pode diferir dependendo se você opera como um indivíduo ou como um negócio, e se você ou o seu negócio são ou não uma pessoa ou entidade dos EUA. Enquanto preenche a entrevista fiscal, tenha em mente o seguinte:

- Informações fornecidas pela AWS, inclusive as informações deste tópico, não constituem orientações jurídicas, fiscais ou profissional de alguma outra forma. Para descobrir como os requisitos de relatório da IRS podem afetar seu negócio, ou se você tiver outras dúvidas, entre em contato com seu orientador fiscal, jurídico ou profissional.
- Para atender os requisitos de relatório da IRS da forma mais eficiente possível, responda todas as perguntas e insira todas as informações solicitadas durante a entrevista.
- Verifique suas respostas. Evite erros de ortografia ou inserir números de identificação fiscal incorretos. Eles podem resultar em um formulário de impostos invalidado.

Com base nas respostas da entrevista fiscal e nos limites de declaração de imposto de renda, a Amazon pode registrar o Formulário 1099-K. A Amazon envia uma cópia do Formulário 1099-K em 31 de janeiro, ou antes disso, do ano seguinte ao ano em que sua conta fiscal chegar aos níveis do limite. Por exemplo, se sua conta atingir o limite em 2018, o formulário 1099-K será enviado até 31 de janeiro de 2019.

Para obter mais informações sobre os requisitos da IRS e o Formulário 1099-K, consulte o site da IRS.

Precificar suas Instâncias reservadas

Ao definir o preço para suas instâncias reservadas, considere o seguinte:

- Preço para pagamento adiantado: o preço para pagamento adiantado é o único preço que pode ser especificado para a instância reservada que você está vendendo. O preço para pagamento adiantado é o preço único que o comprador paga ao adquirir uma instância reservada.

  Como o valor das instâncias reservadas diminui com o tempo, por padrão, a AWS pode definir os preços para diminuir em incrementos iguais mês a mês. No entanto, é possível os preços iniciais diferentes com base nas vendas da sua reserva. Por exemplo, se sua Instância reservada tiver nove meses de prazo restante, é possível especificar a quantidade que aceitaria se um cliente comprar essa Instância reservada com nove meses restantes. É possível definir outro preço com cinco meses restantes, e ainda outro preço com um mês restante.

  O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.
- Limites: os limites para venda de instâncias reservadas a seguir se aplicam à vida útil de sua Conta da AWS. Eles não são limites anuais.
  - É possível vender até 50.000 USD em Instâncias reservadas.
  - É possível vender até 5.000 Instâncias reservadas.

  Esses limites normalmente não podem ser aumentados, mas serão avaliados caso a caso, se solicitado. Para solicitar um aumento de limite, use o formulário Aumento de limite de serviço. Em Tipo de limite, escolha Vendas de instâncias reservadas do EC2.
- Não é possível modificar: você não pode modificar diretamente sua lista. No entanto, é possível alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos.
- É possível cancelar: você pode cancelar sua lista a qualquer momento, desde que ela esteja no estado `active`. Você não poderá cancelar a lista se já houver correspondência ou se ela estiver sendo processada para uma venda. Se houver correspondências em algumas das instâncias da sua lista e você cancelar a lista, somente as instâncias não correspondentes restantes serão removidas.

Liste as suas Instâncias reservadas

Como vendedor registrado, é possível optar por vender uma ou mais de suas Instâncias reservadas. É possível escolher vender todos eles em uma lista ou em partes. Além disso, é possível listar as Instâncias reservadas com qualquer configuração de tipo de instância, plataforma e escopo.

O console determina um preço sugerido. Ele verifica as ofertas que correspondem à Instância reservada e relaciona a que tiver o preço mais baixo. Caso contrário, ele calcula um preço sugerido com base no custo da Instância reservada pelo tempo restante. Se o valor calculado for menor que 1,01 USD, o preço sugerido será de 1,01 USD.

Se você cancelar sua lista e parte da lista tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Para oferecer uma instância reservada no Marketplace de instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione as Instâncias reservadas para listar e escolha Actions (Ações) e Sell Instâncias reservadas (Vender Instâncias reservadas).
4. Na página Configurar a lista de Instância reservada, defina o número de instâncias para vender e o preço inicial para o prazo restante nas colunas relevantes. Veja como o valor de sua reserva muda com o restante do período ao selecionar a seta ao lado da coluna Meses restantes.
5. Se você for um usuário avançado e quiser personalizar o preço, poderá inserir valores diferentes nos meses subsequentes. Para retornar à queda de preço linear padrão, escolha Redefinir.
6. Escolha Continuar quando você tiver terminado de configurar sua lista.
7. Confirme os detalhes da sua lista na página Confirmar a lista da sua Instância reservada e, se estiver satisfeito, escolha Listar instância reservada.

Para visualizar suas listas no console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione a Instância reservada listada e escolha a guia My Listings (Minhas ofertas) na parte inferior da página.

Para gerenciar instâncias reservadas no Marketplace de instâncias reservadas usando a AWS CLI

1. Obtenha a lista das suas Instâncias reservadas usando o comando describe-reserved-instances.

2. Anote o ID da Instância reservada que você deseja listar e chame create-reserved-instances-listing. Especifique o ID da Instância reservada, o número de instâncias e a programação de preços.
3. Para visualizar sua lista, use o comando describe-reserved-instances-listings.
4. Para cancelar sua lista, use o comando cancel-reserved-instances-listings.

Estados de listagem da Instância reservada

O Estado da lista na guia Minhas listagens da página de Instâncias reservadas exibe o status atual das listagens:

As informações exibidas por Listing State (Estado da oferta) se referem ao status de sua oferta no Marketplace de instâncias reservadas. Isso é diferente das informações de status exibidas na coluna Estado da página Instâncias reservadas. Essas informações de Estado são sobre sua reserva.

- ativa—A lista está disponível para compra.
- canceled (cancelada): a oferta foi cancelada e não está disponível para compra no Marketplace de instâncias reservadas.
- closed—A Instância reservada não é listada. Uma Instância reservada pode ser `closed`, pois a venda da listagem foi concluída.

Ciclo de vida de uma lista

Quando todas as instâncias na sua lista forem correspondidas e vendidas, a guia Minhas listas visualizará que a Contagem de instâncias totais corresponde à contagem listada em Vendido. Além disso, não há instâncias Disponíveis deixadas para sua listagem, e o Status é `closed`.

Quando apenas parte da sua oferta é vendida, a AWS remove as instâncias reservadas na oferta e cria o número de instâncias reservadas igual ao das instâncias reservadas restantes na contagem. Assim, o ID da listagem e a listagem que a representa, que agora tem menos reservas à venda, ainda estão ativas.

Todas as vendas futuras das Instâncias reservadas nessa listagem serão processadas dessa maneira. Quando todas as instâncias reservadas na oferta forem vendidas, a AWS marcará a lista como `closed`.

Por exemplo, você cria um ID de listagem de Instâncias reservadas 5ec28771-05ff-4b9b-aa31-9e57dexample com uma contagem de 5.

A guia Minhas listas na página do console da Instância reservada exibirá a lista desta forma:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 0
- Disponíveis = 5
- Status = ativos

Um comprador compra duas das reservas, que deixa uma contagem de três reservas ainda disponíveis para venda. Por conta dessa venda parcial, a AWS cria uma nova reserva com uma contagem de três para representar as reservas restantes que ainda estão à venda.

Sua lista tem a seguinte forma na guia Minha lista:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 2
- Disponíveis = 3
- Status = ativos

Se você cancelar sua lista e parte da lista já tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Depois que a Instância reservada é vendida

Quando a instância reservada for vendida, a AWS enviará uma notificação por e-mail. Cada dia em que houver qualquer tipo de atividade, você receberá uma notificação por e-mail capturando todas as atividades do dia. As atividades podem incluir a criação ou a venda de uma oferta ou o envio de recursos financeiros para sua conta pela AWS.

Como rastrear o status de uma oferta de Instância reservada no console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página de navegação, escolha Reserved Instances (Instâncias reservadas).
3. Escolha a guia My Listings (Minhas ofertas).

A guia Minhas listas contém o valor de Estado da lista. Ela também contém informações sobre o período, o preço de tabela e um detalhamento de quantas instâncias na lista estão disponíveis, pendentes, vendidas e canceladas.

Também é possível usar o comando describe-reserved-instances-listings com o filtro apropriado para obter informações sobre suas listas.

Recebimentos

Assim que a AWS receber os valores do comprador, será enviada uma mensagem ao e-mail da conta do proprietário registrado para a instância reservada vendida.

A AWS faz uma transferência bancária via Automated Clearing House (ACH) para sua conta bancária especificada. Normalmente, essa transferência ocorre entre um e três dias após sua Instância reservada ter sido vendida. Os desembolsos ocorrem uma vez por dia. Você receberá um e-mail com o relatório de desembolso após o recurso financeiro ser liberado. Lembre-se de que você não poderá receber desembolsos até que a AWS tenha recebido verificação do seu banco. Isso pode levar até duas semanas.

A Instância reservada que você vendeu continua aparecendo quando você descreve as Instâncias reservadas.

Você recebe um reembolso em dinheiro pelas instâncias reservadas por meio de uma transferência eletrônica feita diretamente na sua conta bancária. A AWS cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada vendida no Marketplace de instâncias reservadas.

Informações compartilhadas com o comprador

Quando você vender no Marketplace de instâncias reservadas, a AWS compartilhará o nome legal da empresa no extrato do comprador, de acordo com as normas dos EUA. Além disso, se o comprador acessar o suporte da AWS Support porque precisa entrar em contato com você para obter uma fatura ou por outro motivo relacionado a impostos, a AWS pode precisar fornecer ao comprador no seu endereço de e-mail, de modo que ele possa entrar em contato diretamente com você.

Por motivos semelhantes, as informações de código postal do comprador e do país são fornecidas ao vendedor no relatório de desembolso. Como vendedor, é possível precisar dessas informações para acompanhar todos os impostos de transação necessários que você remeter ao governo (como impostos sobre vendas e impostos de valor agregado).

A AWS não pode oferecer orientações sobre impostos, mas se seu especialistas em impostos determinar que você precisa de informações adicionais específicas, entre em contato com o Suporte da AWS Support.

Modificar a Instâncias reservadas

Quando suas necessidades mudarem, será possível modificar seu padrão ou Instâncias reservadas conversíveis e continuar usufruindo o benefício de faturamento. É possível modificar atributos como a zona de disponibilidade, tamanho da instância (na mesma família e geração de instâncias), e escopo de sua Instância reservada.

> **Note**
>
> Também é possível trocar uma Instância reservada convertível por outra Instância reservada convertível com uma configuração diferente. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis.

É possível modificar todas as Instâncias reservadas ou um subconjunto delas. É possível separar suas Instâncias reservadas originais em duas ou mais novas Instâncias reservadas. Por exemplo, se você tiver uma reserva de 10 instâncias em `us-east-1a` e decidir mover 5 instâncias para `us-east-1b`, a solicitação da modificação resultará em duas novas reservas: uma para 5 instâncias em `us-east-1a` e outra para as outras 5 instâncias em `us-east-1b`.

Também é possível mesclar duas ou mais Instâncias reservadas em uma única Instância reservada. Por exemplo, se você tiver quatro `t2.small` Instâncias reservadas de uma instância cada, poderá mesclá-las para criar uma `t2.large` Instância reservada. Para obter mais informações, consulte Suporte para modificar tamanhos de instância.

Após a modificação, o benefício das Instâncias reservadas será aplicado somente às instâncias que correspondem aos novos parâmetros. Por exemplo, se você alterar a zona de disponibilidade de uma reserva, a reserva de capacidade e os benefícios de preço serão automaticamente aplicados ao uso da instância na nova zona de disponibilidade. Das instâncias que não corresponderem mais aos novos parâmetros, será cobrada a taxa sob demanda, a menos que sua conta tenha outras reservas aplicáveis.

Se sua solicitação da modificação tiver sucesso:

- A reserva modificada entra em vigor imediatamente e o benefício de preço é aplicado às novas instâncias que iniciam na hora da solicitação de modificação. Por exemplo, se você modificar com

êxito suas reservas às 9:15PM, o benefício do preço será transferido para sua nova instância às 9:00PM. É possível obter a data efetiva das Instâncias reservadas modificadas usando o comando describe-reserved-instances.

- A reserva original é desativada. A data final é a data inicial da nova reserva, e a data final da nova reserva é a mesma que a data final da Instância reservada original. Se você modificar uma reserva de três anos com 16 meses sobrando de período de vigência, a reserva modificada resultante será uma reserva de 16 meses com a mesma data final que a original.
- A reserva alterada lista um preço fixo de 0 USD e não o preço fixo da reserva original.
- O preço fixo da reserva modificada não afeta os cálculos da camada de preços com desconto aplicados à sua conta, que são baseados no preço fixo da reserva original.

Se sua solicitação de modificação falhar, as Instâncias reservadas manterão a configuração original e serão imediatamente disponibilizadas para outra solicitação de modificação.

Não há taxas para a modificação e você não receber nenhuma conta ou fatura novas.

É possível modificar suas reservas quantas vezes quiser, mas não pode alterar nem cancelar uma solicitação de modificação pendente depois da enviá-la. Depois de a modificação ser concluída com sucesso, é possível enviar outra solicitação de modificação para reverter as alterações que fez, se necessário.

Tópicos

- Requisitos e restrições para modificação
- Suporte para modificar tamanhos de instância
- Enviar solicitações de modificação
- Solucionar problemas de solicitações de modificação

Requisitos e restrições para modificação

É possível modificar esses atributos da maneira a seguir.

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar as zonas de disponibilidade na mesma região	Linux e Windows	-

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar o escopo de zona de disponibilidade para região e vice-versa	Linux e Windows	Uma instância reservada por zona tem escopo para uma zona de disponibilidade e reserva capacidade nessa zona de disponibilidade. Se você alterar o escopo de zona de disponibilidade para região (de zonal para regional), você perderá o benefício da reserva de capacidade. Uma instância reservada por região tem escopo para uma região. O desconto para instância reservada se aplica a instâncias executadas em qualquer zona de disponibilidade nessa região. Além disso, o desconto da instância reservada se aplica ao uso da instância em todos os tamanhos na família de instâncias selecionada. Se você alterar o escopo de região para zona de disponibilidade (ou seja, de regional para zonal), você perderá a flexibilidade da zona de disponibilidade e a flexibilidade de tamanho de instância (se aplicável). Para ter mais informações, consulte Como as Instâncias reservadas são aplicadas.

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar o tamanho da instância na mesma família e geração de instâncias	Somente Linux/UNIX A flexibilidade do tamanho da instância não está disponível para Instâncias reservadas nas outras plataformas, que incluem Linux com SQL Server Standard, Linux com SQL Server Web, Linux com SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web.	A reserva deve usar a locação padrão. Para algumas famílias de instâncias não há suporte, pois não há outros tamanhos disponíveis. Para ter mais informações, consulte Suporte para modificar tamanhos de instância.

Requisitos

O Amazon EC2 processará sua solicitação de modificação se houver capacidade suficiente para sua nova configuração (se aplicável) e se as seguintes condições forem atendidas:

- A Instância reservada não pode ser modificada antes ou ao mesmo tempo da compra
- a Instância reservada deve estar ativa.
- Não pode haver uma solicitação de modificação pendente
- A instância reservada não está listada no Marketplace de instâncias reservadas
- Deve haver correspondência entre o tamanho ocupado pela instância da reserva original e a nova configuração. Para obter mais informações, consulte Suporte para modificar tamanhos de instância.
- As Instâncias reservadas de entrada são todas Instâncias reservadas standard ou todas as Instâncias reservadas conversíveis, e não algumas de cada tipo
- As Instâncias reservadas de entrada deverão expirar na mesma hora, se forem Instâncias reservadas standard

- A instância reservada não é uma instância G4, G4ad, G4dn, G5, G5g, Inf1 ou Inf2.

Suporte para modificar tamanhos de instância

É possível modificar o tamanho da instância de um Instância reservada se os seguintes requisitos forem atendidos.

Requisitos

- A plataforma é Linux/UNIX.
- Você deve selecionar outro tamanho de instância na mesma família de instâncias (indicada por uma letra, p. ex., T) e geração (indicada por um número, p. ex., 2).

  Por exemplo, você pode modificar uma instância reservada de `t2.small` para `t2.large`, pois ambas estão na mesma família e geração T2. Porém, você não pode modificar uma instância reservada de T2 para M2 ou de T2 para T3, porque nesses dois exemplos, a família e a geração de instâncias de destino não são as mesmas da instância reservada original.
- Não é possível modificar o tamanho da instância de instâncias reservadas para as seguintes instâncias, porque cada uma delas tem apenas um tamanho:
  - `t1.micro`
- Não é possível modificar o tamanho da instância de instâncias reservadas para as seguintes combinações de família, geração e atributo da instância:
  - G4ad
  - G4dn
  - G5
  - G5g
  - Inf1
  - Inf2
- As Instância reservada original e modificada devem ter o mesmo espaço para tamanho de instância.

Tópicos

- Espaço para tamanho da instância
- Fatores de normalização para instâncias bare metal

Espaço para tamanho da instância

Cada Instância reservada tem um espaço para tamanho da instância, que é determinado pelo fator de normalização do tamanho de instância e pelo número de instâncias na reserva. Ao modificar os tamanhos da instância em uma Instância reservada, o espaço da nova configuração deverá ser equivalente ao da configuração original; caso contrário, a solicitação de modificação não será processada.

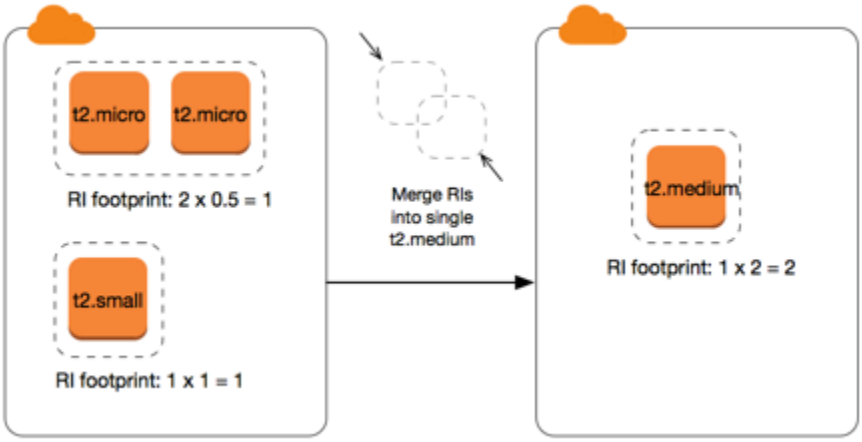
Para calcular o espaço para tamanho de instância de uma Instância reservada, multiplique o número de instâncias pelo fator de normalização. No console do Amazon EC2, o fator de normalização é medido em unidades. A tabela a seguir descreve o fator de normalização para os tamanhos de instância em uma família de instâncias. Por exemplo, `t2.medium` tem um fator de normalização de 2, por isso, uma reserva para quatro instâncias `t2.medium` tem um espaço de 8 unidades.

Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80

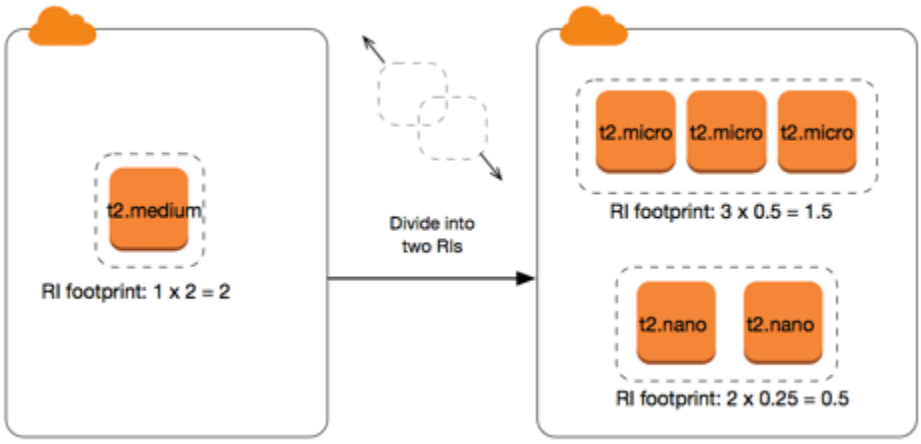
Tamanho da instância	Fator de normalização
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

É possível alocar suas reservas para tamanhos de instância diferentes na mesma família de instâncias, desde que o espaço para o tamanho da instância da sua reserva permaneça o mesmo. Por exemplo, é possível dividir uma reserva para uma instância `t2.large` (1 @ 4 unidades) em quatro instâncias `t2.small` (4 @ 1 unidade). Da mesma forma, é possível combinar uma reserva para quatro instâncias `t2.small` em uma instância `t2.large`. No entanto, você não pode alterar sua reserva para duas instâncias `t2.small` em uma instância `t2.large` porque o espaço da nova reserva (4 unidades) é maior que o espaço da reserva original (2 unidades).

No exemplo a seguir, você tem uma reserva com duas instâncias `t2.micro` (1 unidade) e uma reserva com uma instância `t2.small` (1 unidade). Se você mesclar ambas as reservas em uma única reserva com uma instância `t2.medium` (2 unidades), o espaço da nova reserva será igual ao espaço das reservas combinadas.



Também é possível modificar uma reserva para dividi-la em duas ou mais reservas. No exemplo a seguir, você tem uma reserva com uma instância `t2.medium` (2 unidades). É possível dividir a reserva em duas reservas, uma com duas instâncias `t2.nano` (0,5 unidades) e a outra com três instâncias `t2.micro` (1,5 unidades).



Fatores de normalização para instâncias bare metal

É possível modificar uma reserva com instâncias `metal` usando outros tamanhos na mesma família de instâncias. É possível modificar uma reserva com instâncias diferentes de instâncias bare metal usando o tamanho `metal` na mesma família de instâncias. Geralmente, uma instância bare metal tem o mesmo tamanho que o maior tamanho de instância disponível na mesma família de instâncias. Por exemplo, uma instância `i3.metal` é do mesmo tamanho que uma instância `i3.16xlarge`. Portanto, elas têm o mesmo fator de normalização.

A tabela a seguir descreve o fator de normalização para os tamanhos de instâncias bare metal em famílias de instâncias com instâncias bare metal. O fator de normalização para instâncias `metal` depende da família de instâncias, ao contrário dos outros tamanhos de instância.

Tamanho da instância	Fator de normalização
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Por exemplo, uma instância i3.metal tem um fator de normalização de 128. Se você comprar uma Instância reservada i3.metal de Linux/Unix da Amazon de locação padrão, será possível dividir a reserva da seguinte maneira:

- Uma instância i3.16xlarge é do mesmo tamanho que uma instância i3.metal, portanto, seu fator de normalização é de 128 (128/1). A reserva para uma instância i3.metal pode ser modificada para uma instância i3.16xlarge.
- Uma instância i3.8xlarge tem a metade do tamanho de uma instância i3.metal, portanto, seu fator de normalização é de 64 (128/2). A reserva para uma instância i3.metal pode ser dividida em duas instâncias i3.8xlarge.
- Uma instância i3.4xlarge é um quarto do tamanho de uma instância i3.metal, portanto, seu fator de normalização é de 32 (128/4). A reserva para uma instância i3.metal pode ser dividida em quatro instâncias i3.4xlarge.

Enviar solicitações de modificação

Antes de realizar modificações nas instâncias reservadas, certifique-se de ter lido as restrições aplicáveis. Antes de realizar modificações no tamanho da instância, calcule a área de ocupação do tamanho da instância das reservas originais que deseja modificar e certifique-se de que essa área corresponda à área de ocupação do tamanho da instância das suas novas configurações.

New console

Para modificar as instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página Reserved Instances (Instâncias reservadas), selecione uma ou mais Instâncias reservadas para modificar e escolha Actions (Ações), Modify Reserved Instances (Modificar instâncias reservadas).

   > **Note**
   >
   > Se as Instâncias reservadas não estiverem no estado ativo ou não puderem ser modificadas, a opção Modificar Instâncias reservadas estará desativada.

3. A primeira entrada na tabela de modificação exibe os atributos da Instâncias reservadas selecionada e pelo menos uma configuração de destino abaixo dela. A coluna Unidades exibe o espaço para tamanho total da instância. Escolha Adicionar para cada nova configuração a ser adicionada. Modifique os atributos conforme necessário para cada configuração.

   - Scope (Escopo): escolha se a configuração se aplica a uma zona de disponibilidade ou a toda a região.
   - Zona de disponibilidade: Escolha a zona de disponibilidade necessária. Não aplicável para Instâncias reservadas regionais.
   - Tipo de instância: selecione o tipo de instância necessário. As configurações combinadas devem ser iguais ao tamanho da instância das configurações originais.
   - Count (Contagem): especifique o número de instâncias. Para dividir as Instâncias reservadas em várias configurações, reduza a contagem, escolha Add (Adicionar) e especifique uma contagem para a configuração adicional. Por exemplo, se você tiver uma única configuração com uma contagem de 10, poderá alterar sua contagem para 6 e

adicionar uma configuração com uma contagem de 4. Esse processo desativa a Instância reservada original assim que as novas Instâncias reservadas são ativadas.

4. Escolha Continue.
5. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Submit modifications (Enviar modificações).
6. É possível determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. Os estados possíveis são os seguintes.

   - ativo (modificação pendente) — estado de transição das Instâncias reservadas originais.
   - desativado (modificação pendente) — estado de transição das Instâncias reservadas originais enquanto as novas Instâncias reservadas são criadas
   - desativado — Instâncias reservadas modificadas e substituídas com êxito
   - ativo — uma das seguintes opções:
     - Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida
     - Instâncias reservadas originais após falha na solicitação da modificação

Old console

Para modificar as instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página Reserved Instances (Instâncias reservadas), selecione uma ou mais Instâncias reservadas para modificar e escolha Actions (Ações), Modify Reserved Instances (Modificar instâncias reservadas).

   > **Note**
   >
   > Se as Instâncias reservadas não estiverem no estado ativo ou não puderem ser modificadas, a opção Modificar Instâncias reservadas estará desativada.

3. A primeira entrada na tabela de modificação exibe os atributos das Instâncias reservadas selecionadas e pelo menos uma configuração de destino abaixo dela. A coluna Unidades exibe o espaço para tamanho total da instância. Escolha Adicionar para cada nova configuração a ser adicionada. Modifique os atributos conforme o necessário para cada configuração e selecione Continue (Continuar):

- Scope (Escopo): escolha se a configuração se aplica a uma zona de disponibilidade ou a toda a região.
- Zona de disponibilidade: Escolha a zona de disponibilidade necessária. Não aplicável para Instâncias reservadas regionais.
- Tipo de instância: selecione o tipo de instância necessário. As configurações combinadas devem ser iguais ao tamanho da instância das configurações originais.
- Count (Contagem): especifique o número de instâncias. Para dividir as Instâncias reservadas em várias configurações, reduza a contagem, escolha Add (Adicionar) e especifique uma contagem para a configuração adicional. Por exemplo, se você tiver uma única configuração com uma contagem de 10, poderá alterar sua contagem para 6 e adicionar uma configuração com uma contagem de 4. Esse processo desativa a Instância reservada original assim que as novas Instâncias reservadas são ativadas.

4. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Submit modifications (Enviar modificações).
5. É possível determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. Os estados possíveis são os seguintes.

   - ativo (modificação pendente) — estado de transição das Instâncias reservadas originais.
   - desativado (modificação pendente) — estado de transição das Instâncias reservadas originais enquanto as novas Instâncias reservadas são criadas
   - desativado — Instâncias reservadas modificadas e substituídas com êxito
   - ativo — uma das seguintes opções:
     - Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida
     - Instâncias reservadas originais após falha na solicitação da modificação

Como modificar as Instâncias reservadas usando a linha de comando

1. Para modificar as Instâncias reservadas, é possível usar um dos comandos a seguir:
   - modify-reserved-instances (AWS CLI)
   - Edit-EC2ReservedInstance (AWS Tools for Windows PowerShell)
2. Para obter o status da modificação (`processing`, `fulfilled` ou `failed`) use um dos comandos a seguir:

- describe-reserved-instances-modifications (AWS CLI)
- Get-EC2ReservedInstancesModification (AWS Tools for Windows PowerShell)

Solucionar problemas de solicitações de modificação

Se as configurações de destino solicitadas forem exclusivas, você receberá uma mensagem de que sua solicitação está sendo processada. Neste ponto, o Amazon EC2 só determinou que os parâmetros da sua solicitação de modificação são válidos. A solicitação da modificação ainda pode falhar durante o processo em função de capacidade indisponível.

Em algumas situações, é possível receber uma mensagem indicando solicitações de modificação incompletas ou falhas em vez de confirmação. Use as informações nessas mensagens como ponto inicial para enviar novamente outra solicitação de modificação. Certifique-se de que você leu as restrições aplicáveis antes de enviar a solicitação.

Nem todas as Instâncias reservadas selecionadas podem ser processadas para modificação

O Amazon EC2 identifica e lista as Instâncias reservadas que não podem ser modificadas. Se você receber uma mensagem como essa, acesse a página Reserved Instances (Instâncias reservadas) no console do Amazon EC2 e verifique as informações sobre as Instâncias reservadas.

Erro ao processar sua solicitação de modificação

Você enviou uma ou mais Instâncias reservadas para modificação e nenhuma das solicitações pode ser processada. Dependendo do número de reservas que estiver modificando, é possível obter versões diferentes da mensagem.

O Amazon EC2 exibe os motivos pelos quais sua requisição não pode ser processada. Por exemplo, é possível ter especificado a mesma combinação de destino — uma combinação de zona de disponibilidade e plataforma — para um ou mais subconjuntos das Instâncias reservadas que está modificando. Experimente enviar as solicitações de modificação novamente, mas verifique se os detalhes da instância das reservas correspondem, e as configurações de destino para todos os subconjuntos que estiverem sendo modificados são exclusivas.

Trocar Instâncias reservadas conversíveis

É possível trocar uma ou mais Instâncias reservadas conversíveis por outra Instância reservada convertível com uma configuração diferente, inclusive a família de instâncias, o sistema operacional e a locação. Não há limites de quantas vezes você realiza uma troca, desde que a nova Instância

reservada conversível tenha valor igual ou superior às Instâncias reservadas conversíveis que você está trocando.

Ao trocar sua instância reservada conversível, o número de instâncias da sua reserva atual é trocado por um número de instâncias que cobrem o valor igual ou superior da configuração da nova instância reservada conversível. O Amazon EC2 calcula o número de instâncias reservadas que é possível receber como resultado da troca.

Você não pode trocar Instâncias reservadas padrão, mas pode modificá-las. Para obter mais informações, consulteModificar a Instâncias reservadas

Tópicos

- Requisitos para trocar de Instâncias reservadas conversíveis
- Calcular trocas de Instâncias reservadas conversíveis
- Mesclar Instâncias reservadas conversíveis
- Trocar uma parte de uma Instância reservada convertível
- Enviar solicitações de troca

Requisitos para trocar de Instâncias reservadas conversíveis

Se as condições a seguir forem atendidas, o Amazon EC2 processará sua solicitação de troca. A Instância reservada convertível deve estar:

- Ativo
- Não pode haver uma solicitação de troca anterior pendente
- Tenha pelo menos 24 horas restantes do prazo de validade

As seguintes regras se aplicam:

- As instâncias reservadas conversíveis só podem ser trocadas por outras instâncias reservadas conversíveis oferecidas atualmente pela AWS.
- As Instâncias reservadas conversíveis são associadas a uma região específica, que é fixada para a duração do período da reserva. Não é possível trocar uma Instância reservada convertível por uma Instância reservada convertível de outra região.
- É possível trocar uma ou mais Instâncias reservadas conversíveis por vez por uma única Instância reservada convertível somente.

- Para trocar parte de uma Instância reservada convertível, é possível modificá-la em duas ou mais reservas e, em seguida, trocar uma ou mais reservas por uma nova Instância reservada convertível. Para ter mais informações, consulte Trocar uma parte de uma Instância reservada convertível. Para obter mais informações sobre como modificar Instâncias reservadas, consulte Modificar a Instâncias reservadas.
- As Instâncias reservadas conversíveis com adiantamento total podem ser trocadas por Instâncias reservadas conversíveis com adiantamentos parciais e vice-versa.

> **Note**
>
> Se o pagamento adiantado total necessário para a troca (custo alinhado) for menor do que USD 0,00, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá o custo alinhado de USD 0,00 ou mais.

> **Note**
>
> Se o valor total (preço adiantado + preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Para se beneficiar com preços melhores, é possível trocar uma Instância reservada convertível sem adiantamento por uma Instância reservada convertível com adiantamento total ou parcial.
- Você não pode trocar Instâncias reservadas conversíveis com adiantamento total e parcial por Instâncias reservadas conversíveis sem adiantamento.
- Só é possível trocar uma Instância reservada convertível sem adiantamento por uma outra Instância reservada convertível sem adiantamento se o preço por hora da nova Instância reservada convertível for igual ou superior ao preço por hora da Instância reservada convertível que foi trocada.

> **Note**
>
> Se o valor total (preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância

reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Se você trocar várias Instâncias reservadas conversíveis com datas de expiração diferentes, a data de expiração da nova Instância reservada convertível será a data futura mais longe.
- Se você trocar uma única Instância reservada convertível, ela deverá ter o mesmo período de vigência (um ano ou três anos) da nova Instância reservada convertível. Se você mesclar várias Instâncias reservadas conversíveis com períodos de vigência diferentes, a nova Instância reservada convertível terá um período de vigência de três anos. Para ter mais informações, consulte Mesclar Instâncias reservadas conversíveis.
- Quando o Amazon EC2 troca uma instância reservada conversível, ele retira a reserva associada e transfere a data de término para a nova reserva. Após a troca, o Amazon EC2 define a data de término da reserva antiga e a data de início da nova reserva como a data da troca. Por exemplo, se você trocar uma reserva de três anos com 16 meses restantes do período de vigência, a nova reserva será uma reserva de 16 meses com a mesma data de término que a reserva da Instância reservada conversível que você trocou.

Calcular trocas de Instâncias reservadas conversíveis

A troca de Instâncias reservadas conversíveis são gratuitas. Porém, pode ser necessário pagar o custo diferencial, que é o custo à vista pro rata da diferença entre as Instâncias reservadas conversíveis que você tinha e as novas Instâncias reservadas conversíveis que você recebe na troca.

Cada Instância reservada convertível tem um valor de tabela. Esse valor de tabela é comparado ao valor de tabela das Instâncias reservadas conversíveis que você deseja para determinar quantas reservas de instância é possível receber com a troca.

Por exemplo: você tem uma Instância reservada convertível com valor de tabela de 35 USD que deseja trocar por um novo tipo de instância com um valor de tabela de 10 USD.

```
$35/$10 = 3.5
```

É possível trocar sua Instância reservada convertível por três Instâncias reservadas conversíveis de US$ 10. Não é possível adquirir meias reservas; portanto, é necessário comprar uma Instância reservada convertível adicional que cubra o restante:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

A quarta Instância reservada convertível tem a mesma data de término das outras três. Se você estiver trocando Instâncias reservadas conversíveis com adiantamento integral ou parcial, pagará o custo alinhado da quarta reserva. Se o custos iniciais restante das Instâncias reservadas conversíveis forem USD 500 e a reserva de destino custar normalmente USD 600 pro rata, será cobrado de você USD 100.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Mesclar Instâncias reservadas conversíveis

Se você combinar duas ou mais Instâncias reservadas conversíveis, o termo da nova Instância reservada conversível deverá ser o mesmo das instâncias reservadas conversíveis originais ou o mais alto das instâncias reservadas conversíveis originais. A data de expiração da nova Instância reservada convertível é a data de expiração mais avançada no futuro.

Por exemplo, você tem as seguintes Instâncias reservadas conversíveis na conta:

ID da Instância reservada	Prazo	Data de validade
aaaa1111	1 ano	31/12/2018
bbbb2222	1 ano	31/07/2018
cccc3333	3 anos	30/06/2018
dddd4444	3 anos	31/12/2019

- É possível mesclar `aaaa1111` e `bbbb2222` e trocá-las por uma Instância reservada convertível de um ano. Você não pode trocá-las por uma Instância reservada convertível de três anos. A data de expiração da nova Instância reservada convertível é 31/12/2018.
- É possível mesclar `bbbb2222` e `cccc3333` e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/07/2018.

- É possível mesclar `cccc3333` e `dddd4444` e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/12/2019.

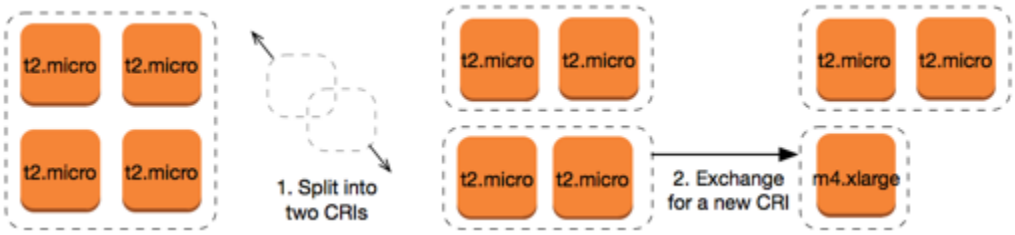
Trocar uma parte de uma Instância reservada convertível

É possível usar o processo de modificação para dividir a Instância reservada convertível em reservas menores e, em seguida, trocar uma ou mais reservas novas por uma nova Instância reservada convertível. Os exemplos a seguir demonstram como fazer isso.

Example Exemplo: Instância reservada convertível com várias instâncias

Neste exemplo, você tem uma `t2.micro` Instância reservada convertível com quatro instâncias na reserva. Para trocar duas instâncias `t2.micro` por uma instância `m4.xlarge`:

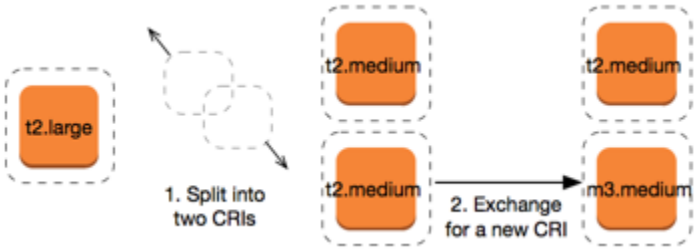
1. Modifique a `t2.micro` Instância reservada convertível dividindo-a em duas `t2.micro` Instâncias reservadas conversíveis com duas instâncias cada uma.
2. Troque uma das novas `t2.micro` Instâncias reservadas conversíveis por uma `m4.xlarge` Instância reservada convertível.



Example Exemplo: Instância reservada convertível com uma única instância

Neste exemplo, você tem uma `t2.large` Instância reservada convertível. Para transformá-la em uma instância `t2.medium` menor e em uma instância `m3.medium`:

1. Modifique a `t2.large` Instância reservada convertível dividindo-a em duas `t2.medium` Instâncias reservadas conversíveis. Uma única instância `t2.large` tem o mesmo espaço para tamanho da instância que duas instâncias `t2.medium`.
2. Troque uma das novas `t2.medium` Instâncias reservadas conversíveis por uma `m3.medium` Instância reservada convertível.



Para ter mais informações, consulte Suporte para modificar tamanhos de instância e Enviar solicitações de troca.

Enviar solicitações de troca

É possível trocar as Instâncias reservadas conversíveis usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Troque uma Instância reservada convertível usando o console

É possível procurar ofertas de Instâncias reservadas conversíveis e selecionar sua nova configuração entre as escolhas apresentadas.

New console

Para trocar Instâncias reservadas conversíveis usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias reservadas, selecione as Instâncias reservadas conversíveis a serem trocadas e escolha Ações, Trocar Instância reservada.
3. Selecione os atributos da configuração desejada e escolha Find offering (Localizar oferta).
4. Selecione uma nova Instância reservada convertível. Na parte inferior da tela, é possível visualizar o número da Instâncias reservadas que você receber para a troca, além de quaisquer custos adicionais.
5. Ao selecionar uma Instância reservada convertível que atenda às suas necessidades, escolha Review (Revisar).
6. Escolha Exchange (Troca) e, em seguida, Close (Fechar).

Old console

Para trocar Instâncias reservadas conversíveis usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias reservadas, selecione as Instâncias reservadas conversíveis a serem trocadas e escolha Ações, Trocar Instância reservada.
3. Selecione os atributos da configuração desejada e escolha Find Offering (Localizar oferta).
4. Selecione uma nova Instância reservada convertível. A coluna Instance Count (Contagem de instâncias) exibirá o número de Instâncias reservadas que você recebe pela troca. Ao selecionar uma Instância reservada convertível que atenda às suas necessidades, escolha Exchange (Troca).

As Instâncias reservadas que foram trocadas foram eliminadas e as novas Instâncias reservadas são exibidas no console do Amazon EC2. Esse processo pode levar alguns minutos para ser propagado.

Trocar uma Instância reservada convertível usando a interface da linha de comando

Para trocar uma Instância reservada convertível, primeiro localize uma Instância reservada convertível de destino que atenda às suas necessidades:

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering (Tools for Windows PowerShell)

Obtenha uma cotação para a troca, que inclua o número de Instâncias reservadas obtidas na troca e o custo alinhado da troca:

- get-reserved-instances-exchange-quote (AWS CLI)
- GetEC2-ReservedInstancesExchangeQuote (Tools for Windows PowerShell)

Por fim, execute a troca:

- accept-reserved-instances-exchange-quote (AWS CLI)
- Confirm-EC2ReservedInstancesExchangeQuote (Tools for Windows PowerShell)

Cotas de instâncias reservadas

Você poderá comprar novas instâncias reservadas a cada mês. O número de novas instâncias reservadas que é possível comprar por mês é determinado por sua cota mensal, da seguinte forma:

Descrição da cota	Cota padrão
Novas instâncias reservadas regionais	20 por região por mês
Novas instâncias reservadas zonais	20 por zona de disponibilidade por mês

Por exemplo, em uma região com três zonas de disponibilidade, a cota padrão é de 80 novas instâncias reservadas por mês, calculada da seguinte forma:

- 20 instâncias reservadas regionais para a região
- Mais 60 instâncias reservadas zonais (20 para cada uma das três zonas de disponibilidade)

As instâncias no estado `running` contam para sua cota. As instâncias que estão nos estados `pending`, `stopping`, `stopped` e `hibernated` não contam para sua cota.

Visualizar o número de instâncias reservadas que você comprou

O número de instâncias reservadas compradas por você é indicado pelo campo Instance count (Contagem de instâncias) (console) ou o parâmetro `InstanceCount` (AWS CLI). Quando você compra novas instâncias reservadas, a cota é medida em relação à contagem total de instâncias. Por exemplo, se você comprar uma única configuração de instância reservada com uma contagem de instâncias igual 10, a compra contará para sua cota como 10, e não como 1.

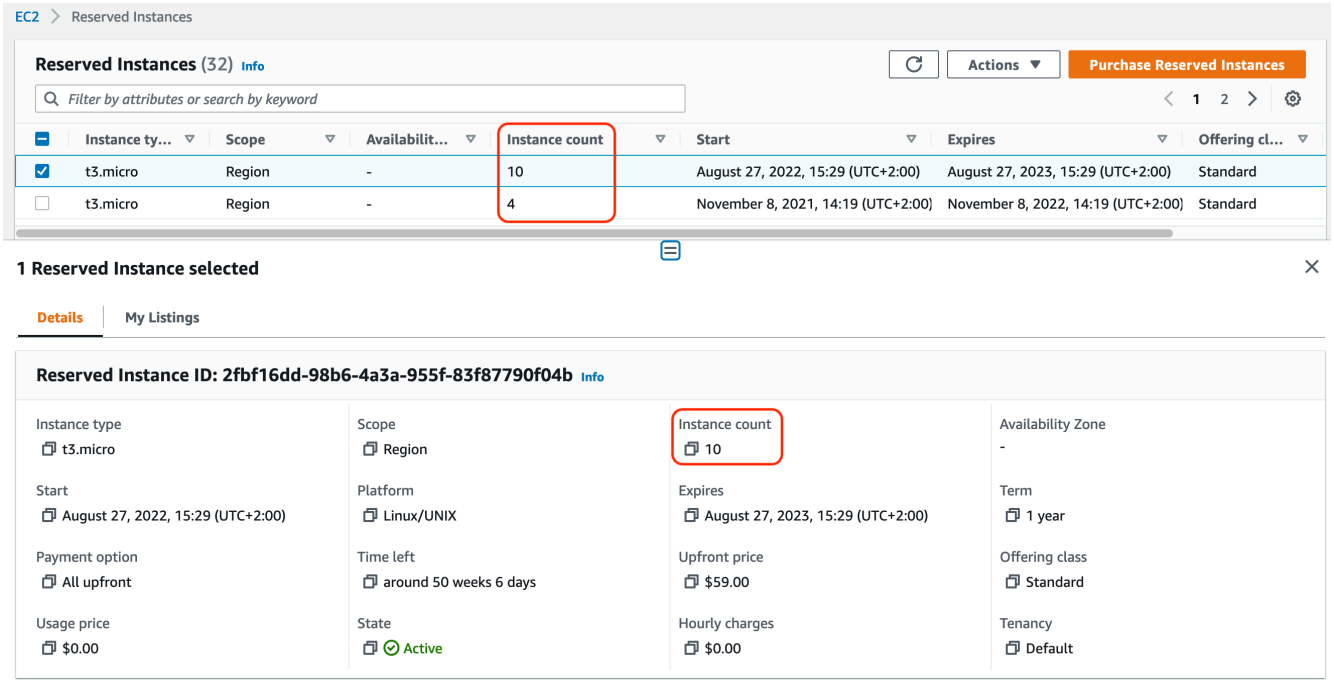
É possível ver quantas instâncias reservadas você comprou usando o Amazon EC2 ou a AWS CLI.

Console

Para ver o número de instâncias reservadas que você comprou

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma configuração de instância reservada na tabela e verifique o campo Instance count (Contagem de instâncias).

Na captura de tela a seguir, a linha selecionada representa uma única configuração de instância reservada para um tipo de instância `t3.micro`. A coluna Instance count (Contagem de instâncias) na visualização da tabela e no campo Instance count (Contagem de instâncias) na visualização detalhada (descrito na captura de tela) indica que há 10 instâncias reservadas para essa configuração.



AWS CLI

Para ver o número de instâncias reservadas que você comprou

User o comando describe-reserved-instances da CLI e especifique o ID da configuração da instância reservada.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
    --output table
```

Exemplo de saída: o campo `InstanceCount` indica que há 10 instâncias reservadas para essa configuração.

```
-------------------------------------------------------------------
|                   DescribeReservedInstances                     |
+-----------------------------------------------------------------+
```

```
||                      ReservedInstances                          ||
|+----------------------+-----------------------------------------+|
||  CurrencyCode        |  USD                                    ||
||  Duration            |  31536000                               ||
||  End                 |  2023-08-27T13:29:44+00:00              ||
||  FixedPrice          |  59.0                                   ||
||  InstanceCount       |  10                                     ||
||  InstanceTenancy     |  default                                ||
||  InstanceType        |  t3.micro                               ||
||  OfferingClass       |  standard                               ||
||  OfferingType        |  All Upfront                            ||
||  ProductDescription  |  Linux/UNIX                             ||
||  ReservedInstancesId |  2fbf16dd-98b6-4a3a-955f-83f87790f04b   ||
||  Scope               |  Region                                 ||
||  Start               |  2022-08-27T13:29:45.938000+00:00       ||
||  State               |  active                                 ||
||  UsagePrice          |  0.0                                    ||
|+----------------------+-----------------------------------------+|
|||                      RecurringCharges                         |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

Considerações

Um regional Instância reservada aplica um desconto para um instância sob demanda em execução. O instância sob demanda padrão é 20. Não é possível exceder o limite de execução do instância sob demanda, comprando regional Instâncias reservadas. Por exemplo, se você já tem 20 Instâncias on-demand em execução e você adquiri 20 regional Instâncias reservadas, essas 20 regional Instâncias reservadas serão usadas para aplicar desconto nas 20 Instâncias on-demand em execução. Se você compra mais regional Instâncias reservadas, não será possível iniciar mais instâncias porque alcançou seu limite do instância sob demanda.

Antes de comprar Instâncias reservadas regionais, verifique se o limite de instância sob demanda corresponde ou excede o número de Instâncias reservadas regionais que você pretende ter. Se necessário, solicite um aumento de seu limite de instância sob demanda antes de comprar mais Instâncias reservadas regionais.

Uma instância reservada zonal (uma Instância reservada que é comprada para uma zona de disponibilidade específica) e que fornece reserva de capacidade, bem como um desconto. É

possível exceder o limite de execução do instância sob demanda, comprando zonal Instâncias reservadas. Por exemplo, se você já tem 20 Instâncias on-demand em execução e você adquiri 20 zonal Instâncias reservadas, é possível iniciar mais 20 Instâncias on-demand que correspondam às especificações de sua zonal Instâncias reservadas, dando a você um total de 40 instâncias em execução.

Visualize suas cotas de instância reservada e solicite um aumento de cota

O console do Amazon EC2 fornece informações sobre as cotas. Também é possível solicitar um aumento em suas cotas. Para ter mais informações, consulte Visualizar as cotas atuais e Solicitar um aumento.

Instâncias spot

Uma instância spot é uma instância que usa capacidade adicional do EC2 que está disponível por um valor mais baixo que o preço sob demanda. Como as Instâncias spot permitem que você solicite instâncias do EC2 não usadas com descontos consideráveis, é possível reduzir seus custos do Amazon EC2 significativamente. O preço por hora de uma instância spot é chamado de preço spot. O preço spot de cada tipo de instância em cada zona de disponibilidade é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e a demanda de longo prazo das Instâncias spot. Sua instância spot executará sempre que houver capacidade disponível.

As Instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executadas e se as aplicações poderão ser interrompidas. Por exemplo, as Instâncias spot são adequadas para análise de dados, trabalhos em lote, processamento em segundo plano e tarefas opcionais. Para obter mais informações, consulte Instâncias spot do Amazon EC2.

Para obter uma comparação das diferentes opções de compra de instância do EC2, consulte Opções de compra de instância.

Tópicos

- Conceitos
- Como começar a usar
- Serviços relacionados
- Definição de preço e economia

Conceitos

Antes de começar a trabalhar com instâncias spot, é necessário se familiarizar com os seguintes conceitos:

- Grupo de capacidade spot: um conjunto de instâncias do EC2 não utilizadas com o mesmo tipo de instância (por exemplo, `m5.large`) e zona de disponibilidade.
- Preço spot: o preço atual de uma instância spot por hora.
- Solicitação de instância Spot: solicita uma instância spot. Quando houver capacidade disponível, o Amazon EC2 atenderá à solicitação. Uma solicitação de instância spot é única ou persistente. O Amazon EC2 reenvia automaticamente uma solicitação de instância spot persistente depois que a instância spot associada à solicitação for interrompida.

- Recomendação de rebalanceamento de instância do EC2: o Amazon EC2 emite um sinal de recomendação de rebalanceamento de instância para avisar que uma instância spot apresenta risco elevado de interrupção. Esse sinal fornece uma oportunidade de rebalancear proativamente as workloads entre instâncias spot novas ou existentes sem que seja necessário aguardar o aviso de interrupção de dois minutos da instância spot.
- Interrupção de instância spot: o Amazon EC2 encerra, interrompe ou coloca em hibernação a instância spot quando o Amazon EC2 precisa novamente da capacidade. O Amazon EC2 fornece um aviso de interrupção da instância spot, enviando à instância um aviso de dois minutos antes que ela seja interrompida.

Principais diferenças entre Instâncias spot e Instâncias on-demand

A tabela a seguir lista as principais diferenças entre instâncias spot e instâncias sob demanda.

	Spot Instances	On-Demand Instances
Horário do lançamento	Só poderá ser executado imediatamente se a solicitação da instância spot estiver ativa e a capacidade estiver disponível.	Só poderá ser executado imediatamente se você fizer uma solicitação de execução manual e se a capacidade estiver disponível.
Capacidade disponível	Se a capacidade não estiver disponível, a solicitação de instância spot continuará a fazer a solicitação de inicialização automaticamente até que a capacidade seja disponibilizada.	Se a capacidade não estiver disponível quando você fizer uma solicitação de execução, você receberá um erro de capacidade insuficiente (ICE).
Custo por hora	O preço por hora das instâncias spot varia de acordo com a demanda e oferta de longo prazo.	O preço por hora de Instâncias on-demand é estático.
Recomendação de rebalanceamento	O sinal que o Amazon EC2 emite para uma instância spot em execução quando a instância possui risco elevado de interrupção.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).

	Spot Instances	On-Demand Instances
Interrupção de instância	É possível interromper e iniciar uma instância spot baseada no Amazon EBS. Além disso, o Amazon EC2 poderá interromper uma instância spot individual se a capacidade não estiver mais disponível.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).

Como começar a usar

A primeira coisa que é necessário fazer é se preparar para usar o Amazon EC2. Também pode ser útil testar a execução de Instâncias on-demand antes de executar Instâncias spot.

Noções básicas do spot

- Como as Instâncias spot funcionam

Trabalho com Instâncias spot

- Criar uma solicitação de instância spot
- Obter informações do status da solicitação
- Interrupções de instâncias spot

Serviços relacionados

É possível provisionar Instâncias spot usando diretamente o Amazon EC2. É possível provisionar as instâncias spot usando outros serviços da AWS. Para obter mais informações, consulte a documentação a seguir.

Amazon EC2 Auto Scaling e Instâncias spot

> É possível criar configurações ou modelos de execução para que o Amazon EC2 Auto Scaling possa executar Instâncias Spot. Para obter mais informações, consulte Solicitar Instâncias spot aplicações flexíveis e tolerantes a falhas e Auto Scaling grupos com vários tipos de instância e opções de compra no Guia do usuário do Amazon EC2 Auto Scaling.

Amazon EMR e Instâncias spot

Há cenários em que pode ser útil executar Instâncias spot em um cluster do Amazon EMR. Para obter mais informações, consulte Instâncias spot e Quando use Instâncias spot no Guia de gerenciamento do Amazon EMR.

Modelos do AWS CloudFormation

O AWS CloudFormation permite que você crie e gerencie uma coleção de recursos da AWS utilizando um modelo no formato JSON. Para obter mais informações, consulte EC2 Spot Instance Updates - Auto Scaling and CloudFormation Integration (Atualizações de instâncias spot do EC2: integração do Auto Scaling e do CloudFormation).

AWS SDK for Java

É possível usar a linguagem de programação Java para gerenciar as Instâncias spot. Para obter mais informações, consulte Tutorial: Instâncias spot do Amazon EC2 e Tutorial: Gerenciamento avançado de solicitações spot do Amazon EC2.

AWS SDK for .NET

É possível usar o ambiente de programação .NET para gerenciar as Instâncias spot. Para obter mais informações, consulte Tutorial: Instâncias spot do Amazon EC2.

Definição de preço e economia

Você paga o preço spot por Instâncias spot, que é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e demanda de longo prazo das Instâncias spot. Suas Instâncias spot serão executadas até que você as encerre, a capacidade não esteja mais disponível ou seu grupo do Amazon EC2 Auto Scaling as encerre durante o processo de reduzir a escala horizontalmente.

Se você ou o Amazon EC2 interromper uma instância spot em execução, você será cobrado pelos segundos usados ou pela hora completa, ou então não será cobrado, dependendo do sistema operacional usado e de quem interrompeu a instância spot. Para ter mais informações, consulte Faturamento para Instâncias spot interrompidas.

As instâncias spot não são cobertas pelos Savings Plans. Se tiver um Savings Plan, ele não oferecerá vantagens econômicas adicionais, além das que você já obtém com o uso de instâncias spots. Além disso, seus gastos com instâncias spot não aplicam os compromissos dos Savings Plans para computação.

Visualizar preços

Para ver o menor preço atual de instâncias spot (atualizado a cada cinco minutos) por Região da AWS e tipo de instância, consulte a página Definição de preço de instâncias spot do Amazon EC2.

Para visualizar o histórico de preços spot dos últimos três meses, use o console do Amazon EC2 ou o comando describe-spot-price-history (AWS CLI). Para ter mais informações, consulte Histórico de definição de preço da instância spot.

Mapeamos as zonas de disponibilidade para os códigos de cada Conta da AWS de maneira independente. Portanto, é possível obter resultados diferentes para o mesmo código de zona de disponibilidade (por exemplo, `us-west-2a`) entre contas diferentes.

Visualizar economias

É possível visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. É possível visualizar as economias feitas na última hora ou nos últimos três dias, além de visualizar o custo médio por hora de vCPU e por hora de memória (GiB). As economias são estimadas e podem ser diferentes das economias reais porque não incluem os ajustes de faturamento de seu uso. Para obter mais informações sobre a visualização das economias, consulte Economia na compra das Instâncias spot.

Exibir faturamento

Sua fatura fornece detalhes sobre seu uso do serviço. Para obter mais informações, consulte Exibição da sua fatura no Guia do usuário do AWS Billing.

Melhores práticas para o EC2 Spot

As instâncias spot do Amazon EC2 são a capacidade computacional sobressalente do EC2 na Nuvem AWS que está disponível para você com um desconto de até 90% em comparação com os preços de instâncias spot sob demanda. A única diferença entre Instâncias on-demand e Instâncias spot é que as Instâncias spot podem ser interrompidas pelo Amazon EC2, com dois minutos de notificação, quando o Amazon EC2 precisa da capacidade de volta.

As Instâncias spot são recomendadas para aplicações flexíveis, tolerantes a falhas e sem estado. Por exemplo, as Instâncias spot funcionam bem para big data, workloads em contêineres, CI/CD, servidores Web sem estado, computação de alta performance (HPC) e workloads de renderização.

Durante a execução, as Instâncias spot são exatamente as mesmos que as Instâncias on-demand. No entanto, o Spot não garante que você possa manter as instâncias em execução tempo suficiente

para concluir as workloads. O Spot também não garante que você possa obter disponibilidade imediata das instâncias que está procurando, nem que sempre possa obter a capacidade agregada solicitada. Além disso, as interrupções e a capacidade da instância spot podem mudar ao longo do tempo porque a disponibilidade da instância spot varia de acordo com a oferta e a demanda, e a performance passada não é uma garantia de resultados futuros.

As Instâncias spot não são adequadas para workloads que são inflexíveis, com estado, intolerantes a falhas ou fortemente acopladas entre nós de instância. As instâncias spot também não são recomendadas para workloads que não sejam tolerantes a períodos ocasionais em que a capacidade-alvo não está totalmente disponível. Seguir as práticas recomendadas para spot de ser flexível em termos de tipos de instância e zonas de disponibilidade é a melhor chance de ter alta disponibilidade, mas isso não garante que haverá capacidade disponível, pois os picos na demanda de instâncias sob demanda podem perturbar as workloads nas instâncias spot.

Não é recomendável usar instâncias spot para essas workloads nem tentar fazer failover para instâncias sob demanda como forma de lidar com interrupções ou períodos de indisponibilidade. Fazer failover para instâncias sob demanda pode inadvertidamente causar interrupções em outras instâncias spot. Além disso, se as instâncias spot de uma combinação de tipo de instância e zona de disponibilidade forem interrompidas, poderá ser difícil obter instâncias sob demanda com a mesma combinação.

Independentemente de você ser um usuário spot experiente ou iniciante na utilização de instâncias spot, se estiver enfrentando problemas com interrupções ou disponibilidade de instâncias spot no momento, recomendamos que siga essas práticas recomendadas para ter a melhor experiência usando o serviço spot.

Melhores práticas do Spot

- Preparar instâncias individuais para interrupções
- Ser flexível sobre tipos de instância e zonas de disponibilidade
- Usar grupos do Auto Scaling ou a Frota do EC2 para gerenciar a capacidade agregada
- Usar a estratégia de alocação otimizada para preço e capacidade
- Use serviços integrados da AWS para gerenciar as instâncias spot
- Qual é o melhor método de solicitação spot para usar?

Preparar instâncias individuais para interrupções

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, é possível aproveitar as recomendações de rebalanceamento de instâncias do EC2 e avisos de interrupção de instâncias spot.

Uma recomendação de rebalanceamento de uma instância do EC2 é um sinal que notifica você quando uma instância spot corre grande risco de interrupção. O sinal oferece a oportunidade de gerenciar proativamente a instância spot antes do aviso de interrupção de dois minutos da instância spot. É possível decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção. Tornamos mais fácil para você usar esse sinal por meio do atributo de rebalanceamento de capacidade nos grupos do Auto Scaling e na Frota do EC2.

Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 interromper uma instância spot. Se a workload tiver “flexibilidade de tempo”, também é possível configurar as instâncias Spot para serem interrompidas ou para hibernarem, em vez de serem encerradas, quando forem interrompidas. O Amazon EC2 interrompe ou hiberna automaticamente suas instâncias spot durante a interrupção e retoma automaticamente as instâncias quando tivermos capacidade disponível.

Recomendamos que você crie uma regra no Amazon EventBridge que capture as recomendações de rebalanceamento e os avisos de interrupção e acione um ponto de verificação para o andamento da workload ou lide tranquilamente com a interrupção. Para ter mais informações, consulte Monitorar os sinais de recomendação de rebalanceamento. Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte Aproveitar os avisos de interrupção de instância spot do Amazon EC2.

Para ter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2 e Interrupções de instâncias spot.

Ser flexível sobre tipos de instância e zonas de disponibilidade

Um grupo de capacidade spot é um conjunto de instâncias do EC2 não utilizadas, com o mesmo tipo de instância (por exemplo, `m5.large`) e a zona de disponibilidade (por exemplo, us-east-1a). É necessário ser flexível sobre quais tipos de instância solicita e em quais zonas de disponibilidade pode implantar a workload. Isso dá ao Spot uma chance melhor de encontrar e alocar a quantidade necessária de capacidade computacional. Por exemplo, não peça apenas `c5.large` se você está disposto a usar grandes das famílias c4, m5 e m4.

Dependendo de suas necessidades específicas, é possível avaliar para quais tipos de instância é possível ter flexibilidade para atender aos requisitos de computação. Se uma workload puder ser dimensionada verticalmente, é necessário incluir tipos de instância maiores (mais vCPUs e memória) nas solicitações. Se você puder dimensionar somente horizontalmente, deverá incluir tipos de instância de geração mais antiga, pois eles têm menos demanda de clientes sob demanda.

Uma boa regra geral é ser flexível para pelo menos 10 tipos de instância para cada workload. Além disso, verifique se todas as zonas de disponibilidade estão configuradas para uso na VPC e selecionadas para a workload.

Usar grupos do Auto Scaling ou a Frota do EC2 para gerenciar a capacidade agregada

O spot permite que você pense em termos de capacidade agregada, ou seja, em unidades que incluem vCPUs, memória, armazenamento ou throughput de rede, em vez de pensar em termos de instâncias individuais. Os grupos do Auto Scaling e a Frota do EC2 permitem iniciar e manter uma capacidade pretendida, e solicitar recursos para substituir automaticamente os que forem interrompidos ou encerrados manualmente. Ao configurar um grupo do Auto Scaling ou uma Frota do EC2, você só precisa especificar os tipos de instância e a capacidade pretendida de acordo com as necessidades da aplicação. Para obter mais informações, consulte Grupos de Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling e Criar uma Frota do EC2. neste guia do usuário.

Usar a estratégia de alocação otimizada para preço e capacidade

As estratégias de alocação nos grupos de Auto Scaling ajudam a provisionar a capacidade prevista sem a necessidade de procurar manualmente os grupos de capacidade spot com capacidade adicional. Recomendamos o uso da estratégia `price-capacity-optimized`, pois ela provisiona automaticamente as instâncias dos grupos de capacidade spot mais disponíveis que também têm o menor preço possível. Também é possível aproveitar a estratégia de alocação de `price-capacity-optimized` na Frota do EC2. Como a capacidade da instância spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam recuperadas. Para obter mais informações sobre estratégias de alocação, consulte Instâncias spot no Guia do usuário do Amazon EC2 Auto Scaling e Quando as workloads têm um alto custo de interrupção neste guia do usuário.

Use serviços integrados da AWS para gerenciar as instâncias spot

Outros serviços da AWS integram-se ao Spot para reduzir os custos gerais de computação sem a necessidade de gerenciar instâncias ou frotas individuais. Recomendamos considerar as seguintes soluções para as workloads aplicáveis: Amazon EMR, Amazon Elastic Container Service, AWS Batch, Amazon Elastic Kubernetes Service, Amazon SageMaker, AWS Elastic Beanstalk e Amazon

GameLift. Para saber mais sobre as melhores práticas do Spot com esses serviços, consulte o Site de workshops de Instâncias spot do Amazon EC2.

Qual é o melhor método de solicitação spot para usar?

Use a tabela a seguir para determinar qual API usar ao solicitar instâncias spot.

API	Quando usar?	Caso de uso	Devo usar esta API?
CreateAutoScalingGroup	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja automatizar o gerenciamento do ciclo de vida por meio de uma API configurável.	Crie um grupo do Auto Scaling que gerencie o ciclo de vida de suas instâncias enquanto mantém o número desejado de instâncias. Compatível com dimensionamento horizontal da escala (adição de mais instâncias) entre os limites mínimo e máximo especificados.	Sim
CreateFleet	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja gerenciar por conta própria o ciclo de vida da instância. •	Crie uma frota de instâncias sob demanda e instâncias spot em uma única solicitação, com várias especificações de execução, que variam de acordo com o tipo de instância, a AMI, a zona de disponibilidade ou a sub-rede. Por padrão, a	Sim. No modo `instant` se não houver necessidade de autoescalabilidade

API	Quando usar?	Caso de uso	Devo usar esta API?
	Se não precisar de autoescalabilidade, recomendamos que use um tipo `instant` de frota.	estratégia de alocação de instância spot usa o `lowest-price` por unidade, mas é possível alterá-la para `price-capacity-optimized`, `capacity-optimized` ou `diversified`.	
RunInstances	• Você já está usando a API RunInstances para executar instâncias sob demanda e simplesmente deseja mudar para a execução de instâncias spot alterando um só parâmetro. • Você não precisa de várias instâncias com diferentes tipos de instância.	Execute um número especificado de instâncias usando uma AMI e um tipo de instância.	Não. Porque RunInstances não permite tipos de instâncias mistas em uma única solicitação

API	Quando usar?	Caso de uso	Devo usar esta API?
RequestSpotFleet	• Desencorajamos fortemente o uso da API RequestSpotFleet por ser uma API herdada e sem investimento planejado. • Se quiser gerenciar o ciclo de vida da sua instância, use a API CreateFleet. • Se não quiser gerenciar o ciclo de vida da sua instância, use a API CreateAutoScalingGroup.	NÃO USE. RequestSpotFleet é uma API herdada e sem investimento planejado.	Não
RequestSpotInstances	• Desencorajamos fortemente o uso da API RequestSpotInstances por ser uma API herdada e sem investimento planejado.	NÃO USE. RequestSpotInstances é uma API herdada e sem investimento planejado.	Não

Como as Instâncias spot funcionam

Para iniciar uma instância Spot, você cria uma solicitação de instância spot ou o Amazon EC2 cria uma solicitação de instância spot em seu nome. A instância spot é iniciada quando a solicitação de instância spot é atendida.

É possível iniciar uma instância spot usando vários serviços diferentes. Para obter mais informações, consulte Conceitos básicos das instâncias spot do Amazon EC2. Neste guia do usuário, descrevemos as seguintes maneiras de executar uma instância spot usando o EC2:

- É possível criar uma solicitação de instância spot usando o assistente de execução de instância no console do Amazon EC2 ou no comando run-instances da AWS CLI. Para ter mais informações, consulte Criar uma solicitação de instância spot.
- É possível criar uma EC2 Fleet e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na EC2 Fleet. Para ter mais informações, consulte Criar uma Frota do EC2..
- É possível criar uma frota spot e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na solicitação de frota spot. Para ter mais informações, consulte Criar uma solicitação de frota spot.

Sua instância spot será iniciada se houver capacidade disponível.

Sua instância spot será executada até que você a interrompa ou a encerre, ou até que o Amazon EC2 a interrompa (processo conhecido como interrupção da instância spot).

Quando você usa instâncias spot, deve estar preparado para interrupções. O Amazon EC2 poderá interromper a sua instância spot quando a demanda por instâncias spot aumentar ou quando o suprimento de instâncias spot diminuir. Quando o Amazon EC2 interrompe uma instância spot, ele fornece um aviso de interrupção de instância spot, enviando à instância um aviso de dois minutos antes que o Amazon EC2 a interrompa. Você não pode habilitar a proteção contra encerramento para Instâncias spot. Para obter mais informações, consulte Interrupções de instâncias spot.

É possível parar, iniciar, reiniciar ou encerrar uma instância baseada no Amazon EBS. O serviço spot pode parar, encerrar ou hibernar uma instância spot quando a interrompe.

Tópicos

- Executar Instâncias spot em um grupo de execução
- Executar Instâncias spot em um grupo de zonas de disponibilidade

- Executar Instâncias spot em uma VPC

Executar Instâncias spot em um grupo de execução

Especifique um grupo de execução na solicitação de instância spot para instruir o Amazon EC2 a executar um conjunto de instâncias spot somente se ele puder executar todas elas. Além disso, se o serviço spot precisar encerrar uma das instâncias em um grupo de execução, ele deverá encerrar todas elas. Contudo, se você encerrar uma ou mais instâncias em um grupo de execução, o Amazon EC2 não encerrará as instâncias restantes no grupo de execução.

Embora essa opção possa ser útil, adicionar essa restrição pode diminuir as chances de a sua solicitação de instância spot ser atendida e aumenta as chances de encerramento das instâncias spot. Por exemplo, seu grupo de execução inclui instâncias em várias zonas de disponibilidade. Se a capacidade em uma dessas zonas de disponibilidade diminuir e não estiver mais disponível, o Amazon EC2 encerrará todas as instâncias do grupo de execução.

Se você criar outra solicitação de instância spot bem-sucedida que especifique o mesmo grupo de execução (existente) de uma solicitação bem-sucedida anterior, as novas instâncias serão adicionadas ao grupo de execução. Subsequentemente, se uma instância nesse grupo de execução for encerrada, todas as instâncias no grupo de execução serão encerradas, o que inclui instâncias executadas pela primeira e a segunda solicitações.

Executar Instâncias spot em um grupo de zonas de disponibilidade

Especifique um grupo de zonas de disponibilidade na solicitação de instância spot para informar ao Amazon EC2 para iniciar um conjunto de instâncias spot na mesma zona de disponibilidade. O Amazon EC2 não precisa interromper todas as instâncias em um grupo de zonas de disponibilidade ao mesmo tempo. Se o Amazon EC2 precisar interromper uma das instâncias em um grupo de zonas de disponibilidade, as outras permanecerão em execução.

Embora essa opção possa ser útil, a adição dessa restrição pode reduzir as possibilidades de sua solicitação de instância spot ser atendida.

Se você especificar um grupo de zonas de disponibilidade, mas não especificar uma zona de disponibilidade na solicitação de instância spot, o resultado dependerá da rede especificada.

VPC padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada. Se você não especificar uma sub-rede, ele selecionará uma zona de disponibilidade e sua sub-rede padrão, mas não

necessariamente a zona de preço mais baixo. Se você excluir a sub-rede padrão de uma zona de disponibilidade, deverá especificar uma sub-rede diferente.

VPC não padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada.

Executar Instâncias spot em uma VPC

Especifique uma sub-rede para as Instâncias spot da mesma maneira que você especifica uma sub-rede para as Instâncias on-demand.

- [VPC padrão] Se você quiser que a instância spot seja executada em uma zona de disponibilidade de baixo preço, especifique a sub-rede correspondente na solicitação de instância spot. Se você não especificar uma sub-rede, o Amazon EC2 selecionará uma para você, e a zona de disponibilidade para essa sub-rede poderá não ter o menor preço spot.
- [VPC não padrão] Especifique a sub-rede da instância spot.

Histórico de definição de preço da instância spot

Os preços de instâncias spot são definidos pelo Amazon EC2 e ajustados gradualmente de acordo com tendências de longo prazo da oferta e da demanda de capacidade de instâncias spot.

Quando sua solicitação de spot for atendida, as instâncias spot serão iniciadas pelo preço spot atual, não excedendo o preço sob demanda. É possível visualizar o histórico de preços spot dos últimos 90 dias, filtrando por tipo de instância, sistema operacional e zona de disponibilidade.

Para visualizar os preços spot atuais

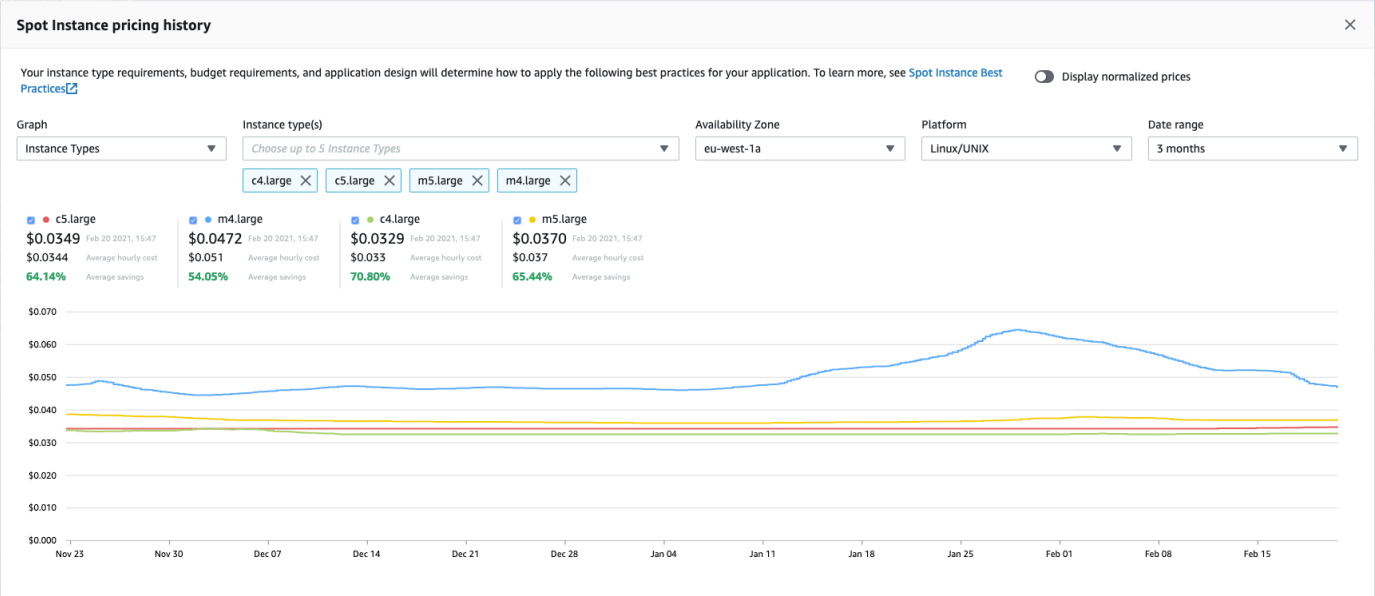
Para obter os preços de instâncias spot atuais, consulte a definição de preço de instâncias spot do Amazon EC2.

Para visualizar o histórico de preços das instâncias spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha Histórico de definição de preço.
4. Em Graph (Gráfico), escolha comparar o histórico de preços por Availability Zones (Zonas de disponibilidade) ou por Instances Types (Tipos de Instância).

- Se escolher Availability Zones (Zonas de disponibilidade), escolha Instance type (Tipo de instância), sistema operacional (Platform [Plataforma]) e Date range (Intervalo de datas) para os quais deseja exibir o histórico de preços.
- Se escolher Instance Types (Tipos de instância), escolha até cinco Instance type(s) (Tipos de instâncias), Availability Zone (Zona de disponibilidade), sistema operacional (Platform [Plataforma]) e Date range (Intervalo de datas) para os quais deseja exibir o histórico de preços.

A captura de tela a seguir mostra uma comparação de preços para diferentes tipos de instância.



5. Mova o ponteiro do mouse sobre o gráfico para exibir os preços em horas específicas no intervalo de datas selecionado. Os preços são exibidos nos blocos de informações acima do gráfico. O preço exibido na linha superior mostra o preço em uma data específica. O preço exibido na segunda linha mostra o preço médio durante o intervalo de datas selecionado.
6. Para exibir o preço por vCPU, ative a opção Display normalized prices (Exibir preços normalizados). Para exibir o preço do tipo de instância, desative Display normalized prices (Exibir preços normalizados).

Para visualizar o histórico de preços spot usando a linha de comando

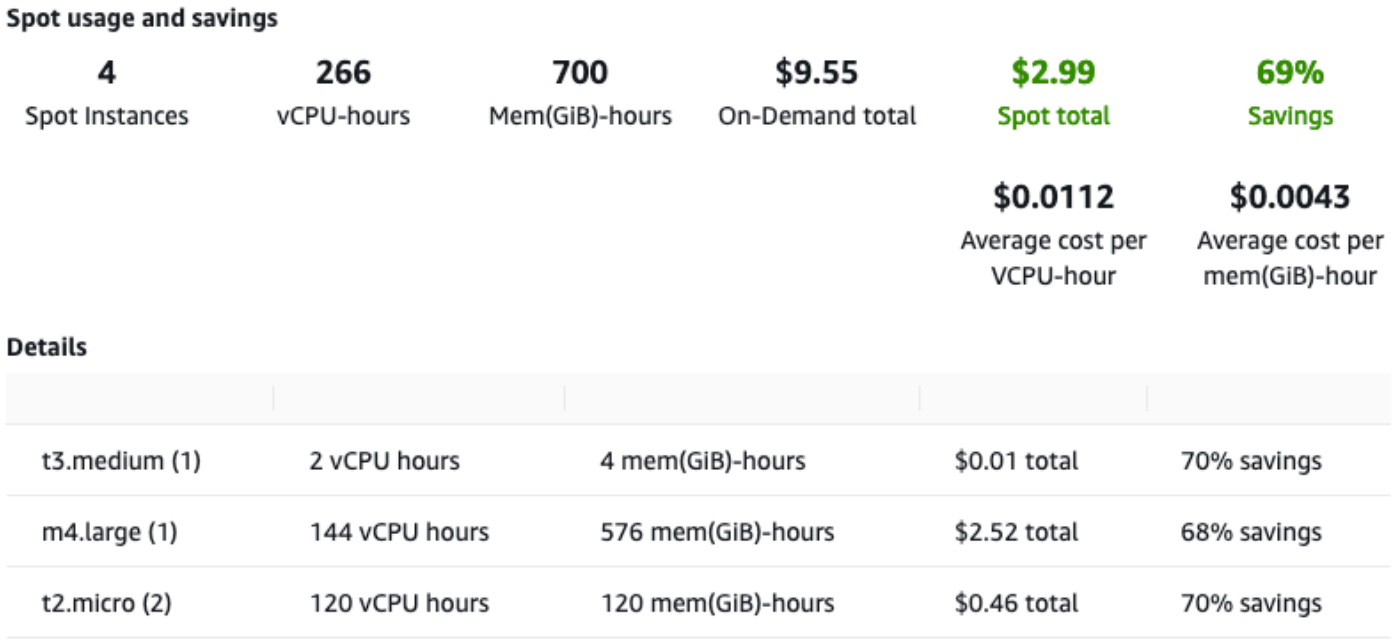
É possível usar um dos comandos a seguir. Para ter mais informações, consulte Acessar o Amazon EC2.

- describe-spot-price-history (AWS CLI)
- Get-EC2SpotPriceHistory (AWS Tools for Windows PowerShell)

Economia na compra das Instâncias spot

É possível visualizar as informações de uso e de economias das Instâncias spot em nível de frota ou de todas as Instâncias spot em execução. No nível por frota, as informações de uso e de economia incluem todas as instâncias executadas e encerradas pela frota. É possível visualizar essas informações da última hora ou dos últimos três dias.

A captura de tela a seguir da seção Savings (Economia) mostra as informações de uso e de economia spot de uma frota spot.



É possível visualizar as seguintes informações de uso e de economia:

- Spot Instances (Instâncias spot): o número de instâncias spot executadas e encerradas pela frota spot. Ao visualizar o resumo de economias, o número representa todas as Instâncias spot em execução.
- vCPU-hours (Horas de vCPU) – o número de horas de vCPU usadas entre todas as Instâncias spot no período selecionado.
- Mem(GiB)-hours (Horas de mem(GiB)) – o número de horas de GiB usadas entre todas as Instâncias spot no período selecionado.

- On-Demand total (Total sob demanda) – a quantidade total que você pagaria pelo período de tempo selecionado se tivesse executado essas instâncias como Instâncias on-demand.
- Spot total (Total de Spot) – a quantidade total a ser paga para o período selecionado.
- Savings (Economias) – a porcentagem economizada por não pagar o preço sob demanda.
- Average cost per vCPU-hour (Custo médio por hora de vCPU) – o custo médio por hora de uso das vCPUs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per vCPU-hour (Custo médio por hora de vCPU) = Spot total (Total de Spot) / vCPU-hours (Horas de vCPU).
- Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) – o custo médio por hora de uso de GiBs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) = Spot total (Total de Spot) / mem(GiB)-hours (Horas de mem(GiB)).
- Tabela Details (Detalhes): os diferentes tipos de instância (o número de instâncias por tipo de instância está entre parênteses) que compõem a frota spot. Ao visualizar o resumo de economias, isso representa todas as Instâncias spot em execução.

As informações de economias podem ser visualizadas apenas usando o console do Amazon EC2.

Para visualizar informações sobre as vantagens econômicas de uma frota spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione o ID de uma frota spot e role até seção Savings (Economia).

   Se preferir, marque a caixa de seleção ao lado do ID de solicitação de frota spot e escolha a guia seção Savings (Economia).
4. Por padrão, a página exibe as informações de uso e de economia dos últimos três dias. É possível escolher a last hour (última hora) ou os last three days (últimos três dias). Para Frotas spot que foram executadas há menos de uma hora, a página mostra a economia estimada para a hora.

Para visualizar informações sobre as vantagens econômicas de todas as Instâncias spot em execução usando o console

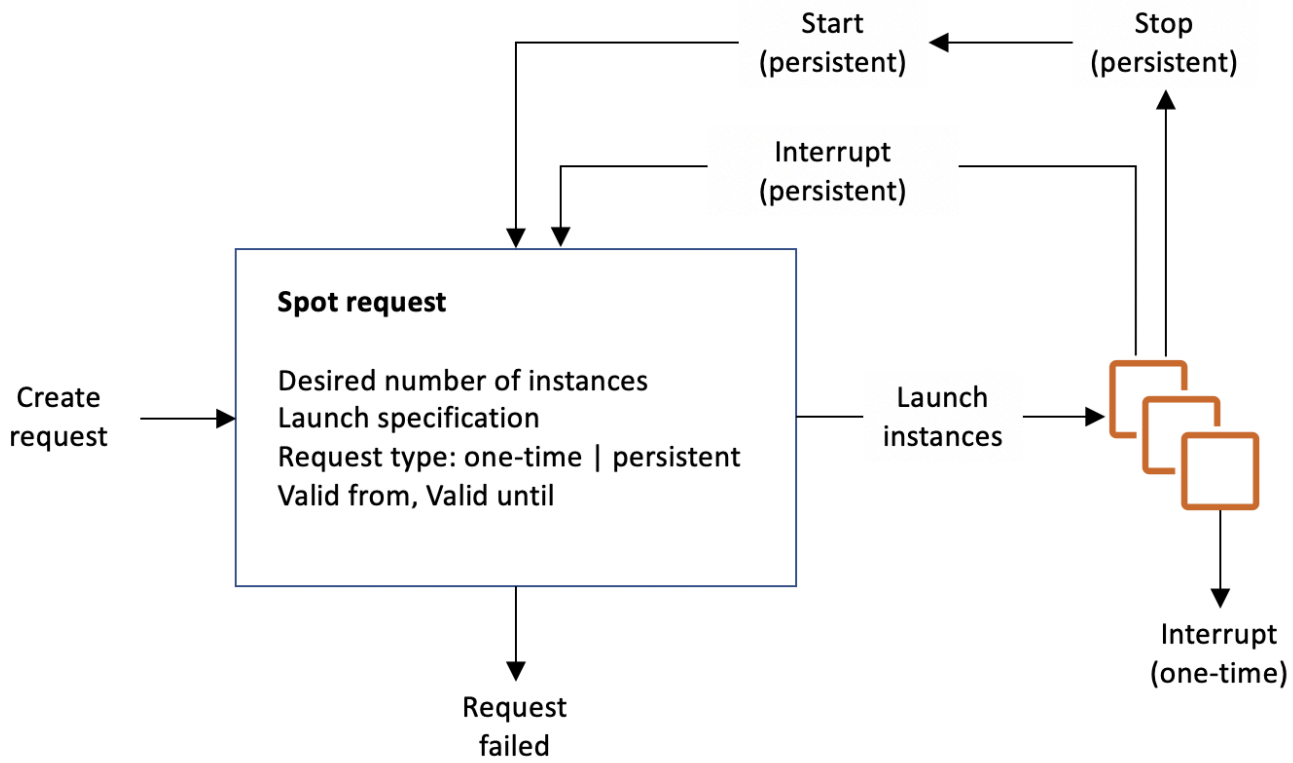
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Solicitações spot.
3. Escolha Savings Summary (Resumo das economias).

Trabalhar com Instâncias spot

Para usar instâncias spot, crie uma solicitação de instância spot que inclua o número de instâncias desejado, o tipo de instância e a zona de disponibilidade. Se houver capacidade disponível, o Amazon EC2 atenderá à solicitação imediatamente. Caso contrário, o Amazon EC2 esperará até a sua solicitação puder ser atendida ou até você cancelar a solicitação.

A ilustração a seguir mostra como as solicitações de instância spot funcionam. Observe que o tipo de solicitação (única ou persistente) determina se a solicitação será exibida novamente quando o Amazon EC2 ou você interromper uma instância spot. Se a requisição for persistente, ela será aberta novamente depois que a instância spot for interrompida. Se a solicitação for persistente e você interromper a instância spot, a solicitação será exibida somente depois que você iniciar a instância spot.



Conteúdo

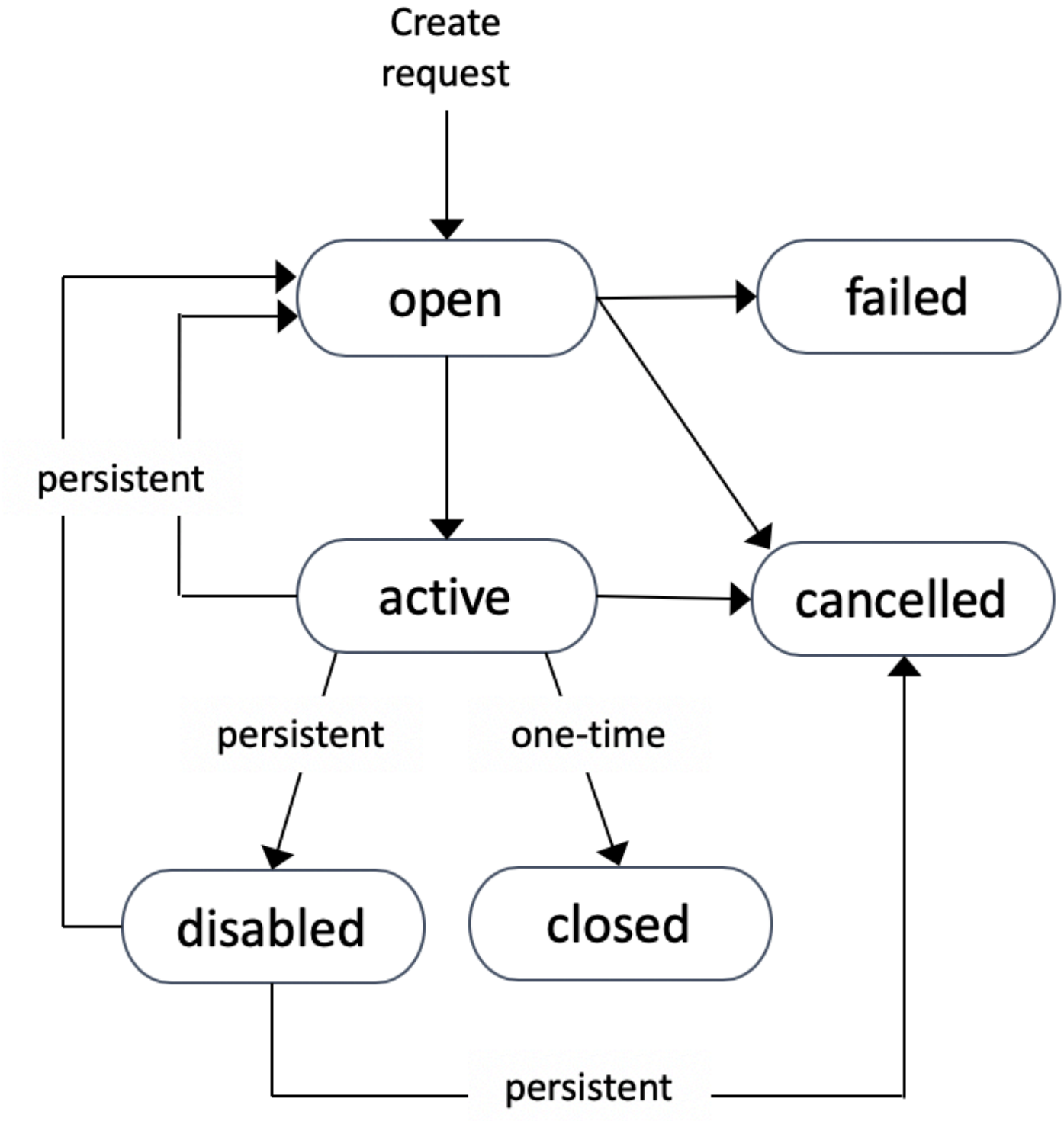
- Estados da solicitação de instância spot
- Especificar uma locação para suas Instâncias spot
- Função vinculada ao serviço para solicitações de instâncias spot
- Criar uma solicitação de instância spot
- Encontrar as instâncias spot
- Marcar solicitações de instância spot
- Cancelar uma solicitação de instância spot
- Interromper uma instância spot
- Iniciar uma instância spot
- Encerrar uma instância spot
- Exemplo de especificações de execução de solicitações de instância spot

Estados da solicitação de instância spot

Uma solicitação de instância spot pode estar em um dos seguintes estados:

- `open` – A solicitação está esperando para ser atendida.
- `active` – A solicitação foi atendida e tem uma instância spot associada.
- `failed` – A solicitação tem um ou mais parâmetros inválidos.
- `closed` – A instância spot foi interrompida ou encerrada.
- `disabled` – Você interrompeu a instância spot.
- `cancelled` – Você cancelou a solicitação ou ela expirou.

A ilustração a seguir representa as transições entre os estados da solicitação. Observe que as transições dependem do tipo de solicitação (única ou persistente).



Uma solicitação de instância spot única permanece ativa até o Amazon EC2 executar a instância spot, a solicitação expirar ou você cancelar a solicitação. Se não houver capacidade disponível, sua instância spot será encerrada e a solicitação de instância spot será fechada.

Uma solicitação de instância spot persistente permanecerá ativa até expirar ou até que você a cancele, mesmo se a solicitação tiver sido atendida. Se não houver capacidade disponível, sua instância spot será interrompida. Depois que a instância é interrompida, quando a capacidade se torna disponível novamente, a instância spot será iniciada se estiver parada ou retomada se estiver em hibernação. É possível interromper uma instância spot e iniciá-la novamente quando há capacidade disponível. Se a instância spot for encerrada (independentemente da instância spot estar interrompida ou estar em execução), a solicitação de instância spot será aberta novamente e o Amazon EC2 executará uma nova instância spot. Para obter mais informações, consulte Interromper uma instância spot, Iniciar uma instância spot e Encerrar uma instância spot.

É possível acompanhar o status das solicitações de instância spot, bem como o status das instâncias spot executadas, pelo status. Para ter mais informações, consulte Status da solicitação spot.

Especificar uma locação para suas Instâncias spot

É possível executar uma instância spot no hardware de ocupante único. As instâncias spot dedicadas são fisicamente isoladas de instâncias que pertencem a outras contas da AWS. Para obter mais informações, consulte Dedicated Instances e a página do produto Instâncias dedicadas do Amazon EC2.

Para executar uma instância spot dedicada, execute um dos seguintes procedimentos:

- Especifique um locação `dedicated` ao criar a solicitação de instância spot. Para ter mais informações, consulte Criar uma solicitação de instância spot.
- Solicite uma solicitação spot em uma VPC com uma locação de instância `dedicated`. Para ter mais informações, consulte Criar uma VPC com uma locação de instância dedicada. Não é possível solicitar uma instância spot com um locação `default` se você solicitá-la em uma VPC com uma locação de instância `dedicated`.

Todas as famílias de instâncias são compatíveis com Instâncias spot dedicadas, exceto instâncias T. Para cada família de instâncias compatíveis, apenas o maior tamanho de instância ou tamanho de metal é compatível com Instâncias spot dedicadas.

Função vinculada ao serviço para solicitações de instâncias spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões necessárias para chamar outros produtos da AWS em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculado diretamente a um serviço da AWS. As funções vinculadas a serviços

oferecem uma maneira segura de delegar permissões a serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulteUso de funções vinculadas ao serviço no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço denominada AWSServiceRoleForEC2Spot para executar e gerenciar Instâncias spot em seu nome.

Permissões concedidas pelo AWSServiceRoleForEC2Spot

O Amazon EC2 usa AWSServiceRoleForEC2Spot para concluir as ações a seguir:

- `ec2:DescribeInstances` – Descrever instâncias spot
- `ec2:StopInstances` – Interromper instâncias spot
- `ec2:StartInstances` – Iniciar instâncias spot

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2Spot vinculada ao serviço na primeira vez que você solicita uma instância spot usando o console.

Se você tinha uma solicitação de instância spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2Spot em sua conta da AWS. Para obter mais informações, consulte Uma nova função apareceu na minha conta no Guia do usuário do IAM.

Se você usar a AWS CLI ou uma API para solicitar uma instância spot, deverá assegurar que essa função existe.

Para criar AWSServiceRoleForEC2Spot usando o console

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Roles.
3. Selecione Create role.
4. Na página Select type of trusted entity (Selecionar tipo de entidade confiável), escolha EC2, EC2 - Spot Instances (EC2 - instâncias spot), Next: Permissions (Próximo: permissões).
5. Na próxima página, escolha Next:Review (Próximo: revisar).

6. Na página Review (Revisar), selecione Create role (Criar função).

Para criar AWSServiceRoleForEC2Spot usando a AWS CLI

Use o comando create-service-linked-role da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Se você não precisar mais usar Instâncias spot, é recomendável excluir a função AWSServiceRoleForEC2Spot. Depois que essa função for excluída da sua conta, o Amazon EC2 criará a função novamente se você solicitar Instâncias spot.

Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado para suas instâncias spot e usar uma chave gerenciada pelo cliente para criptografia, deverá conceder à função AWSServiceRoleForEC2Spot permissão para usar a chave gerenciada pelo cliente de forma que o Amazon EC2 consiga executar instâncias spot em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Uso de concessões e Uso de políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder as permissões para a função AWSServiceRoleForEC2Spot para usar a chave gerenciada pelo cliente

- Use o comando create-grant para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é especificada pelo parâmetro `key-id` e o ARN da chave gerenciada pelo cliente. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço AWSServiceRoleForEC2Spot.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Criar uma solicitação de instância spot

Você pode usar o assistente de execução de instância no console do Amazon EC2 ou no comando da AWS CLI run-instances para solicitar uma instância spot da mesma forma que você pode executar uma instância sob demanda. Este método é recomendado apenas pelos seguintes motivos:

- Você já está usando o assistente de execução de instância ou o comando run-instances para executar instâncias sob demanda e quer mudar para a execução de instâncias spot alterando um único parâmetro.
- Você não precisa de várias instâncias com diferentes tipos de instância.

Esse método geralmente não é recomendado para executar instâncias spot porque você não pode especificar vários tipos de instância e não é possível executar instâncias spot e instâncias sob demanda na mesma solicitação. Para os métodos preferidos de execução de instâncias spot, que incluem a execução de uma frota que inclui instâncias spot e instâncias sob demanda com vários tipos de instância, consulte Qual é o melhor método de solicitação spot para usar?

Se você solicitar várias instâncias spot ao mesmo tempo, o Amazon EC2 criará solicitações de instância spot separadas para que você possa acompanhar o status de cada uma separadamente. Para obter mais informações sobre como monitorar solicitações de instâncias spot, consulte Status da solicitação spot.

New console

Para criar uma solicitação de instância spot usando o assistente de execução de instâncias

As etapas de 1 a 9 são as mesmas que você usaria para executar uma instância sob demanda. Na Etapa 10, você configura a solicitação da instância spot.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma região.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).

4. (Opcional) Em Name and tags (Nome e etiquetas), é possível nomear a instância e marcar a solicitação de instância spot, a instância, os volumes e os gráficos elásticos. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2.

   a. Em Name (Nome), insira um nome descritivo para a instância.

      O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar. Se você não especificar um nome, a instância poderá ser identificada por seu ID, que é gerado automaticamente quando você inicia a instância.

   b. Para marcar a solicitação de instância spot, a instância, os volumes e os elementos gráficos elásticos, escolha Add additional tags (Adicionar outras etiquetas). Escolha Add tag (Adicionar tag), insira uma chave e um valor, e selecione o tipo de recurso a aplicar a tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

5. Em Application and OS Images (Amazon Machine Image), (Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha o sistema operacional da instância e selecione uma AMI. Para ter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).

6. Em Instance type (Tipo de instância), selecione o tipo de instância que atende aos requisitos para a configuração do hardware e o tamanho da instância. Para ter mais informações, consulte Tipo de instância.

7. Em Key pair (login) (Par de chaves: login) escolha um par de chaves existente ou selecione Create new key pair (Criar um novo par de chaves) para criar um novo. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

   > **Important**
   >
   > Se você escolher a opção Proceed without key pair (Not recommended) (Prosseguir sem par de chaves, não recomendado), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir que os usuários façam login de outro modo.

8. Em Network settings (Configurações de rede), use as configurações padrão ou escolha Edit (Editar) para definir as configurações de rede, conforme necessário.

   Os grupos de segurança fazem parte das configurações de rede e definem regras de firewall para a instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância.

Para ter mais informações, consulte Configurações de rede.

9. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Configure storage (Configurar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Para ter mais informações, consulte Configurar armazenamento.
10. Em Advanced details (Detalhes avançados), configure a solicitação de instância spot da seguinte maneira:

    a. Em Purchasing option (Opção de compra), selecione Request Spot Instances (Solicitar instâncias spot).

    b. Você pode manter a configuração padrão para a solicitação de instância spot ou escolher Customize (Personalizar), à direita, para especificar configurações personalizadas para a solicitação da instância spot.

    Ao escolher a opção Customize (Personalizar), os campos a seguir serão exibidos.

    i. Preço máximo: e possível solicitar instâncias spot pelo preço spot, limitado ao preço sob demanda ou especificar o valor máximo que você está disposto a pagar.

> **Warning**
>
> Se você especificar um preço máximo, as instâncias serão interrompidas com mais frequência do que se você escolher No maximum price (Sem preço máximo).

- Sem preço máximo: a instância spot será executada pelo preço spot atual. O preço nunca excederá o preço sob demanda. (Recomendado)
- Defina seu preço máximo (por instância/hora): você pode especificar o valor máximo que estiver disposto a pagar.
  - Se você especificar um preço máximo inferior ao preço spot atual, a instância spot não será executada.
  - Se você especificar um preço máximo superior ao preço spot atual, a instância spot será executada e cobrada de acordo com o preço spot atual. Depois que a instância spot estiver em execução, se o preço spot subir acima do preço máximo, o Amazon EC2 interromperá a instância spot.

- Independentemente do preço máximo especificado, você sempre será cobrado o preço Spot atual.

Para analisar as tendências de preços spot, consulte Histórico de definição de preço da instância spot.

ii. Tipos de solicitação: o tipo de solicitação de instância spot escolhido determina o que acontece se a instância spot for interrompida.

- Única: o Amazon EC2 faz uma solicitação única para a instância spot. Se a instância spot for interrompida, a solicitação não será reenviada.
- Solicitação persistente: o Amazon EC2 faz uma solicitação persistente para a instância spot. Se a instância spot for interrompida, a solicitação será reenviada para reabastecer a instância spot interrompida.

Se você não especificar um valor, o padrão é uma solicitação única.

iii. Valid to (Válido para): a data de expiração de uma solicitação de instância spot persistente.

Esse campo não é compatível com solicitações únicas. Uma solicitação única permanece ativa até que todas as instâncias da solicitação expirem ou você cancele a solicitação.

- Nenhuma data de expiração da solicitação: a solicitação permanecerá ativa até você cancelá-la.
- Defina a data de validade da solicitação: a solicitação persistente permanece ativa até a data especificada ou até que você a cancele.

iv. Comportamento de interrupção: o comportamento escolhido determina o que acontece quando uma instância spot é interrompida.

- Para solicitações persistentes, os valores válidos são Stop (Parar) e Hibernate (Hibernar). Quando uma instância é interrompida, cobranças pelo armazenamento em volume do EBS são aplicadas.

> **Note**
>
> As instâncias spot agora usam a mesma funcionalidade de hibernação que as instâncias sob demanda. Para habilitar a hibernação, você pode

escolher Hibernar aqui ou Habilitar no campo Comportamento de parar - hibernar, que aparece mais abaixo no assistente de inicialização de instância. Para conhecer os pré-requisitos de hibernação, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.

- Para as solicitações únicas, somente Terminate (Encerrar) é válido.

Se você não especificar um valor, o padrão é Terminate (Encerrar) que não é válido para uma solicitação de instância spot persistente. Se você mantiver o padrão e tentar executar uma solicitação de instância spot persistente, receberá um erro.

Para ter mais informações, consulte Comportamento das interrupções de instâncias spot.

11. No painel Summary (Resumo), para Number of instances (Número de instâncias), insira o número de instâncias a serem executadas.

> **Note**
>
> O Amazon EC2 cria uma solicitação distinta para cada instância spot.

12. No painel Summary (Resumo), revise os detalhes da instância e faça as alterações necessárias. Depois de enviar sua solicitação de instância spot, não é possível alterar os parâmetros da solicitação. É possível navegar diretamente para uma seção no assistente de execução de instância, escolhendo seu link no painel Summary (Resumo). Para ter mais informações, consulte Resumo.
13. Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Old console

Para criar uma solicitação de instância spot usando o assistente de execução de instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma região.
3. No painel do console do Amazon EC2, selecione Launch Instance (Executar instância).

4. Na página Escolher imagem de máquina da Amazon (AMI), escolha uma AMI. Para ter mais informações, consulte Etapa 1: Escolher uma imagem de máquina da Amazon (AMI).
5. Na página Choose an Instance Type (Escolher um tipo de instância), selecione a configuração de hardware e o tamanho da instância a ser executada e Next: Configure Instance Details (Próximo: configurar detalhes da instância). Para ter mais informações, consulte Etapa 2: escolher um tipo de instância.
6. Na página Configure Instance Details (Configurar os detalhes da instância) configure a solicitação de instância spot da seguinte maneira:

   - Number of instances (Número de instâncias): Digite o número de instâncias para executar.

     > **Note**
     >
     > O Amazon EC2 cria uma solicitação distinta para cada instância spot.

   - (Opcional) Para ajudar a assegurar que você mantenha o número de instâncias para lidar com a demanda da aplicação, escolha Launch into Auto Scaling Group (Executar no grupo de Auto Scaling) para criar uma configuração de execução e um grupo de Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.
   - Purchasing option (Opção de compra): escolha Request Spot instances (Solicitar instâncias spot) para executar uma instância Spot. Ao escolher essa opção, os campos a seguir são exibidos.
   - Preço atual: o preço spot atual em cada zona de disponibilidade é exibido para o tipo de instância selecionada.
   - (Opcional) Preço máximo: é possível deixar o campo vazio ou especificar o valor máximo que está disposto a pagar.

     > **Warning**
     >
     > Se você especificar um preço máximo, suas instâncias serão interrompidas com mais frequência do que se você deixar esse campo vazio.

     - Se você especificar um preço máximo inferior ao preço spot, a instância spot não será iniciada.

- Se você especificar um preço máximo superior ao preço spot atual, a instância spot será executada e cobrada de acordo com o preço spot atual. Depois que a instância spot estiver em execução, se o preço spot subir acima do preço máximo, o Amazon EC2 interromperá a instância spot.
- Independentemente do preço máximo especificado, você sempre será cobrado o preço Spot atual.
- Se você deixar o campo vazio, pagará o preço spot atual.

- Persistent request (Solicitação persistente): escolha Solicitação persistente para reenviar a solicitação de instância spot se a instância spot for interrompida.
- Interruption behavior (Comportamento de interrupção): por padrão, o serviço spot encerra uma instância spot quando ela é interrompida. Se escolher Solicitação persistente, será possível especificar que o serviço spot interrompa ou hiberne a instância spot quando ela for interrompida. Para ter mais informações, consulte Comportamento das interrupções de instâncias spot.
- (Opcional) Request valid to (Solicitação válida até): escolha Edit (Editar) para especificar a expiração da solicitação de instância spot.

Para obter mais informações sobre como configurar sua instância spot, consulte Etapa 3: configurar detalhes da instância.

7. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Add Storage (Adicionar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Para obter mais informações, consulte Etapa 4: adicionar armazenamento.
8. Na página Add Tags (Adicionar tags), especifique as tags fornecendo combinações de chave e valor. Para obter mais informações, consulte Etapa 5: Adicionar tags.
9. Na página Configurar grupo de segurança, use um grupo de segurança para definir regras do firewall para sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. (Para mais informações sobre grupos de segurança, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.) Selecione ou crie um grupo de segurança e escolha Revisar e executar. Para ter mais informações, consulte Etapa 6: configurar o grupo de segurança.
10. Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da sua instância e faça qualquer alteração necessária selecionando o link Edit (Editar)

apropriado. Quando estiver pronto, escolha Launch (Executar). Para ter mais informações, consulte Etapa 7: Revisar a execução da instância e selecionar o par de chaves.

11. Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), será possível escolher um par de chaves existente ou poderá criar um novo. Por exemplo, Escolha um par de chaves existente e selecione o par de chaves que você criou para a configuração. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

    > **Important**
    >
    > Se você escolher a opção Proceed without key pair (Continuar sem par de chaves), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir aos usuários uma maneira efetuar login.

12. Para executar uma instância, selecione a caixa de confirmação e escolha Launch Instances (Executar instâncias).

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

AWS CLI

Para criar uma solicitação de instância spot usando run-instances

Use o comando run-instances e especifique as opções da instância spot no parâmetro `--instance-market-options`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

Veja a seguir a estrutura de dados a ser especificada no arquivo JSON `--instance-market-options`. Também é possível especificar `ValidUntil` e `InstanceInterruptionBehavior`. Se você não especificar um campo na estrutura de dados, será usado o valor padrão.

O exemplo a seguir cria uma solicitação `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Para criar uma solicitação de instância spot usando request-spot-instances

> **Note**
>
> Não recomendamos o uso do comando request-spot-instances por ser uma API herdada e sem investimento planejado. Para obter mais informações, consulte Qual é o melhor método de solicitação spot para usar?

Use o comando request-spot-instances para criar uma solicitação única:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Use o comando request-spot-instances para criar uma requisição persistente:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Para que os arquivos de especificação de execução de exemplo sejam usados com esses comandos, consulte Exemplo de especificações de execução de solicitações de instância spot. Se você baixar um arquivo de especificação de execução no console de solicitações de spot, use o comando request-spot-fleet (o console de solicitações spot especifica uma solicitação de instância spot usando uma frota spot).

Encontrar as instâncias spot

O Amazon EC2 inicia uma instância spot quando há capacidade disponível. A instância spot será executada até ser interrompida ou até você a encerrar.

Uma instância spot aparece na página Instâncias no console junto com as instâncias sob demanda. Use o procedimento a seguir para encontrar as instâncias spot.

Console

Para registrar as instâncias spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Para encontrar todas as instâncias spot, no painel de pesquisa, escolha Ciclo de vida da instância = spot.
4. Para confirmar que uma instância é uma instância spot, selecione a instância, escolha a guia Detalhes e verifique o valor de Ciclo de vida. O valor de uma instância spot é `spot` e o valor de uma instância sob demanda é `normal`.

AWS CLI

Para encontrar as instâncias spot usando a AWS CLI

Use o comando describe-instante com a opção `--filters`.

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

Para determinar se uma instância é uma instância spot

Use o comando describe-instances, usando a opção `--query` para verificar o valor do ciclo de vida.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Se a saída for `spot`, a instância será uma instância spot. Se não houver saída, a instância será uma instância sob demanda.

Use o procedimento a seguir para encontrar as instâncias spot iniciadas por uma solicitação específica de instância spot ou frota spot.

Console

Para encontrar as instâncias spot para uma solicitação usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot. A lista contém tanto as solicitações de instância spot quanto as solicitações de frota spot.
3. Se uma solicitação de instância spot for atendida, Capacidade será o ID da instância spot. Em uma frota spot, a Capacity (Capacidade) indica quanto da capacidade solicitada foi atendida. Para visualizar os IDs das instâncias em uma frota spot, escolha a seta de expansão ou selecione a frota e escolha Instances (Instâncias).
4. Em uma frota spot, Capacidade indica quanto da capacidade solicitada foi fornecida. Para visualizar os IDs das instâncias em uma frota spot, escolha o ID da frota para abrir sua página de detalhes e localize o painel Instâncias.

AWS CLI

Para encontrar as instâncias spot para uma solicitação usando a AWS CLI

Use o comando describe-spot-instance-requests com a opção `--query`.

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

A seguir está um exemplo de saída:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
```

```
    }
]
```

Marcar solicitações de instância spot

Para categorizar e gerenciar as solicitações de instância spot, é possível marcá-las com metadados personalizados. É possível atribuir uma tag a uma solicitação de instância spot ao criá-la ou posteriormente. É possível atribuir tags usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Quando você marca uma solicitação de instância spot, as instâncias e os volumes executados pela solicitação de instância spot não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela solicitação de instância spot. É possível atribuir volumes e uma tag a uma instância spot durante a execução ou posteriormente.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Conteúdos

- Pré-requisitos
- Marcar uma nova solicitação de instância spot
- Marcar uma solicitação de instância spot existente
- Exibir tags de solicitação de instância spot

Pré-requisitos

Conceda ao usuário permissão para marcar recursos. Para obter mais informações sobre políticas do IAM e políticas de exemplo, consulte Exemplo: marcar recursos.

A política do IAM criada é determinada pelo método usado para criação de uma solicitação de instância spot.

- Se você usar o assistente de execução de instâncias ou `run-instances` para solicitar uma Instâncias spot, consulte To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Se você utiliza o comando `request-spot-instances` para solicitar instâncias spot, consulte To grant a user the permission to tag resources when using request-spot-instances.

Para conceder a um usuário do IAM permissão para marcar recursos ao usar o assistente de inicialização ou run-instances

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RunInstances`. Essa ação concede ao usuário permissão para iniciar uma instância.
- Em `Resource`, especifique `spot-instances-request`. Essa ação permite que os usuários criem solicitações de instância spot, que solicitam instâncias spot.
- A ação `ec2:CreateTags`. Essa ação concede ao usuário permissão para criar tags.
- Em `Resource`, especifique `*`. Isso permite que os usuários marquem todos os recursos criados durante a execução da instância.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Quando você usa a ação RunInstances para criar solicitações de instância spot e marcar as solicitações de instância spot ao criá-las, deve estar ciente de que o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances segundo a política do IAM, como se segue:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use RunInstances para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada terá êxito.
- Caso use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, você deverá incluir o recurso `spot-instances-request` na instrução de permissão RunInstances, caso contrário, a chamada falhará.
- Caso você use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou inclua um curinga * na instrução de permissão CreateTags, caso contrário, a chamada falhará.

Por exemplo, políticas do IAM, incluindo políticas que não são compatíveis com solicitações de instância spot, consulte Trabalhar com Instâncias spot.

Para conceder a um usuário permissão para marcar recursos ao usar request-spot-instances

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RequestSpotInstances`. Isso concede ao usuário permissão para criar uma solicitação de instância spot.
- A ação `ec2:CreateTags`. Essa ação concede ao usuário permissão para criar tags.
- Em `Resource`, especifique `spot-instances-request`. Isso permite que os usuários marquem somente a solicitação de instância spot.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

Marcar uma nova solicitação de instância spot

Console

Para marcar uma nova solicitação de instância spot usando o console

1. Siga o procedimento do Criar uma solicitação de instância spot.
2. Para adicionar uma tag, na página Adicionar tags, escolha Adicionar tag e insira a chave e o valor da tag. Escolha Adicionar outra tag para cada tag adicional.

   Para cada tag, é possível marcar a solicitação de instância spot, as instâncias spot e os volumes com a mesma tag. Para marcar os três, verifique se as opções Instances (Instâncias), Volumes e Spot Instance Requests (Solicitações de instâncias spot) estão selecionadas. Para marcar apenas um ou dois, verifique se os recursos que deseja marcar estão selecionados e os outros recursos estão limpos.
3. Preencha os campos obrigatórios para criar uma solicitação de instância spot e escolha Launch (Executar). Para ter mais informações, consulte Criar uma solicitação de instância spot.

AWS CLI

Para marcar uma nova solicitação de instância spot usando a AWS CLI

Para marcar uma solicitação de instância spot ao criá-la, defina-a da seguinte maneira:

- Especifique as tags para a solicitação de instância spot usando o parâmetro `--tag-specification`.

- Para `ResourceType`, especifique `spot-instances-request`. Se você especificar outro valor, ocorrerá falha na solicitação de instância spot.
- Em `Tags`, especifique o par de chave/valor. É possível especificar mais de um par de chave/valor.

No exemplo a seguir, a solicitação de instância spot é marcada com duas tags: Key=Environment e Value=Production, e Key=Cost-Center e Value=123.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Marcar uma solicitação de instância spot existente

Console

Para marcar uma solicitação de instância spot existente usando o console

Depois de criar uma solicitação de instância spot, é possível adicionar tags à solicitação de instância spot usando o console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de instância spot.
4. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de instância spot existente usando o console

Depois que sua solicitação de instância spot tiver executado a instância spot, será possível adicionar tags à instância usando o console. Para ter mais informações, consulte Adicionar e excluir tags em um recurso individual.

AWS CLI

Para marcar uma solicitação de instância spot existente ou instância spot usando a AWS CLI

Use o comando create-tags para marcar os recursos existentes. No exemplo a seguir, a solicitação de instância spot e a instância spot existentes são marcadas com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Exibir tags de solicitação de instância spot

Console

Para visualizar tags de solicitação de instância spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de instância spot e escolha a guia Tags.

AWS CLI

Para descrever as tags de solicitação de instância spot

Também é possível visualizar as tags de uma solicitação de instância spot descrevendo a solicitação de instância spot. Use o comando describe-spot-instance-requests para visualizar a configuração da solicitação de instância spot especificada, que inclui todas as tags especificadas para a solicitação.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-EXAMPLE1 \
    --query "SpotInstanceRequests[*].Tags"
```

O seguinte é um exemplo de saída.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
```

```
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

Cancelar uma solicitação de instância spot

Se você não quiser mais sua solicitação de instância spot, poderá cancelá-la. Você só pode cancelar solicitações de instância spot que estão `open`, `active` ou `disabled`.

- A solicitação de instância spot é `open` quando sua requisição não ainda não foi atendida e nenhuma instância foi iniciada.
- A solicitação de instância spot é `active` quando ela foi atendida e as instâncias spot foram inicializadas como resultado.
- Sua solicitação de instância spot é `disabled` quando você interrompe a instância spot.

Se a solicitação de instância spot estiver `active` e tiver uma instância spot associada em execução, o cancelamento da solicitação não encerrará a instância. Para obter mais informações sobre como encerrar uma instância spot, consulte Encerrar uma instância spot.

Console

Para cancelar uma solicitação de instância spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione a solicitação de instância spot.
4. Escolha Ações, Cancelar solicitação.
5. (Opcional) Ao terminar de trabalhar com as Instâncias spot associadas, será possível encerrá-las. Na caixa de diálogo Cancelar solicitação spot, selecione Encerrar instâncias e escolha Confirmar.

AWS CLI

Para cancelar uma solicitação de instância spot usando a AWS CLI

Use o comando cancel-spot-instance-requests para cancelar a solicitação de instância spot especificada.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Interromper uma instância spot

Caso você não precise da Instâncias spot agora, mas quiser reiniciá-las posteriormente sem perder os dados persistentes no volume do Amazon EBS, é possível interrompê-los. As etapas para interromper uma instância spot são semelhantes às etapas para interromper uma instância sob demanda.

> **Note**
>
> Quando uma instância spot for interrompida, será possível modificar alguns atributos da instância, mas não o tipo dela.
> Não cobramos pelo uso de uma instância spot interrompida nem por taxas de transferência de dados, mas cobramos pelo armazenamento dos volumes do Amazon EBS.

Limitações

- Será possível interromper uma instância spot somente se ela tiver sido executada por meio de uma solicitação de instância spot `persistent`.
- Não será possível interromper uma instância spot se a solicitação da instância spot associada for cancelada. Quando a solicitação da instância spot for cancelada, você só poderá terminar a instância spot.
- Não é possível interromper uma instância spot se ela for parte de uma frota ou de um grupo de inicialização ou grupo de zona de disponibilidade.

Console

Para interromper uma instância spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione a instância spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
4. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância).
5. Quando a confirmação for solicitada, escolha Parar.

AWS CLI

Para interromper uma instância spot usando a AWS CLI

Use o comando stop-instances para interromper manualmente as Instâncias spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Iniciar uma instância spot

É possível iniciar uma instância spot que você encerrou anteriormente.

Pré-requisitos

É possível iniciar uma instância spot somente se:

- Você interrompeu manualmente a instância spot.
- A instância spot é uma instância com EBS.
- A capacidade da instância spot está disponível.
- O preço spot é inferior ao preço máximo.

Limitações

- Não é possível iniciar uma instância spot se ela fizer parte da frota ou do grupo de inicialização ou grupo de zona de disponibilidade.

As etapas para iniciar uma instância spot são semelhantes às etapas para iniciar uma instância sob demanda.

Console

Para iniciar uma instância spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
4. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

AWS CLI

Para iniciar uma instância spot usando a AWS CLI

Use o comando start-instances para iniciar manualmente as Instâncias spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Encerrar uma instância spot

Se você terminar uma instância spot em execução ou interrompida que foi executada por uma solicitação de instância spot persistente, a solicitação de instância spot fará a transição para o estado `open` para que a nova instância spot seja iniciada. Para garantir que nenhuma instância spot nova seja iniciada, primeiro é necessário cancelar a solicitação de instância spot.

Se você cancelar uma solicitação de instância spot `active` com uma instância spot em execução, a instância spot em execução não será automaticamente terminada, e você deverá terminá-la manualmente.

Se você cancelar uma solicitação de instância spot `disabled` com uma instância spot interrompida, a instância spot interrompida será automaticamente terminada pelo serviço spot do Amazon EC2. Pode haver um pequeno atraso entre o momento em que você cancelar a solicitação de instância spot e o momento em que o serviço spot terminar a instância spot.

Para ter mais informações, consulte Cancelar uma solicitação de instância spot.

Console

Para encerrar manualmente uma instância spot usando o console

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
5. Escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
6. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

AWS CLI

Para encerrar manualmente uma instância spot usando a AWS CLI

Use o comando terminate-instances para encerrar manualmente as Instâncias spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Exemplo de especificações de execução de solicitações de instância spot

Os exemplos a seguir mostram configurações de execução que é possível usar com o comando request-spot-instances para criar uma solicitação de instância spot. Para ter mais informações, consulte Criar uma solicitação de instância spot.

> **Important**
>
> Não recomendamos o uso do comando request-spot-instances por ser uma API herdada e sem investimento planejado. Para obter mais informações, consulte Qual é o melhor método de solicitação spot para usar?.

Exemplos

- Exemplo 1: Executar Instâncias spot
- Exemplo 2: executar Instâncias spot na zona de disponibilidade especificada
- Exemplo 3: executar Instâncias spot na sub-rede especificada
- Exemplo 4: executar uma instância spot dedicada

Exemplo 1: Executar Instâncias spot

O exemplo a seguir não inclui uma zona de disponibilidade nem sub-rede. O Amazon EC2 seleciona uma zona de disponibilidade para você. O Amazon EC2 executa as instâncias na sub-rede padrão da zona de disponibilidade selecionada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemplo 2: executar Instâncias spot na zona de disponibilidade especificada

O exemplo a seguir inclui uma zona de disponibilidade. O Amazon EC2 executa as instâncias na sub-rede padrão da zona de disponibilidade especificada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemplo 3: executar Instâncias spot na sub-rede especificada

O exemplo a seguir inclui uma sub-rede. O Amazon EC2 executa as instâncias na sub-rede especificada. Se a VPC não for padrão, a instância não receberá um endereço IPv4 público por padrão.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Para atribuir um endereço IPv4 público a uma instância em uma VPC não padrão, especifique o campo `AssociatePublicIpAddress` conforme exibido no seguinte exemplo. Ao especificar uma interface de rede, é necessário incluir o ID da sub-rede e o ID do grupo de segurança usando a interface de rede, em vez de usar os campos `SubnetId` e `SecurityGroupIds` mostrados no bloco de código anterior.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemplo 4: executar uma instância spot dedicada

O exemplo a seguir solicita uma instância spot com a locação de `dedicated`. Uma instância spot dedicada deve ser executada em uma VPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Status da solicitação spot

Para ajudar você a acompanhar suas solicitações de instância spot e planejar o uso de instâncias spot, use o status de solicitação fornecido pelo Amazon EC2. Por exemplo, um status de solicitação informa o motivo por que sua solicitação spot ainda não foi atendida ou lista as restrições que estão impedindo o atendimento de sua solicitação spot.

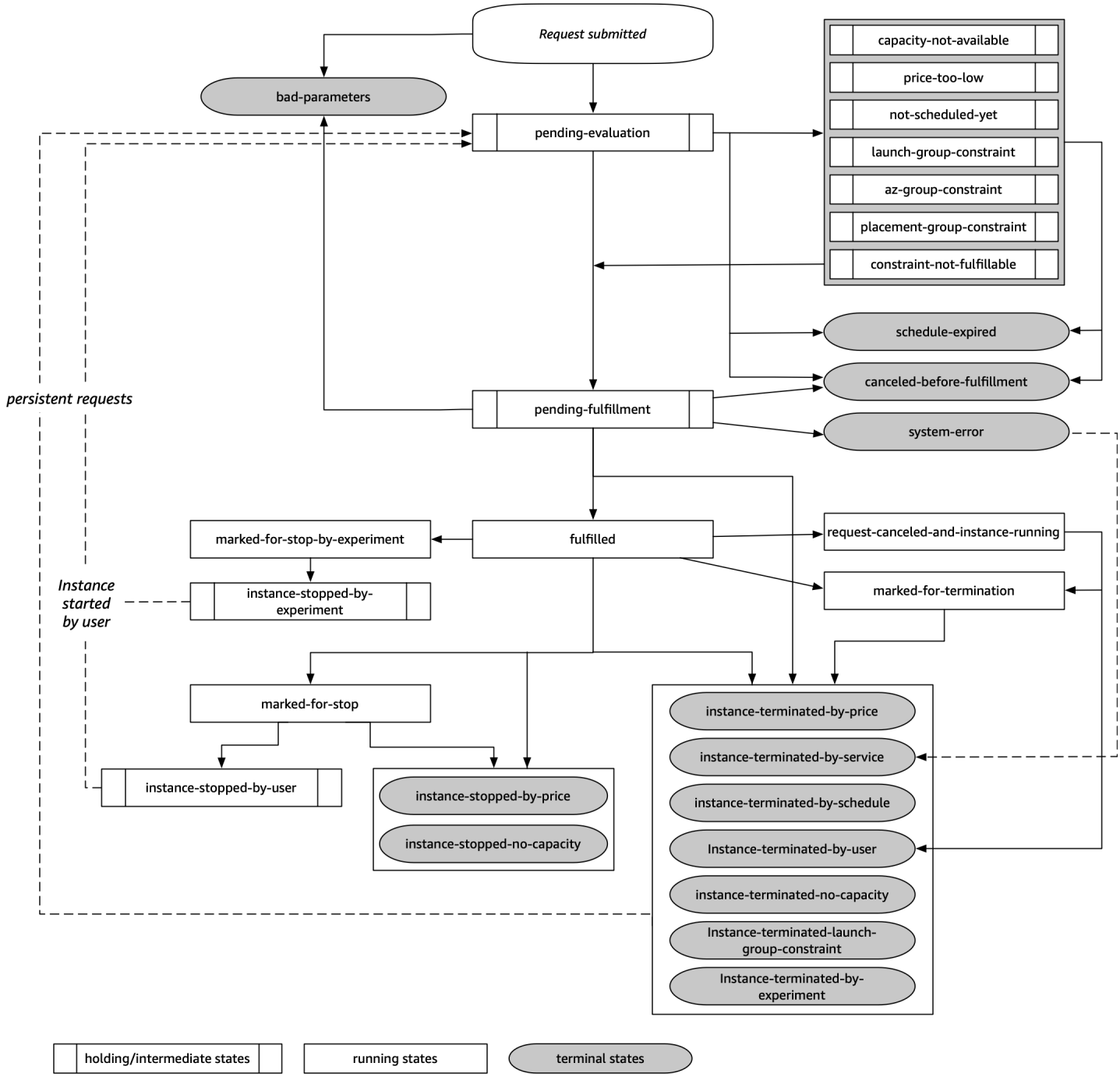
Em cada etapa do processo — também denominado ciclo de vida da solicitação spot — eventos específicos determinam estados sucessivos de solicitação.

Tópicos

- Ciclo de vida de uma solicitação spot
- Obter informações do status da solicitação
- Códigos de status das solicitações spot
- Evento de atendimento de solicitação de instância spot do EC2

Ciclo de vida de uma solicitação spot

O diagrama a seguir mostra os caminhos que a solicitação spot pode seguir durante todo o ciclo de vida, do envio ao encerramento. Cada etapa é representada como um nó, e o código de status de cada nó descreve o status da solicitação spot e da instância spot.



Avaliação pendente

Assim que você cria uma solicitação de instância spot, ela entra no estado `pending-evaluation`, a menos que um ou mais parâmetros da solicitação não sejam válidos (`bad-parameters`).

Código de status	Estado da solicitação	Estado da instância
`pending-evaluation`	`open`	Não aplicável
`bad-parameters`	`closed`	Não aplicável

Em espera

Se uma ou mais restrições da solicitação forem válidas, mas ainda não for possível atendê-las, ou se não houver capacidade suficiente, a solicitação assumirá um estado em espera aguardando que as restrições sejam atendidas. As opções de solicitação afetam a probabilidade de atendimento da solicitação. Por exemplo, se não houver capacidade, sua solicitação permanecerá no estado de hibernação até que haja capacidade disponível. Se você especificar um grupo de zonas de disponibilidade, a solicitação permanecerá no estado de espera até a restrição de zona de disponibilidade ser atendida.

No caso de interrupção de uma das zonas de disponibilidade, há uma chance de que a capacidade extra do EC2 disponível para solicitações de instância spot em outras zonas de disponibilidade possa ser afetada.

Código de status	Estado da solicitação	Estado da instância
`capacity-not-available`	`open`	Não aplicável
`price-too-low`	`open`	Não aplicável
`not-scheduled-yet`	`open`	Não aplicável
`launch-group-constraint`	`open`	Não aplicável
`az-group-constraint`	`open`	Não aplicável
`placement-group-constraint`	`open`	Não aplicável

Código de status	Estado da solicitação	Estado da instância
`constraint-not-fulfillable`	`open`	Não aplicável

Avaliação pendente/atendimento - terminal

A solicitação de instância spot poderá entrar no estado `terminal` se você criar uma solicitação que seja válida somente em um período específico e esse período expirar antes da solicitação atingir a fase de atendimento pendente. Isso também poderá ocorrer se você cancelar a solicitação ou se ocorrer um erro.

Código de status	Estado da solicitação	Estado da instância
`schedule-expired`	`cancelled`	Não aplicável
`canceled-before-fulfillment` [1]	`cancelled`	Não aplicável
`bad-parameters`	`failed`	Não aplicável
`system-error`	`closed`	Não aplicável

[1] Se a solicitação for cancelada.

Atendimento pendente

Quando as restrições especificadas (se houver) forem atendidas, sua solicitação spot entrará no estado `pending-fulfillment`.

Nesse momento, o Amazon EC2 está se preparando para provisionar as instâncias solicitadas. Se o processo parar nesse momento, provavelmente foi devido ao seu cancelamento pelo usuário antes da execução de uma instância spot. Isso também pode ocorrer devido a um erro inesperado do sistema.

Código de status	Estado da solicitação	Estado da instância
`pending-fulfillment`	`open`	Não aplicável

Atendido

Quando todas as especificações das instâncias spot forem atendidas, sua solicitação spot será atendida. O Amazon EC2 executa as instâncias spot, o que pode levar alguns minutos. Se uma instância spot ficar em estado de hibernação, ela permanecerá nesse estado até que a solicitação possa ser atendida novamente ou seja cancelada.

Código de status	Estado da solicitação	Estado da instância
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Se você interromper uma instância spot, a solicitação spot entrará no estado `marked-for-stop` ou `instance-stopped-by-user` até que ela possa ser iniciada novamente ou até que a solicitação seja cancelada.

Código de status	Estado da solicitação	Estado da instância
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user` [1]	`disabled` ou `cancelled` [2]	`stopped`

[1] Uma instância spot entrará no estado `instance-stopped-by-user` se você interromper a instância ou executar o comando de desligamento na própria instância. Depois de interromper a instância, é possível iniciá-la novamente. Na reinicialização, a solicitação de instância spot retornará para o estado `pending-evaluation` e o Amazon EC2 iniciará uma nova instância spot quando as restrições forem atendidas.

² O estado da solicitação spot será `disabled` se você interromper a instância spot, mas não cancelar a solicitação. O estado da solicitação será `cancelled` se a instância spot for interrompida e a solicitação expirar.

Atendido - terminal

As instâncias spot continuarão em execução, contanto que haja capacidade disponível para o tipo de instância e você não encerre a instância. Se o Amazon EC2 precisar encerrar as instâncias spot, a solicitação spot assumirá um estado terminal. Uma solicitação também entrará no estado terminal se você cancelar a solicitação spot ou encerrar as Instâncias spot.

Código de status	Estado da solicitação	Estado da instância
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (única), `open` (persistente)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`

Código de status	Estado da solicitação	Estado da instância
`instance-terminated-by-user`	`closed` ou `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (única), `open` (persistente)	`running` †
`instance-terminated-no-capacity`	`closed` (única), `open` (persistente)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (única), `open` (persistente)	`terminated`

[1] O estado da solicitação será `closed` se você encerrar a instância, mas não cancelar a solicitação. O estado da solicitação será `cancelled` se você encerrar a instância e cancelar a solicitação. Mesmo que você encerre uma instância spot antes de cancelar a solicitação, talvez o Amazon EC2 atrase a detecção de que a instância spot foi encerrada. Nesse caso, o estado da solicitação poderá ser `closed` ou `cancelled`.

† Quando o Amazon EC2 interrompe uma instância spot, se precisa da capacidade de volta e a instância está configurada para terminar na interrupção, o status é imediatamente definido como`instance-terminated-no-capacity` (não é definido como `marked-for-termination`). No entanto, a instância permanece no estado `running` por 2 minutos para refletir o período de 2 minutos quando a instância recebe o aviso de interrupção da instância spot. Após 2 minutos, o estado da instância é definido como `terminated`.

Experimentos de interrupção

Você pode usar AWS Fault Injection Service para iniciar a interrupção de uma instância spot e poder testar como as aplicações nessas instâncias spot respondem. Se o AWS FIS interromper uma instância spot, sua solicitação de spot entrará no estado `marked-for-stop-by-experiment` e depois no estado `instance-stopped-by-experiment`. Se o AWS FIS encerrar uma instância spot, sua solicitação de spot entrará no estado `instance-terminated-by-experiment`. Para ter mais informações, consulte the section called “Iniciar uma interrupção”.

Código de status	Estado da solicitação	Estado da instância
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Requisições persistentes

Quando as instâncias spot forem encerradas (por você ou pelo Amazon EC2), se a solicitação spot for uma requisição persistente, ela retornará ao estado `pending-evaluation` e, em seguida, o Amazon EC2 poderá iniciar uma nova instância spot quando as restrições forem cumpridas.

Obter informações do status da solicitação

É possível obter informações de status da solicitação usando o AWS Management Console ou a ferramenta da linha de comando.

Para obter informações sobre o status de uma solicitação usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Spot Requests (Solicitações spot) e selecione a solicitação spot.
3. Para verificar o status, na guia Descrição, marque o campo Status .

Para obter informações de status da solicitação usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-spot-instance-requests (AWS CLI)
- Get-EC2SpotInstanceRequest (AWS Tools for Windows PowerShell)

Códigos de status das solicitações spot

As informações de status da solicitação spot são compostas de um código de status da solicitação, o tempo de atualização e uma mensagem de status. Juntas, essas informações ajudam a determinar a disposição de sua solicitação spot.

Veja a seguir os códigos de status de solicitação spot:

`az-group-constraint`

O Amazon EC2 não pode executar todas as instâncias que você solicitou na mesma zona de disponibilidade.

`bad-parameters`

Um ou mais parâmetros para sua solicitação spot são inválidos (por exemplo, a AMI que você especificou não existe). A mensagem de status de solicitação indica qual parâmetro é inválido.

`canceled-before-fulfillment`

O usuário cancelou a solicitação spot antes de ser atendida.

`capacity-not-available`

Não há capacidade suficiente disponível para as instâncias solicitadas.

`constraint-not-fulfillable`

A solicitação spot não pode ser atendida porque uma ou mais restrições são inválidas (por exemplo, a zona de disponibilidade não existe). A mensagem de status de solicitação indica qual restrição é inválida.

`fulfilled`

A solicitação spot é `active` e Amazon EC2 está executando seu Instâncias spot.

`instance-stopped-by-price`

Sua instância foi interrompida porque o preço spot excedeu seu preço máximo.

`instance-stopped-by-user`

A instância foi interrompida porque um usuário interrompeu a instância ou executou o comando de desligamento a partir da instância.

`instance-stopped-no-capacity`

Sua instância foi interrompida devido às necessidades de gerenciamento de capacidade do EC2.

`instance-terminated-by-price`

Sua instância foi encerrada porque o preço spot excedeu seu preço máximo. Se sua solicitação for uma sugestão de preço persistente, o processo será reiniciado, portanto, sua solicitação está com a avaliação pendente.

`instance-terminated-by-schedule`

Sua instância spot foi encerrada no final da duração prevista.

`instance-terminated-by-service`

A instância foi encerrada em um estado interrompido.

`instance-terminated-by-user` ou `spot-instance-terminated-by-user`

Você encerrou uma instância spot que tinha sido atendida, portanto, o estado da solicitação é `closed` (a menos que se trate de uma requisição persistente) e o estado da instância é `terminated` .

`instance-terminated-launch-group-constraint`

Uma ou mais instâncias no grupo de execução foram encerradas, portanto, a restrição do grupo de execução deixou de ser atendida.

`instance-terminated-no-capacity`

Sua instância foi encerrada devido aos processos padrão de gerenciamento de capacidade.

`launch-group-constraint`

O Amazon EC2 não pode executar todas as instâncias que você solicitou ao mesmo tempo. Todas as instâncias em um grupo de execução são iniciadas e encerradas juntas.

`limit-exceeded`

O limite no número de volumes EBS ou de armazenamento de volume total foi excedido. Para obter mais informações sobre esses limites e como solicitar um aumento, consulte Limites do Amazon EBS no Referência geral da Amazon Web Services.

`marked-for-stop`

A instância spot é marcada para interrupção.

`marked-for-termination`

A instância spot é marcada para encerramento.

`not-scheduled-yet`

A solicitação spot não é avaliada até a data programada.

`pending-evaluation`

Após criar uma solicitação de instância spot, ela entrará no estado `pending-evaluation` enquanto o sistema avalia os parâmetros da solicitação.

`pending-fulfillment`

O Amazon EC2 está tentando provisionar as Instâncias spot.

`placement-group-constraint`

A solicitação spot ainda não pode ser atendida porque uma instância spot não pode ser adicionada ao grupo de posicionamento no momento.

`price-too-low`

A solicitação ainda não pode ser atendida porque seu preço máximo está abaixo do preço spot. Nesse caso, nenhuma instância é executada e sua solicitação permanece `open`.

`request-canceled-and-instance-running`

Você cancelou a solicitação spot enquanto as Instâncias spot ainda estão em execução. A solicitação é `cancelled`, mas instâncias permanecem `running`.

`schedule-expired`

A solicitação spot expirou porque não foi atendida antes da data especificada.

`system-error`

Houve um erro de sistema inesperado. Se esse for um problema recorrente, entre em contato com o AWS Support para obter assistência.

Evento de atendimento de solicitação de instância spot do EC2

Quando uma solicitação de instância spot é atendida, o Amazon EC2 envia um evento de atendimento de solicitação de instância spot do EC2 ao Amazon EventBridge. É possível criar uma regra para realizar uma ação sempre que esse evento ocorrer, como invocar uma função Lambda ou notificar um tópico do Amazon SNS.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Recomendações de rebalanceamento de instâncias do EC2

Uma recomendação de rebalanceamento de instância do EC2 é um sinal que envia uma notificação quando uma instância Spot tem risco elevado de interrupção. O sinal pode chegar antes do aviso de interrupção da instância Spot de dois minutos, dando a você a oportunidade de gerenciar proativamente a instância spot. É possível decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção.

Nem sempre é possível para o Amazon EC2 enviar o sinal de recomendação de rebalanceamento antes do aviso de interrupção da instância spot de dois minutos. Portanto, o sinal de recomendação de rebalanceamento pode chegar junto com o aviso de interrupção de dois minutos.

As recomendações de rebalanceamento são disponibilizadas como um evento do EventBridge e como um item nos metadados de instância na instância spot. Os eventos são emitidos com base no melhor esforço.

> **Note**
>
> As recomendações de rebalanceamento só são aceitas para Instâncias spot que sejam executadas depois de 5 de novembro de 2020, 0h (UTC).

Tópicos

- Rebalancear ações que é possível executar
- Monitorar os sinais de recomendação de rebalanceamento
- Serviços que usam o sinal de recomendação de rebalanceamento

Rebalancear ações que é possível executar

Estas são algumas das possíveis ações de rebalanceamento que é possível executar:

Desligamento normal

Quando você receber o sinal de recomendação de rebalanceamento para uma instância spot, poderá iniciar os procedimentos de desligamento da instância, o que pode incluir a garantia de que os processos sejam concluídos antes de serem interrompidos. Por exemplo, é possível fazer upload de logs de sistema ou de aplicações para o Amazon Simple Storage Service (Amazon S3), desligar operadores do Amazon SQS ou concluir o cancelamento do registro do Sistema de Nomes de Domínio (DNS). Também é possível salvar seu trabalho em armazenamento externo e retomá-lo mais tarde.

Impedir que novos trabalhos sejam programados

Quando você recebe o sinal de recomendação de rebalanceamento para uma instância spot, pode impedir que novos trabalhos sejam programados na instância enquanto ela continuar a ser usada até o trabalho programado ser concluído.

Executar proativamente novas instâncias de substituição

É possível configurar grupos do Auto Scaling, EC2 Fleet ou frota spot para iniciar automaticamente as instâncias spot de substituição quando um sinal de recomendação de rebalanceamento é emitido. Para obter mais informações, consulte Usar o rebalanceamento de capacidade para lidar com interrupções spot do Amazon EC2, no Guia do usuário do Amazon EC2 Auto Scaling, e Rebalanceamento de capacidade para frota do EC2 e Rebalanceamento de capacidade para a frota spot neste guia de usuário.

Monitorar os sinais de recomendação de rebalanceamento

É possível monitorar o sinal de recomendação de rebalanceamento de modo que, quando ele for emitido, você possa executar as ações especificadas na seção anterior. O sinal de recomendação de rebalanceamento é disponibilizado como um evento que é enviado para o Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events) e como metadados de instância na instância spot.

Monitorar sinais de recomendação de rebalanceamento:

- Usar o Amazon EventBridge
- Usar metadados da instância

Usar o Amazon EventBridge

Quando o sinal de recomendação de rebalanceamento é emitido para uma instância spot, o evento para o sinal é enviado para o Amazon EventBridge. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Veja a seguir um exemplo de evento para o sinal de recomendação de rebalanceamento.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Os campos a seguir formam o padrão de evento definido na regra:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifica que o evento é um evento de recomendação de rebalanceamento

`"source": "aws.ec2"`

Identifica que o evento é de Amazon EC2

Criar uma regra de EventBridge

É possível escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra.

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivos móveis sempre que Amazon EC2 emite um sinal de recomendação de rebalanceamento. O sinal é emitido como um evento de `EC2 Instance Rebalance Recommendation`, que aciona a ação definida pela regra.

Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para um evento de recomendação de rebalanceamento

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   d. Escolha Próximo.
4. Em Build event pattern (Criar padrão de evento), faça o seguinte:
   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
   b. Em Event pattern (Padrão de evento), neste exemplo você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Instance Rebalance Recommendation` e, em seguida, escolherá Save (Salvar).

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Em AWS Service (Produto da), escolha EC2 Spot Fleet (Frota spot do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Instance Rebalance Recommendation (Recomendação de rebalanceamento da instância do EC2).

E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar Regra.

Para obter mais informações, consulte Amazon EventBridge rules (Regras do Amazon EventBridge) e Amazon EventBridge event patterns (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Guia do usuário do Amazon EventBridge).

Usar metadados da instância

A categoria de metadados da instância `events/recommendations/rebalance` fornece o horário aproximado, em UTC, quando o sinal de recomendação de rebalanceamento foi emitido para uma instância spot.

Recomendamos que você verifique se há sinais de recomendação de rebalanceamento a cada 5 segundos para que você não perca a oportunidade de agir de acordo com a recomendação de rebalanceamento.

Se uma instância spot receber uma recomendação de rebalanceamento, o horário em que o sinal foi emitido estará presente nos metadados da instância. É possível recuperar o horário em que o sinal foi emitido da seguinte forma.

Use o comando referente ao seu sistema operacional.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/
recommendations/rebalance
```

A seguir, é mostrado um exemplo de saída, que indica o horário, em UTC, em que o sinal de recomendação de rebalanceamento foi emitido para a instância spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Se o sinal não tiver sido emitido para a instância, o `events/recommendations/rebalance` não estará presente e você receberá uma mensagem de erro HTTP 404 quando tentar recuperá-lo.

Serviços que usam o sinal de recomendação de rebalanceamento

O Amazon EC2 Auto Scaling, a EC2 Fleet e a frota spot usam o sinal de recomendação de rebalanceamento para facilitar a manutenção da disponibilidade da workload, aumentando proativamente a frota com uma nova instância spot antes que uma instância em execução receba o aviso de interrupção da instância spot de dois minutos. É possível fazer com que esses serviços monitorem e respondam proativamente às alterações que afetam a disponibilidade da suas Instâncias spot. Para obter mais informações, consulte as informações a seguir.

- Usar o rebalanceamento de capacidade para lidar com interrupções spot do Amazon EC2 no Guia do usuário do Amazon EC2 Auto Scaling.
- Rebalanceamento de capacidade no tópico Frota do EC2 deste guia do usuário
- Rebalanceamento de capacidade no tópico Frota spot deste guia do usuário

Interrupções de instâncias spot

É possível executar Instâncias spot na capacidade adicional do EC2 para obter grandes descontos em troca de devolvê-los quando o Amazon EC2 precisar da capacidade de volta. Quando o Amazon EC2 recupera uma instância spot, chamamos esse evento de interrupção de instância spot.

Quando o Amazon EC2 interrompe uma instância spot, ele termina, para ou hiberna a instância, dependendo do que você especificou ao criar a solicitação de spot.

A demanda por Instâncias spot pode variar significativamente de um momento para outro, e a disponibilidade das Instâncias spot também pode variar significativamente dependendo de quantas

instâncias do EC2 não utilizadas estão disponíveis. É sempre possível que sua instância spot seja interrompida.

Uma instância sob demanda especificada em uma EC2 Fleet ou frota spot não pode ser interrompida.

Conteúdo

- Motivos para interrupção de uma instância spot
- Comportamento das interrupções de instâncias spot
- Parar Instâncias spot interrompida
- Hibernar Instâncias spot interrompida
- Terminar instâncias spot interrompidas
- Preparar para interrupções de instâncias spot
- Iniciar a interrupção de uma instância spot
- Avisos de interrupção de instância spot
- Encontrar Instâncias spot interrompidas
- Determinar se o Amazon EC2 terminou uma instância spot
- Faturamento para Instâncias spot interrompidas

Motivos para interrupção de uma instância spot

Veja a seguir os possíveis motivos pelos quais o Amazon EC2 pode interromper Instâncias spot:

Capacidade

O Amazon EC2 pode interromper sua instância spot quando ele precisar dela de volta. O EC2 recupera sua instância principalmente para redirecionar a capacidade, mas também pode ocorrer por outros motivos, como manutenção de host ou descomissionamento de hardware

Preço

O preço spot é superior ao preço máximo.

Você pode especificar o preço máximo em sua solicitação spot. No entanto, se você especificar um preço máximo, as instâncias serão interrompidas com mais frequência do que se você não especificar esse parâmetro.

Restrições

Se a solicitação de spot incluir uma restrição como um grupo de execução ou um grupo de zonas de disponibilidade, essas instâncias spot serão encerradas como um grupo quando não for mais possível atender à restrição.

É possível ver o histórico de taxas de interrupção para o seu tipo de instância no Supervisor de instâncias spot.

Comportamento das interrupções de instâncias spot

É possível especificar que o Amazon EC2 deve executar uma das seguintes opções ao interromper uma instância spot:

- Parar Instâncias spot interrompida
- Hibernar Instâncias spot interrompida
- Terminar instâncias spot interrompidas (esse é o comportamento padrão)

Especificar o comportamento de interrupção

É possível especificar o comportamento de interrupção ao criar uma solicitação spot. Se você não especificar um comportamento de interrupção, o padrão será o Amazon EC2 terminar as instâncias spot quando elas forem interrompidas.

A maneira pela qual você especifica o comportamento de interrupção pode diferir dependendo de como você solicita as Instâncias spot.

- Se você solicitar instâncias spot usando o assistente de inicialização de instância, poderá especificar o comportamento de interrupção da seguinte forma: no assistente de inicialização de instâncias, expanda Detalhes avançados e marque a caixa de seleção Solicitar Instâncias spot. Escolha Customize (Personalizar). Em Comportamento de interrupção, escolha um comportamento de interrupção. Se o comportamento de interrupção for hibernação, você também pode escolher Habilitar em Comportamento de parar - hibernar.
- Se você solicitar Instâncias spot usando a CLI run-instances, poderá especificar o comportamento de interrupção da seguinte forma: na configuração da solicitação (`--instance-market-options`), em `InstanceInterruptionBehavior`, especifique um comportamento de interrupção. Se o comportamento de interrupção for `hibernate`, você terá a alternativa de habilitar a hibernação usando o parâmetro `--hibernation-options Configured=true`.

- Se você configurar as Instâncias spot em um modelo de execução, poderá especificar o comportamento de interrupção da seguinte forma: no modelo de execução, expanda Advanced details) (Detalhes avançados) e marque a caixa de seleção Request (Solicitar) Instâncias spot. Escolha Personalizar e, em Comportamento de interrupção, escolha um comportamento de interrupção.
- Se você solicitar as Instâncias spot usando o console do Spot, poderá especificar o comportamento de interrupção da seguinte maneira: marque a caixa de seleção Manter capacidade de destino e, em Comportamento de interrupção, escolha um comportamento de interrupção.
- Se você configurar as instâncias spot na configuração de solicitação ao usar a CLI create-fleet, poderá especificar o comportamento de interrupção da seguinte maneira: para `InstanceInterruptionBehavior`, especifique um comportamento de interrupção.
- Se você configurar as instâncias spot na configuração de solicitação ao usar a CLI request-spot-fleet, poderá especificar o comportamento de interrupção da seguinte maneira: para `InstanceInterruptionBehavior`, especifique um comportamento de interrupção.
- Se você configurar as Instâncias spot usando a CLI de request-spot-instances, poderá especificar o comportamento de interrupção da seguinte forma: para `--instance-interruption-behavior`, especifique um comportamento de interrupção.

> **Note**
>
> Não recomendamos o uso dos comandos request-spot-fleet e request-spot-instances para solicitar instâncias spot por serem APIs herdadas sem investimento planejado. Para ter mais informações, consulte Qual é o melhor método de solicitação spot para usar?.

Parar Instâncias spot interrompida

É possível especificar que o Amazon EC2 pare suas instâncias spot quando elas são interrompidas. Para ter mais informações, consulte Especificar o comportamento de interrupção.

Considerações

- Somente o Amazon EC2 pode reiniciar uma instância spot interrompida parada.
- Para uma instância spot iniciada por uma solicitação de instância spot `persistent`: o Amazon EC2 reinicia a instância parada quando a capacidade está disponível na mesma zona de

disponibilidade e para o mesmo tipo de instância que a instância parada (a mesma especificação de início deve ser usada).

- Para instâncias spot executadas por uma frota do EC2 ou frota spot do tipo`maintain`: depois que uma instância spot é interrompida, o Amazon EC2 executa uma instância de substituição para manter a capacidade-alvo. O Amazon EC2 localiza os melhores grupos de capacidade spot com base na estratégia de alocação especificada (`lowestPrice`, `diversified` ou `InstancePoolsToUseCount`); ele não prioriza o grupo com a instância parada anteriormente. Posteriormente, se a estratégia de alocação levar a um grupo contendo a instância parada anteriormente, o Amazon EC2 reiniciará as instâncias paradas para atender à capacidade-alvo.

  Por exemplo, considere a frota spot com a estratégia de alocação `lowestPrice`. Na execução inicial, um grupo `c3.large` atende aos critérios de `lowestPrice` para a especificação de execução. Posteriormente, quando as instâncias `c3.large` são interrompidas, o Amazon EC2 para as instâncias e repõe a capacidade de outro grupo que se encaixe na estratégia `lowestPrice`. Desta vez, o grupo passa a ser um grupo `c4.large` e o Amazon EC2 inicia instâncias `c4.large` para atender à capacidade-alvo. Da mesma forma, a frota spot poderia se mover para um grupo `c5.large` da próxima vez. Em cada uma dessas transições, o Amazon EC2 não prioriza grupos com instâncias paradas anteriormente, mas prioriza apenas a estratégia de alocação especificada. A estratégia `lowestPrice` pode levar de volta a grupos com instâncias interrompidas anteriormente. Por exemplo, se instâncias forem interrompidas no grupo `c5.large` e a estratégia `lowestPrice` levar de volta aos grupos `c3.large` ou `c4.large`, as instâncias interrompidas anteriormente serão reiniciadas para atender à capacidade de destino.
- Quando uma instância spot for interrompida, será possível modificar alguns atributos da instância, mas não o tipo dela. Se você desanexar ou excluir um volume do EBS, ele não será anexado quando a instância spot for iniciada. Se você desvincular o volume raiz e o Amazon EC2 tentar iniciar a instância spot, a instância falhará ao iniciar e o Amazon EC2 terminará a instância interrompida.
- É possível encerrar uma instância spot enquanto ela está interrompida.
- Se você cancelar uma solicitação de instância spot, uma EC2 Fleet ou uma frota spot, o Amazon EC2 terminará todas as instâncias spot associadas que estiverem paradas.
- Enquanto uma instância spot estiver parada, você será cobrado apenas pelos volumes do EBS, que são preservados. Com a EC2 Fleet e a frota spot, se houver muitas instâncias interrompidas, será possível exceder o limite de número de volumes do EBS na sua conta. Para obter mais informações sobre como você é cobrado quando uma instância spot é interrompida, consulteFaturamento para Instâncias spot interrompidas.

- Certifique-se de estar familiarizado com as implicações de parar uma instância. Para obter informações sobre o que acontece quando uma instância está parada, consulte Diferenças entre reinicialização, interrupção, hibernação e encerramento.

Pré-requisitos

Para parar uma instância spot interrompida, os seguintes pré-requisitos devem estar implementados:

Tipo de solicitação de spot

Tipo de solicitação de instância spot: deve ser `persistent`. Não é possível especificar um grupo de execução na solicitação de instância spot.

Tipo de solicitação de frota do EC2 ou frota spot: deve ser `maintain`.

Tipo do volume de raiz

Deve ser um volume do EBS, e não um volume de armazenamento de instâncias.

Hibernar Instâncias spot interrompida

É possível especificar que o Amazon EC2 hiberne suas instâncias spot quando elas estão interrompidas. Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.

O Amazon EC2 agora oferece a mesma experiência de hibernação para as instâncias spot que está disponível atualmente para as instâncias sob demanda. Ele oferece um suporte mais amplo, sendo compatível com o seguinte para hibernação de instâncias spot:

- Mais AMIs compatíveis
- Mais famílias de instâncias compatíveis
- Hibernação iniciada pelo usuário

Terminar instâncias spot interrompidas

Quando o Amazon EC2 interrompe uma instância spot, ele termina a instância por padrão, a menos que você especifique um comportamento de interrupção diferente, como parar ou hibernar. Para ter mais informações, consulte Especificar o comportamento de interrupção.

Preparar para interrupções de instâncias spot

A demanda por Instâncias spot pode variar significativamente de um momento para outro, e a disponibilidade das Instâncias spot também pode variar significativamente dependendo de quantas instâncias do EC2 não utilizadas estão disponíveis. É sempre possível que sua instância spot seja interrompida. Portanto, é necessário garantir que a aplicação esteja preparada para uma interrupção de instância spot.

Recomendamos que você siga essas práticas recomendadas para estar preparado para uma interrupção da instância spot.

- Crie sua solicitação de spot usando um grupo do Auto Scaling. Se suas Instâncias spot forem interrompidas, o grupo do Auto Scaling iniciará automaticamente as instâncias de substituição. Para obter mais informações, consulte Grupos de Auto Scaling com vários tipos de instância e opções de compra no Manual do usuário do Amazon EC2 Auto Scaling.
- Certifique-se de que sua instância esteja preparada assim que a solicitação seja atendida usando uma Imagem de máquina da Amazon (AMI) que contenha a configuração de software necessária. Também é possível usar dados de usuário para executar comandos no startup.
- Os dados nos volumes de armazenamento de instância são perdidos quando a instância é interrompida ou encerrada. Faça backup de todos os dados importantes em volumes de armazenamento de instância para um armazenamento mais persistente, como o Amazon S3, o Amazon EBS ou o Amazon DynamoDB.
- Armazene regularmente os dados importantes em um lugar em que eles não sejam afetados se a instância spot for terminada. Por exemplo, é possível usar o Amazon S3, o Amazon EBS ou o DynamoDB.
- Divida o trabalho em tarefas pequenas (usando uma grade, um Hadoop ou uma arquitetura baseada em fila) ou use pontos de verificação para que você possa salvar seu trabalho com frequência.
- O Amazon EC2 emite um sinal de recomendação de rebalanceamento para a instância spot quando a instância apresenta risco elevado de interrupção. É possível confiar na recomendação de rebalanceamento para gerenciar proativamente as interrupções de instância spot sem precisar aguardar o aviso de interrupção de dois minutos da instância spot. Para ter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.
- Use os avisos de interrupção de instância spot para monitorar o status das instâncias spot. Para ter mais informações, consulte Avisos de interrupção de instância spot.

- Embora nos esforcemos ao máximo para fornecer esse aviso o mais rápido possível, pode ser que a instância spot seja interrompida antes que o aviso seja disponibilizado. Teste sua aplicação para garantir que ele lide tranquilamente com a interrupção inesperada de uma instância, mesmo que você esteja monitorando sinais de recomendação de rebalanceamento e avisos de interrupção. É possível fazer isso executando a aplicação com uma instância sob demanda e, em seguida, terminando a instância sob demanda por conta própria.
- Execute um experimento de injeção de falhas controlado com AWS Fault Injection Service para testar como sua aplicação responde quando sua instância spot é interrompida. Para obter mais informações, consulte o Tutorial: Teste interrupções de instância spot usando o AWS FIS no Guia do usuário do AWS Fault Injection Service.

Iniciar a interrupção de uma instância spot

Você pode selecionar uma instância spot no console do Amazon EC2 e iniciar uma interrupção para poder testar como as aplicações nessas instâncias spot lidam com interrupções. Quando você inicia a interrupção de uma instância spot, o Amazon EC2 avisa que a instância spot será interrompida em dois minutos e, passados os dois minutos, o Amazon EC2 interrompe a instância spot.

O serviço subjacente que realiza a interrupção da instância spot é o AWS Fault Injection Service (AWS FIS). Para obter mais informações sobre o AWS FIS, consulte AWS Fault Injection Service.

> **Note**
>
> Os comportamentos de interrupção são `terminate`, `stop` e `hibernate`. Se o comportamento de interrupção for definido como `hibernate`, quando você iniciar a interrupção de uma instância spot, o processo de hibernação começará imediatamente.

Iniciar uma interrupção de insitância spot é compatível com todas as Regiões da AWS, exceto Ásia-Pacífico (Jacarta), Ásia-Pacífico (Osaka), China (Pequim), China (Ningxia) e Oriente Médio (EAU).

Tópicos

- Iniciar a interrupção de uma instância spot
- Verificar a interrupção da instância spot
- Cotas

Iniciar a interrupção de uma instância spot

Você pode usar o console do EC2 para iniciar rapidamente a interrupção de uma instância spot. Ao selecionar uma solicitação de Instância Spot, você pode iniciar a interrupção de uma Instância Spot. Ao selecionar uma solicitação de frota spot, você pode iniciar a interrupção de várias instâncias spot de uma só vez.

Para fazer experimentos mais avançados para testar interrupções de instâncias spot, você pode criar seus próprios experimentos usando o console do AWS FIS.

Para iniciar a interrupção de uma instância spot usando o console do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Selecione uma solicitação de instância spot e escolha Actions (Ações), Initiate interruption (Iniciar interrupção). Você não pode selecionar várias solicitações de instância spot para iniciar uma interrupção.
4. Na caixa de diálogo Initiate Spot Instance interruption (Iniciar interrupção de instância spot), em Service access (Acesso ao serviço), use o perfil padrão ou escolha um perfil existente. Para escolher uma função existente, escolha Usar uma função de serviço existente e, em seguida, para Função do IAM}, selecione a função a ser usada.
5. Quando estiver pronto para iniciar a interrupção da instância spot, escolha Initiate interruption (Iniciar interrupção).

Para iniciar a interrupção de uma ou mais instâncias spot em uma solicitação de frota spot usando o console EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Selecione uma solicitação de instância spot e escolha Actions (Ações), Initiate interruption (Iniciar interrupção). Você não pode selecionar várias solicitações do Spot Fleet para iniciar uma interrupção.
4. Na caixa de diálogo Especificar número de instâncias spot, em Número de instâncias a serem interrompidas, insira o número de instâncias spot a serem interrompidas e escolha Confirmar.

> **Note**
>
> O número não pode exceder o número de instâncias spot na frota ou sua cota para o número de instâncias spot que AWS FIS podem ser interrompidas por experimento.

5. Na caixa de diálogo Initiate Spot Instance interruption (Iniciar interrupção de instância spot), em Service access (Acesso ao serviço), use o perfil padrão ou escolha um perfil existente. Para escolher uma função existente, escolha Usar uma função de serviço existente e, em seguida, para Função do IAM}, selecione a função a ser usada.
6. Quando estiver pronto para iniciar a interrupção da instância spot, escolha Initiate interruption (Iniciar interrupção).

Para fazer experimentos mais avançados para testar interrupções de instâncias spot usando o console do AWS FIS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Escolha Actions (Ações), Create advanced experiments (Criar experimentos avançados).

   O console do AWS FIS será aberto. Para obter mais informações, consulte o Tutorial: testar interrupções de instância spot usando o AWS FIS no Guia do usuário do AWS Fault Injection Service.

Verificar a interrupção da instância spot

Depois que você inicia a interrupção, ocorre o seguinte:

- A instância spot recebe uma recomendação de rebalanceamento da instância.
- Um aviso de interrupção de instância spot é emitido dois minutos antes de AWS FIS interromper sua instância.
- Passados os dois minutos, a instância spot é interrompida.
- Uma instância spot que foi interrompida pelo AWS FIS permanece parada até ser reiniciada.

Para verificar se a instância foi interrompida depois que você iniciou a interrupção

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, abra Spot Requests (Solicitações de spot) e Instances (Instâncias) em guias ou janelas separadas do navegador.
3. Para Solicitações Spot, selecione a solicitação de Instância Spot ou a solicitação de Frota Spot. O status inicial é `fulfilled`. Depois que a instância é interrompida, o status se altera como se segue, dependendo do comportamento da interrupção:
   - `terminate`: o status se altera para `instance-terminated-by-experiment`.
   - `stop`: o status se altera para `marked-for-stop-by-experiment` e depois `instance-stopped-by-experiment`.
4. Em Instances (Instâncias), selecione a instância spot. O status inicial é `Running`. Dois minutos depois que você recebe o aviso de interrupção da instância spot, o status se altera como se segue, dependendo do comportamento da interrupção:
   - `stop`: o status se altera para `Stopping` e depois `Stopped`.
   - `terminate`: o status se altera para `Shutting-down` e depois `Terminated`.

Cotas

Você Conta da AWS tem a seguinte cota padrão para o número de instâncias spot que AWS FIS podem ser interrompidas por experimento.

Nome	Padrão	Ajustável	Descrição
Instâncias spot de destino para aws:ec2:send-spot-instance-interruptions	Cada região compatível: 5	Sim	O número máximo de instâncias spot que aws:ec2:send-spot-instance-interruptions pode atingir quando você identifica alvos usando tags, por experimento.

É possível solicitar um aumento da cota. Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Para visualizar todas as cotas de AWS FIS, abra o console Service Quotas. No painel de navegação, escolha AWS services (Serviços da) e selecione AWS Fault Injection Service. Você também pode ver todas as cotas AWS Fault Injection Service no Guia do AWS Fault Injection Service usuário.

Avisos de interrupção de instância spot

Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 parar ou encerrar uma instância spot. Se você especificar uma hibernação como o comportamento de interrupção, receberá um aviso de interrupção, mas não receberá o aviso dois minutos antes porque o processo de hibernação começará imediatamente.

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, é possível aproveitar os avisos de interrupção de instância spot. Recomendamos que você verifique esses avisos de interrupção a cada 5 segundos.

Os avisos de interrupção são disponibilizados como um evento do Eventbridge e como itens nos metadados de instância na instância spot. Avisos de interrupção são emitidos de acordo com o melhor esforço.

EC2 Spot Instance interruption notice

Quando o Amazon EC2 vai interromper a instância spot, ele emite um evento dois minutos antes da interrupção real (exceto para a hibernação, que recebe o aviso de interrupção, mas não dois minutos antes, porque a hibernação começa imediatamente). Este evento pode ser detectado pelo Amazon EventBridge. Para obter mais informações sobre eventos no EventBridge, consulte o Guia do usuário do Amazon EventBridge. Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte Aproveitar os avisos de interrupção de instância spot do Amazon EC2.

Este é um exemplo do evento de interrupção da instância spot. Os valores possíveis para `instance-action` são `hibernate`, `stop` ou `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
```

```
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> O formato de ARN do evento de interrupção da instância spot é `arn:aws:ec2:availability-zone:instance/instance-id`. Esse formato é diferente do formato de ARN de recurso do EC2.

instance-action

Se a instância spot estiver marcada para ser parada ou terminada pelo Amazon EC2, o item `instance-action` estará presente nos seus metadados de instância. Caso contrário, não estará presente. Você pode recuperar `instance-action` usando o Instance Metadata Service versão 2 (IMDSv2) da seguinte forma.

Use o comando referente ao seu sistema operacional.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

O item `instance-action` especifica a ação e o tempo aproximado (em UTC) em que a ação ocorrerá.

A saída do exemplo a seguir indica o momento em que essa instância será parada.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

A saída do exemplo a seguir indica o momento em que essa instância será terminada.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Se o Amazon EC2 não estiver se preparando para parar ou terminar a instância, ou se você mesmo terminar a instância, `instance-action` não estará presente nos metadados da instância e você receberá um erro HTTP 404 ao tentar recuperá-la.

termination-time

Este item é mantido para compatibilidade com versões anteriores. Use `instance-action` em seu lugar.

Se a instância spot estiver marcada para ser encerrada pelo Amazon EC2 (devido a uma interrupção da instância spot em que o comportamento de interrupção está definido como `terminate` ou devido ao cancelamento de uma solicitação de instância spot persistente), o item `termination-time` estará presente nos metadados da instância. Caso contrário, não estará presente. É possível recuperar `termination-time` usando o IMDSv2 da seguinte maneira.

Use o comando referente ao seu sistema operacional.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/
latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo
 termination_scheduled; fi
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/
termination-time
```

O item `termination-time` especifica o horário aproximado em UTC em que a instância receberá a sinalização de desligamento. O seguinte é um exemplo de saída.

```
2015-01-05T18:02:00Z
```

Se o Amazon EC2 não estiver se preparando para encerrar a instância (seja porque não há interrupção da instância spot, seja porque o comportamento de interrupção está definido como `stop` ou `hibernate`), ou se você tiver encerrado a instância spot por conta própria, o item `termination-time` não estará presente nos metadados da instância (portanto, você receberá um erro HTTP 404) ou conterá um valor que não corresponde a um valor de tempo.

Se o Amazon EC2 não encerrar a instância, o status da solicitação será definido como `fulfilled`. O valor de `termination-time` permanece nos metadados da instância com o tempo aproximado original, que agora está no passado.

Encontrar Instâncias spot interrompidas

No console, o painel Instâncias exibe todas as instâncias, inclusive Instâncias spot. O ciclo de vida da instância de uma instância spot é `spot`. O estado da instância de uma instância spot é `stopped` ou `terminated`, dependendo do comportamento de interrupção que foi configurado. Para uma instância spot hibernada, o estado da instância é `stopped`.

Para encontrar uma instância spot interrompida usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Aplique o seguinte filtro: Instance lifecycle=spot.
4. Aplique o filtro Instance state=stoped ou Instance state=terminated, dependendo do comportamento de interrupção configurado.
5. Para cada instância spot, na guia Detalhes, em Detalhes da instância, localize a Mensagem de transição de estado. Os códigos a seguir indicam que a instância spot foi interrompida.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`
6. Para obter detalhes adicionais sobre o motivo da interrupção, verifique o código de status da solicitação spot. Para ter mais informações, consulte the section called “Status da solicitação spot”.

Para encontrar instâncias spot interrompidas usando a AWS CLI

É possível listar as Instâncias spot interrompidas usando o comando describe-instances com o parâmetro `--filters`. Para listar apenas os IDs das instâncias na saída, inclua o parâmetro `--query`.

Se o comportamento de interrupção da instância for encerrar as instâncias spot, use o seguinte comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Se o comportamento de interrupção da instância for interromper as instâncias spot, use o seguinte comando:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

Determinar se o Amazon EC2 terminou uma instância spot

Se uma instância spot for terminada, é possível usar o CloudTrail para ver se o Amazon EC2 terminou a instância spot. Em AWS CloudTrail, o nome do evento `BidEvictedEvent` indica que o Amazon EC2 terminou a instância spot.

Para visualizar eventos BidEvictedEvent no CloudTrail

1. Abra o console do CloudTrail em https://console.aws.amazon.com/cloudfront/.
2. No painel de navegação, selecione Event history (Histórico de eventos).
3. No menu suspenso de filtros, escolha Event name (Nome do evento) e, em seguida, no campo de filtro à direita, digite BidEvictedEvent.
4. Selecione BidEvictedEvent na lista resultante e será possível visualizar seus detalhes. Em Event record (Registro de evento), é possível encontrar o ID da instância.

Para ter mais informações sobre o uso de CloudTrail, consulte Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail.

Faturamento para Instâncias spot interrompidas

Quando uma instância spot é interrompida, você recebe uma cobrança pelo uso da instância e do volume do EBS, podendo incorrer em outras da maneira indicada a seguir.

Uso da instância

Quem interrompe a instância spot	Sistema operacional	Interrompida na primeira hora	Interrompida em qualquer hora após a primeira
Se você interromper ou encerrar a instância spot	Windows e Linux (com exceção de SUSE)	Cobrança pelos segundos usados	Cobrança pelos segundos usados
	SUSE	Cobrança pela hora completa, mesmo se você usou somente uma parte da hora	Cobrança pelas horas completas usadas e cobrança por uma hora completa pela hora parcial interrompida
Se o Amazon EC2 interromper a instância spot	Windows e Linux (com exceção de SUSE)	Sem cobrança	Cobrança pelos segundos usados
	SUSE	Sem cobrança	Cobrança pelas horas completas usadas, mas sem cobrança pela hora parcial interrompida

Uso do volume do EBS

Enquanto uma instância spot estiver parada, você será cobrado apenas pelos volumes do EBS, que são preservados.

Com a EC2 Fleet e a frota spot, se houver muitas instâncias interrompidas, será possível exceder o limite de número de volumes do EBS na sua conta.

Outras cobranças

Se a sua instância spot em execução incorrer em cobranças por outros serviços, como transferência de dados, endereços IP elásticos ou uso de outros serviços gerenciados da AWS, você receberá cobranças pelo uso deles. Isso ocorre independentemente de quem interrompe a instância spot ou de quando ela foi interrompida. Mesmo que o uso da instância spot não seja cobrado quando o Amazon EC2 interromper sua instância spot na primeira hora, poderão ocorrer outras cobranças.

Para obter mais informações sobre outras cobranças, consulte Preço sob demanda do Amazon EC2.

Pontuação de posicionamento de spot

O recurso de pontuação de posicionamento de spot recomenda uma região ou zona de disponibilidade da AWS com base nos requisitos de capacidade spot. A capacidade de spot flutua e você não pode ter certeza de que sempre obterá a capacidade de que precisa. Uma pontuação de posicionamento de spot indica a probabilidade de uma solicitação de spot ter êxito em uma região ou zona de disponibilidade.

> **Note**
>
> Uma pontuação de posicionamento de spot não oferece nenhuma garantia em termos de capacidade disponível ou risco de interrupção. Uma pontuação de posicionamento de spot serve apenas como uma recomendação.

Benefícios

É possível usar o recurso de pontuação de posicionamento de spot para o seguinte:

- Para realocar e escalar a capacidade computacional de spot em uma região diferente, conforme necessário, em resposta ao aumento das necessidades de capacidade ou diminuição da capacidade disponível na região atual.
- Para identificar a zona de disponibilidade ideal para executar workloads de zona de disponibilidade única.
- Para simular futuras necessidades de capacidade spot para que você possa escolher uma região ideal para a expansão de suas workloads baseadas em spot.
- Para encontrar uma combinação ideal de tipos de instância para atender às suas necessidades de capacidade spot.

Tópicos

- Custos
- Como funciona a pontuação de posicionamento de spot
- Limitações
- Permissões do IAM necessárias
- Calcular uma pontuação de posicionamento de spot

- Exemplos de configuração

Custos

Não há cobrança adicional pelo uso do recurso de pontuação de posicionamento de spot.

Como funciona a pontuação de posicionamento de spot

Ao usar o recurso de pontuação de posicionamento de spot, primeiramente você especifica os requisitos de computação para suas instâncias spot e, em seguida, o Amazon EC2 retorna as 10 principais regiões ou zonas de disponibilidade nas quais sua solicitação de spot provavelmente vai obter êxito. Cada região ou zona de disponibilidade é pontuada em uma escala de 1 a 10, com 10 indicando que é altamente provável que sua solicitação de spot tenha êxito e 1 indicando que sua solicitação de spot provavelmente não terá êxito.

Para usar o recurso de pontuação de posicionamento de spot, siga estas etapas:

- Etapa 1: especificar seus requisitos de spot
- Etapa 2: filtrar a resposta da pontuação de posicionamento de spot
- Etapa 3: revisar as recomendações
- Etapa 4: usar as recomendações

Etapa 1: especificar seus requisitos de spot

Primeiro, você especifica a capacidade-alvo de spot desejada e seus requisitos de computação, da seguinte forma:

1. Especifique a capacidade-alvo de spot e, opcionalmente, a unidade da capacidade-alvo.

   É possível especificar a capacidade-alvo de spot desejada em termos do número de instâncias ou vCPUs, ou em termos de quantidade de memória em MiB. Para especificar a capacidade-alvo em número de vCPUs ou quantidade de memória, especifique a unidade de capacidade-alvo como `vcpu` ou `memory-mib`. Caso contrário, o padrão é o número de instâncias.

   Ao especificar a capacidade-alvo em termos de número de vCPUs ou quantidade de memória, é possível usar essas unidades ao calcular a capacidade total. Por exemplo, se você quiser usar uma combinação de instâncias de tamanhos diferentes, é possível especificar a capacidade-alvo como um número total de vCPUs. O recurso de pontuação de posicionamento de spot considera

cada tipo de instância na solicitação pelo número de vCPUs e conta o número total de vCPUs em vez do número total de instâncias ao totalizar a capacidade-alvo.

Por exemplo, digamos que você especifique uma capacidade-alvo total de 30 vCPUs e sua lista de tipos de instância consista em c5.xlarge (4 vCPUs), m5.2xlarge (8 vCPUs) e r5.large (2 vCPUs). Para atingir um total de 30 vCPUs, é possívelria obter uma combinação de 2 c5.xlarge (2*4 vCPUs), 2 m5.2xlarge (2*8 vCPUs) e 3 r5.large (3*2 vCPUs).

2. Especifique tipos de instância ou atributos de instância.

   É possível especificar os tipos de instância a serem usados ou especificar os atributos de instância necessários para seus requisitos de computação e deixar o Amazon EC2 identificar os tipos de instância que têm esses atributos. Isso é conhecido como seleção de tipo de instância baseada em atributos.

   Você não pode especificar os tipos de instância e os atributos de instância na mesma solicitação de pontuação de posicionamento de spot.

   Se especificar tipos de instância, você deverá especificar pelo menos três tipos de instância diferentes, caso contrário, o Amazon EC2 retornará uma baixa pontuação de posicionamento de spot. Da mesma forma, se você especificar atributos de instância, eles deverão ser resolvidos como, pelo menos, três tipos de instância diferentes.

Para obter exemplos de maneiras diferentes de especificar seus requisitos de spot, consulte Exemplos de configuração.

Etapa 2: filtrar a resposta da pontuação de posicionamento de spot

O Amazon EC2 calcula a pontuação de posicionamento de spot para cada região ou zona de disponibilidade e retorna as 10 principais regiões ou as 10 principais zonas de disponibilidade nas quais sua solicitação de spot provavelmente terá êxito. O padrão é retornar uma lista de regiões pontuadas. Se você planeja iniciar toda a sua capacidade spot em uma única zona de disponibilidade, será útil solicitar uma lista de zonas de disponibilidade pontuadas.

É possível especificar um filtro de região para restringir as regiões que serão retornadas na resposta.

É possível combinar o filtro de região e uma solicitação de zonas de disponibilidade pontuadas. Dessa forma, as zonas de disponibilidade pontuadas serão restringidas às regiões para filtradas. Para encontrar a zona de disponibilidade com a maior pontuação em uma região, especifique

somente essa região, e a resposta retornará uma lista com as pontuações de todas as zonas de disponibilidade na região.

Etapa 3: revisar as recomendações

A pontuação de posicionamento de spot para cada região ou zona de disponibilidade é calculada com base na capacidade-alvo, na composição dos tipos de instância, nas tendências de uso histórico e atual de spot e na hora em que a solicitação é feita. Como a capacidade spot está constantemente flutuando, a mesma solicitação de pontuação de posicionamento de spot pode produzir pontuações diferentes quando calculada em horas diferentes.

Regiões e zonas de disponibilidade são pontuadas em uma escala de 1 a 10. Uma pontuação de 10 indica que sua solicitação de spot tem alta probabilidade, mas não garantia, de ter êxito. Uma pontuação de 1 indica que sua solicitação de spot tem muito pouca probabilidade de ter êxito. A mesma pontuação pode ser retornada para diferentes regiões ou zonas de disponibilidade.

Se pontuações baixas forem retornadas, será possível editar seus requisitos de computação e recalcular a pontuação. Também é possível solicitar recomendações de pontuação de posicionamento de spot para os mesmos requisitos de computação em diferentes horas do dia.

Etapa 4: usar as recomendações

Uma pontuação de posicionamento de spot só é relevante se a solicitação de spot tiver exatamente a mesma configuração que a configuração de pontuação de posicionamento de spot (capacidade-alvo, unidade de capacidade-alvo e tipos de instância ou atributos de instância) e estiver configurada para usar a estratégia de alocação de `capacity-optimized`. Caso contrário, a probabilidade de obter a capacidade de spot disponível não será alinhada com a pontuação.

Embora uma pontuação de posicionamento de spot sirva como diretriz e nenhuma pontuação garanta que sua solicitação de spot será atendida total ou parcialmente, é possível usar as seguintes informações para obter os melhores resultados:

- Usar a mesma configuração: a pontuação de posicionamento de spot é relevante somente se a configuração da solicitação de spot (capacidade-alvo, unidade da capacidade-alvo e tipos de instância ou atributos de instância) no seu grupo do Auto Scaling, frota do EC2 ou frota spot for a mesma que você inseriu para obter a pontuação de posicionamento de spot.

  Se você usou a seleção de tipo de instância baseada em atributo na solicitação de pontuação de posicionamento de spot, poderá usar a seleção de tipo de instância baseada em atributo para configurar seu grupo do Auto Scaling, frota do EC2 ou frota spot. Para obter mais informações,

consulte Criação de um grupo do Auto Scaling com um conjunto de requisitos nos tipos de instância usados, Seleção de tipo de instância baseada em atributos para frota do EC2, e Seleção de tipo de instância baseada em atributos para frota spot.

> **Note**
>
> Se você especificou sua capacidade-alvo em termos do número de vCPUs ou da quantidade de memória e tiver especificado tipos de instância na configuração de pontuação de posicionamento de spot, observe que não é possível criar essa configuração no grupo do Auto Scaling, frota do EC2 ou frota spot. Em vez disso, é necessário definir manualmente a ponderação de instâncias usando o parâmetro `WeightedCapacity`.

- Usar a estratégia de alocação **`capacity-optimized`**: qualquer pontuação pressupõe que sua solicitação de frota será configurada para usar todas as zonas de disponibilidade (para solicitação de capacidade entre regiões) ou uma só zona de disponibilidade (se estiver solicitando capacidade em uma zona de disponibilidade) e a estratégia `capacity-optimized` de alocação de spot para que sua solicitação de capacidade de spot tenha êxito. Se você usar outras estratégias de alocação, como `lowest-price`, a probabilidade de obter a capacidade de spot disponível não será alinhada com a pontuação.
- Agir assim que tiver uma pontuação: a recomendação de pontuação de posicionamento de spot reflete a capacidade de spot disponível no momento da solicitação, e a mesma configuração pode produzir pontuações diferentes quando calculada em momentos diferentes devido a flutuações na capacidade de spot. Embora uma pontuação de 10 signifique que sua solicitação de capacidade de spot tem alta probabilidade, mas não garantia, de ter êxito, para obter os melhores resultados, recomendamos que você aja assim que tiver a pontuação, imediatamente. Também recomendamos que obtenha uma nova pontuação toda vez que tentar fazer uma solicitação de capacidade.

Limitações

- Limite da capacidade-alvo: o limite de capacidade-alvo da pontuação de posicionamento de spot é baseado em seu uso recente de spot, levando em conta um potencial aumento de uso. Se você não fez uso de spot recentemente, fornecemos para você um limite padrão baixo, alinhado com seu limite de solicitação de spot.
- Limite de configurações de solicitação: podemos limitar o número de novas configurações de solicitação dentro de um período de 24 horas se detectarmos padrões não associados ao uso pretendido do recurso de pontuação de posicionamento de spot. Se você atingir o limite,

poderá repetir as configurações de solicitação que já usou, mas não poderá especificar novas configurações de solicitação até o próximo período de 24 horas.

- Número mínimo de tipos de instância: se especificar tipos de instância, você deverá especificar pelo menos três tipos de instância diferentes, caso contrário, o Amazon EC2 retornará uma baixa pontuação de posicionamento de spot. Da mesma forma, se você especificar atributos de instância, eles deverão ser resolvidos como, pelo menos, três tipos de instância diferentes. Tipos de instância são considerados diferentes se tiverem nomes diferentes. Por exemplo, m5.8xlarge, m5a.8xlarge, and m5.12xlarge são todos considerados diferentes.

Permissões do IAM necessárias

Por padrão, as identidades do IAM (usuários, funções ou grupos) não têm permissão para usar o recurso de pontuação de posicionamento de spot. Para permitir que as identidades do IAM usem o recurso de pontuação de posicionamento de spot, crie uma política do IAM que conceda permissão para usar ação `ec2:GetSpotPlacementScores` da API do EC2. Depois, anexe a política às identidades do IAM que requeiram essa permissão.

O exemplo de política do IAM a seguir concede permissão para usar a ação `ec2:GetSpotPlacementScores` da API do EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como editar uma política do IAM, consulte Edição de políticas do IAM no Guia do usuário do IAM.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Calcular uma pontuação de posicionamento de spot

É possível calcular uma pontuação de posicionamento de spot usando o console do Amazon EC2 ou a AWS CLI.

Tópicos

- Calcule uma pontuação de posicionamento de spot especificando atributos de instância (console)
- Calcule uma pontuação de posicionamento de spot especificando tipos de instância (console)
- Calcule uma pontuação de posicionamento de spot (AWS CLI)

Calcule uma pontuação de posicionamento de spot especificando atributos de instância (console)

Para calcular uma pontuação de posicionamento de spot especificando atributos de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha Spot placement score (Pontuação de posicionamento de spot).
4. Escolha Enter requirements (Inserir requisitos).
5. Em Target capacity (Capacidade-alvo), insira a capacidade desejada em termos do número de instances (instâncias) ou vCPUs, ou quantidade de memory (MiB) (memória).
6. Em Instance type requirements (Requisitos de tipo de instância), para especificar seus requisitos de computação e deixar que o Amazon EC2 identifique os tipos de instância ideais com esses requisitos, escolha Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação).

7. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
8. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
9. Em CPU architecture (Arquitetura da CPU), selecione a arquitetura de instância requisitada.
10. (Opcional) Em Additional instance attributes (Atributos de instância adicionais), é possível, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais uma restrição à solicitação. É possível omitir os atributos adicionais; quando omitidos, os valores padrão são usados. Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores na Referência da linha de comando do Amazon EC2.
11. (Opcional) Para visualizar os tipos de instância com os atributos especificados, expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes). Para excluir os tipos de instância de serem usados na avaliação do posicionamento, selecione as instâncias e escolha Exclude selected instance types (Excluir tipos de instância selecionados).
12. Escolha Load placement scores (Carregar pontuações de posicionamento) e analise os resultados.
13. (Opcional) Para exibir a pontuação de posicionamento de spot para regiões específicas, em Regions to evaluate (Regiões a serem avaliadas), selecione as regiões a serem avaliadas e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).
14. (Opcional) Para exibir a pontuação de posicionamento de spot para as zonas de disponibilidade nas regiões que a ferramenta exibe, marque a caixa de seleção Provide placement scores per Availability Zone (Fornecer pontuação de posicionamento por zona de disponibilidade). Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade.
15. (Opcional) Para editar seus requisitos de computação e obter uma nova pontuação de posicionamento, escolha Edit (Editar), faça os ajustes necessários e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).

Calcule uma pontuação de posicionamento de spot especificando tipos de instância (console)

Para calcule uma pontuação de posicionamento de spot especificando tipos de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Solicitações spot.
3. Escolha Spot placement score (Pontuação de posicionamento de spot).
4. Escolha Enter requirements (Inserir requisitos).
5. Em Target capacity (Capacidade-alvo), insira a capacidade desejada em termos do número de instances (instâncias) ou vCPUs, ou quantidade de memory (MiB) (memória).
6. Em Instance type requirements (Requisitos de tipo de instância), para especificar os tipos de instância a serem usados, escolha Manually select instance types (Selecionar manualmente os tipos de instância).
7. Escolha Select instance types (Selecionar tipos de instância), selecione os tipos de instância a serem usados e escolha Select (Selecionar). Para localizar rapidamente tipos de instância, é possível usar a barra de filtro para filtrar os tipos de instância por diferentes propriedades.
8. Escolha Load placement scores (Carregar pontuações de posicionamento) e analise os resultados.
9. (Opcional) Para exibir a pontuação de posicionamento de spot para regiões específicas, em Regions to evaluate (Regiões a serem avaliadas), selecione as regiões a serem avaliadas e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).
10. (Opcional) Para exibir a pontuação de posicionamento de spot para as zonas de disponibilidade nas regiões que a ferramenta exibe, marque a caixa de seleção Provide placement scores per Availability Zone (Fornecer pontuação de posicionamento por zona de disponibilidade). Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade.
11. (Opcional) Para editar a lista de tipos de instância e obter uma nova pontuação de posicionamento, escolha Edit (Editar), faça os ajustes necessários e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).

Calcule uma pontuação de posicionamento de spot (AWS CLI)

Para calcular uma pontuação de posicionamento de spot

1. (Opcional) Para gerar todos os parâmetros possíveis que podem ser especificados para a configuração de pontuação de posicionamento de spot, use o comando get-spot-placement-scores e o parâmetro `--generate-cli-skeleton`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
```

```
    --generate-cli-skeleton
```

Saída esperada

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
```

```
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
```

```
}
```

2. Crie um arquivo de configuração JSON usando a saída da etapa anterior e configure-o da seguinte forma:

   a. Em `TargetCapacity`, insira a capacidade desejada em termos do número de instâncias ou vCPUs, ou quantidade de memória (MiB).

   b. Em `TargetCapacityUnitType`, insira a unidade para a capacidade-alvo. Se você omitir esse parâmetro, ele assumirá o padrão `units`.

      Valores válidos: `units` (o que se traduz em número de instâncias) | `vcpu` | `memory-mib`

   c. Em `SingleAvailabilityZone`, especifique `true` para uma resposta que retorna uma lista de zonas de disponibilidade pontuadas. Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade. Se você omitir esse parâmetro, ele assumirá o padrão `false`, e a resposta retornará uma lista de regiões pontuadas.

   d. (Opcional) Em `RegionNames`, especifique as regiões que deseja usar como filtro. É necessário especificar o código de região, por exemplo, `us-east-1`.

      Com um filtro de região, a resposta retorna apenas as regiões que você especificou. Se tiver especificado `true` para `SingleAvailabilityZone`, a resposta retornará apenas as zonas de disponibilidade nas regiões que você especificou.

   e. É possível incluir um `InstanceTypes` ou `InstanceRequirements`, mas não ambos na mesma configuração.

      Especifique uma das seguintes opções na configuração de JSON:

      - Para especificar uma lista de tipos de instância, especifique os tipos de instância no parâmetro `InstanceTypes`. Especifique pelo menos três tipos de instância diferentes. Se você especificar apenas um ou dois tipos de instância, a pontuação de posicionamento de spot retornará uma pontuação baixa. Para obter uma lista dos tipos de instância , consulte Tipos de instância do Amazon EC2.
      - Para especificar os atributos da instância para que o Amazon EC2 identifique os tipos de instância que correspondem a esses atributos, especifique os atributos localizados na estrutura `InstanceRequirements`.

        É necessário fornecer valores para `VCpuCount`, `MemoryMiB` e `CpuManufacturers`. É possível omitir os outros atributos; quando omitidos, os valores padrão são usados.

Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores na Referência da linha de comando do Amazon EC2.

Para obter configurações de exemplo, consulte Exemplos de configuração.

3. Para obter a pontuação de posicionamento de spot para os requisitos especificados no arquivo JSON, use o comando get-spot-placement-scores e especifique o nome e o caminho do arquivo JSON usando o parâmetro `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Exemplo de saída se `SingleAvailabilityZone` for definido como `false` ou omitido (se omitido, o padrão `false` será usado); uma lista pontuada de regiões será retornada

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Exemplo de saída se `SingleAvailabilityZone` for definido como `true`; uma lista pontuada de zonas de disponibilidade será retornada

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1"
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3"
        "Score": 6
    },
```

```
    ...
```

Exemplos de configuração

Quando usar a AWS CLI, será possível usar os exemplos de configurações as seguir.

Exemplos de configuração

- Exemplo: especificar tipos de instância e capacidade-alvo
- Exemplo: especificar tipos de instância e capacidade-alvo em termos de memória
- Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos
- Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos e retornar uma lista pontuada de zonas de disponibilidade

Exemplo: especificar tipos de instância e capacidade-alvo

O exemplo de configuração a seguir especifica três tipos de instância diferentes e uma capacidade-alvo de spot de 500 instâncias spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Exemplo: especificar tipos de instância e capacidade-alvo em termos de memória

O exemplo de configuração a seguir especifica três tipos de instância diferentes e uma capacidade-alvo de spot de 500.000 MiB de memória, em que o número de Instâncias spot a serem iniciadas deve fornecer um total de 500.000 MiB de memória.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
```

```
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos

O exemplo de configuração a seguir é configurado para seleção de tipo de instância baseada em atributos e é seguido de um texto explicativo do exemplo de configuração.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Para usar a seleção do tipo de instância baseada em atributo, é necessário incluir a estrutura `InstanceRequirementsWithMetadata` na configuração e especificar os atributos desejados para as Instâncias spot.

No exemplo anterior, os seguintes atributos de instância necessários são especificados:

- `ArchitectureTypes`: o tipo de arquitetura dos tipos de instância deve ser `arm64`.
- `VirtualizationTypes`: o tipo de virtualização dos tipos de instância deve ser `hvm`.
- `VCpuCount`: os tipos de instância devem ter no mínimo 1 e no máximo 12 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no mínimo 512 MiB de memória. Omitindo o parâmetro `Max`, você está indicando que não há limite máximo.

Observe que existem vários outros atributos opcionais que é possível especificar. Para obter a lista de atributos, consulte get-spot-placement-scores na Referência da linha de comando do Amazon EC2.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs, em que o número de instâncias spot a serem iniciadas deve fornecer um total de 5000 vCPUs.

Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos e retornar uma lista pontuada de zonas de disponibilidade

O exemplo de configuração a seguir é configurado para seleção de tipo de instância baseada em atributos. Especificando `"SingleAvailabilityZone": true`, a resposta retornará uma lista de zonas de disponibilidade pontuadas.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Feed de dados da instância spot

Para compreender as cobranças relativas às suas instâncias spot, o Amazon EC2 fornece um feed de dados que descreve o uso que você faz de sua instância spot e a definição de preços. Esse feed de dados é enviado a um bucket do Amazon S3 que você especifica ao assinar um feed de dados.

O feed de dados chega em seu bucket geralmente uma vez por hora, e cada hora de uso geralmente é coberto em um único arquivo de dados. Esses arquivos são compactados (gzip) antes de serem entregues ao seu bucket. O Amazon EC2 pode gravar vários arquivos em uma determinada hora de uso quando os arquivos estiverem muito grandes (por exemplo, quando o conteúdo dos arquivos para a hora ultrapassar 50 MB antes da compactação).

> **Note**
>
> Você só pode criar um feed de dados de instância spot para cada Conta da AWS. Se você não tiver uma instância spot em execução em uma hora específica, não receberá um arquivo de feed de dados nessa hora.

O feed de dados da instância spot é compatível em todas as regiões AWS, exceto China (Pequim), China (Ningxia), AWS GovCloud (EUA) e as regiões que estão desabilitadas por padrão.

Conteúdo

- Nome e formato de arquivo do feed de dados
- Requisitos do bucket do Amazon S3
- Assinar seu feed de dados da instância spot
- Descrever seu feed de dados de instância spot
- Visualização dos dados no feed de dados
- Excluir seu feed de dados de instância spot

Nome e formato de arquivo do feed de dados

O nome de arquivo do feed de dados de instância spot usa o seguinte formato (com a data e a hora em UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Por exemplo, se o nome do bucket for **my-bucket-name** e o prefixo for **my-prefix**, os nomes dos arquivos serão semelhantes ao seguinte:

```
my-bucket-name.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Para obter mais informações sobre os nomes de bucket, consulte Regras de nomeação de bucket no Guia do usuário do Amazon S3.

Os arquivos de feed de dados de instância spot são delimitados por tabulação. Cada linha no arquivo de dados corresponde a uma hora de instância e contém os campos listados na tabela a seguir.

Campo	Descrição
`Timestamp`	O time stamp usado para determinar o preço cobrado pelo uso dessa instância.
`UsageType`	O tipo de uso e instância que está sendo cobrado. Para `m1.small` Instâncias spot, este campo está definido como `SpotUsage` . Para todos os outros tipos de instância, esse campo é definido como `SpotUsage:` {instance-type}. Por exemplo, `SpotUsage:c1.medium` .
`Operation`	O produto que está sendo cobrado. Nas Instâncias spot do Linux, este campo é definido como `RunInstances` . Nas Instâncias spot do Windows, este campo é definido como `RunInstances:0002` . O uso de spot é agrupado de acordo com a zona de disponibilidade.
`InstanceID`	O ID da instância spot que gerou este uso de instância.
`MyBidID`	O ID da solicitação de instância spot que gerou este uso de instância.
`MyMaxPrice`	O preço máximo especificado para essa solicitação de spot.
`MarketPrice`	O preço spot na hora especificada no campo `Timestamp` .
`Charge`	O preço cobrado por este uso de instância.
`Version`	A versão do feed de dados. A versão possível é a 1.0.

Requisitos do bucket do Amazon S3

Ao assinar o feed de dados, especifique um bucket do Amazon S3 pra armazenar os arquivos do feed de dados.

Antes de escolher um bucket do Amazon S3 para o feed de dados, considere o seguinte:

- É necessário ter a permissão `FULL_CONTROL` para o bucket. Se você for o proprietário do bucket, terá essa permissão por padrão. Caso contrário, o proprietário do bucket deve conceder essa permissão à sua Conta da AWS.
- Quando você assina um feed de dados, essas permissões são usadas para atualizar o ACL do bucket a fim de fornecer à conta de feed de dados da AWS a permissão `FULL_CONTROL`. A conta de feed de dados da AWS grava arquivos de feed de dados no bucket. Se sua conta não tiver as permissões necessárias, os arquivos de feed de dados não poderão ser gravados no bucket. Para obter mais informações, consulte Logs enviados ao Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

  > **Note**
  >
  > Se você atualizar o ACL e eliminar as permissões para a conta do feed de dados da AWS, os arquivos de feed de dados não poderão ser gravados no bucket. É necessário assinar novamente o feed de dados para receber arquivos de feed de dados.

- Cada arquivo do feed de dados tem sua própria ACL (separada da ACL do bucket). O proprietário do bucket tem a permissão `FULL_CONTROL` para os arquivos de dados. A conta de feed de dados da AWS tem permissões de leitura e gravação.
- Se você aplicou ACLs desabilitadas aos seus buckets, adicione uma política de buckets que permita que os usuários com controle total gravem no bucket. Para obter mais informações, consulte Review and update bucket policies.
- Se você excluir a assinatura do feed de dados, o Amazon EC2 não removerá as permissões de leitura e gravação para a conta de feed de dados da AWS no bucket nem nos arquivos de dados. Você precisa remover essas permissões por conta própria.
- Use uma chave gerenciada pelo cliente se criptografar seu bucket do Amazon S3 usando criptografia no lado do servidor com uma chave do AWS KMS armazenada no AWS Key Management Service (SSE-KMS). Para obter mais informações, consulte Criptografia no lado do servidor de bucket do Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

> **Note**
>
> Para o feed de dados da instância spot, o recurso que gera os arquivos S3 não é mais o Amazon CloudWatch Logs. Portanto, você deve remover a seção `aws:SourceArn` da política de permissão de bucket do S3 e da política do KMS.

Assinar seu feed de dados da instância spot

Para assinar o feed de dados, use o comando create-spot-datafeed-subscription.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket my-bucket-name \
    [--prefix my-prefix]
```

Exemplo de saída

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "111122223333",
        "Bucket": "my-bucket-name",
        "Prefix": "my-prefix",
        "State": "Active"
    }
}
```

Descrever seu feed de dados de instância spot

Para descrever sua assinatura do feed de dados, use o comando describe-spot-datafeed-subscription .

```
aws ec2 describe-spot-datafeed-subscription
```

Exemplo de saída

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "123456789012",
        "Prefix": "spotdata",
        "Bucket": "my-s3-bucket",
```

```
        "State": "Active"
    }
}
```

Visualização dos dados no feed de dados

No AWS Management Console, abra o AWS CloudShell. Use o comando s3 sync a seguir para obter os arquivos .gz do bucket do S3 para o feed de dados e armazená-los na pasta que você especificar.

```
aws s3 sync s3://my-s3-bucket ./data-feed
```

Para exibir o conteúdo de um arquivo .gz, acesse a pasta em que você armazenou o conteúdo do bucket do S3.

```
cd data-feed
```

Use o comando ls para visualizar os nomes dos arquivos. Use o comando zcat com o nome do arquivo para exibir o conteúdo do arquivo compactado. O comando a seguir é um exemplo.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

O seguinte é um exemplo de saída.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Excluir seu feed de dados de instância spot

Para excluir o feed de dados, use o comando delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

Cotas de instâncias spot

Há cotas para o número de instâncias spot em execução e as solicitações de instâncias spot pendentes por Conta da AWS por região. Depois que uma solicitação de instância spot pendente é

atendida, a solicitação não conta mais para a cota porque a instância em execução é contabilizada na cota.

As cotas de instância spot são gerenciadas em termos do número de unidades de processamento central virtuais (vCPUs) que as instâncias spot em execução estão usando ou usarão até o atendimento de solicitações de instância spot abertas. Se você encerrar as instâncias spot, mas não cancelar as solicitações de instância spot, as solicitações serão contabilizadas em relação à cota de vCPU da instância spot até que o Amazon EC2 detecte os encerramentos de instância spot e feche as solicitações.

Fornecemos os seguintes tipos de cota para instâncias spot:

- Todas as solicitações de instância spot DL
- Todas as solicitações de instância spot F
- Todas as solicitações de instância spot G e VT
- Todas as solicitações de instância spot Inf
- Todas as solicitações de instância spot P
- Todas as solicitações de instância spot padrão (A, C, D, H, I, M, R, T, Z)
- Todas as solicitações de instância spot Trn
- Todas as solicitações de instância spot X

Cada tipo de cota especifica o número máximo de vCPUs para uma ou mais famílias de instâncias. Para obter informações sobre as diferentes famílias, gerações e tamanhos de instâncias, consulte Tipos de instância do Amazon EC2.

É possível iniciar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação. Por exemplo: com uma cota de solicitações de todas instâncias spotpadrão de 256 vCPUs, é possível solicitar 32 instâncias spot `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias spot `c5.4xlarge` (16 x 16 vCPUs).

Tarefas

- Monitorar cotas e uso de instâncias spot
- Solicitar um aumento da cota

Monitorar cotas e uso de instâncias spot

É possível visualizar e gerenciar suas cotas de instância spot usando o seguinte:

- A página Service quotas (Cotas de serviços) do Amazon EC2 no console do Service Quotas
- O get-service-quota da AWS CLI

Para obter mais informações, consulte Service Quotas do Amazon EC2 e Viewing service quotas no Guia do usuário do Service Quotas.

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em relação às suas cotas. Também é possível configurar alarmes para alertar quando estiver chegando próximo da cota. Para obter mais informações, consulte Alarmes do Service Quotas e do Amazon CloudWatch no Guia do usuário do Service Quotas.

Solicitar um aumento da cota

Mesmo que o Amazon EC2 aumente automaticamente suas cotas de instância spot com base em seu uso, é possível solicitar um aumento de cota, se for o caso. Por exemplo, se você pretende lançar mais Instâncias spot do que a cota atual permite, solicite um aumento de cota. Também é possível solicitar um aumento de cota se você enviar uma solicitação de instância spot e receber uma mensagem de erro `Max spot instance count exceeded`. Para solicitar aumento de cota, use o console do Service Quotas descrito em Service Quotas do Amazon EC2.

Instâncias expansíveis

Os tipos de instância T são instâncias de desempenho expansível. Se você executar as Instâncias spot usando um tipo de instância expansível e planejar usar as instâncias spot expansíveis imediatamente e por um breve período, sem tempo ocioso para acumular créditos de CPU, recomendamos iniciá-las no modo padrão para evitar pagar custos mais elevados. Se executar as Instâncias spot expansíveis no modo ilimitado e esgotar a CPU imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para expansão. Caso contrário, pagar por créditos excedentes torna a as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para ter mais informações, consulte Quando usar o modo ilimitado versus CPU fixa.

As instâncias T2, quando configuradas no modo Padrão, recebem créditos de inicialização. As instâncias T2 são as únicas instâncias de performance expansível que recebem créditos de

inicialização. Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o modo Ilimitado para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Dedicated Hosts

Um host dedicado do Amazon EC2 é um servidor físico totalmente dedicado para seu uso. Como opção, você pode compartilhar a capacidade da instância com outras contas da AWS. Para obter mais informações, consulte Trabalhar com Hosts dedicados compartilhado.

Os hosts dedicados fornecem visibilidade e controle sobre o posicionamento de instância, além de compatibilidade com afinidade ao host. Isso significa que você pode iniciar e executar instâncias em hosts específicos e garantir que as instâncias sejam executadas somente em hosts específicos. Para ter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade.

O hosts dedicados fornecem compatibilidade abrangente com o modelo traga a sua própria licença (BYOL). Eles permitem que você use suas licenças de software existentes por soquete, por núcleo ou por VM, incluindo o Windows Server, o SQL Server, o SUSE Linux Enterprise Server, o Red Hat Enterprise Linux ou outras licenças de software vinculadas a VMs, soquetes ou núcleos físicos, de acordo com os termos de sua licença.

Se você precisar que suas instâncias sejam executadas em hardware dedicado, mas não precisar de visibilidade ou controle sobre o posicionamento das instâncias e não precisar usar licenças de software por soquete ou por núcleo, avalie a possibilidade de usar instâncias dedicadas. É possível usar instâncias dedicadas e hosts dedicados para iniciar instâncias do Amazon EC2 em servidores físicos dedicados. Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, há algumas diferenças básicas entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Servidor físico dedicado	Servidor físico com capacidade de instância totalmente dedicada para seu uso.	Um servidor físico dedicado a uma única conta de cliente.

	Dedicated Host	Dedicated Instance
Compartilhamento de capacidade de instância	Pode compartilhar a capacidade de instância com outras contas.	Sem compatibilidade
Faturamento	faturamento por host	Faturamento por instância
Visibilidade de soquetes, núcleos e ID de host	Fornece visibilidade do número de soquetes e núcleos físicos	Sem visibilidade
Afinidade de hosts e instâncias	permite implantar de forma consistente suas instâncias no mesmo servidor físico com o momento	Sem suporte
Posicionamento direcionado de instâncias	Proporciona visibilidade e controle adicionais sobre como as instâncias são colocadas em um servidor físico	Não suportado
Recuperação automática de instâncias	Compatível. Para ter mais informações, consulte Recuperação do host.	Compatível
Traga sua própria licença (BYOL)	Compatível	Suporte parcial *
Reservas de capacidade	Não compatível	Compatível

* O Microsoft SQL Server com Mobilidade de Licenças por meio do Software Assurance e as licenças do Windows Virtual Desktop Access (VDA) podem ser usadas com Instância dedicada.

Para obter mais informações sobre as instâncias dedicadas, consulte Dedicated Instances.

Conteúdo

- Configurações de capacidade de instância
- Traga sua própria licença
- Definição de preço e faturamento
- Instâncias T3 expansíveis em hosts dedicados
- Restrições do Hosts dedicados
- Como trabalhar com o Hosts dedicados
- Trabalhar com Hosts dedicados compartilhado
- Hosts dedicados no AWS Outposts
- Recuperação do host
- Manutenção de host
- Monitorar alterações de configuração

Configurações de capacidade de instância

Os hosts dedicados oferecem suporte a diferentes configurações (núcleos físicos, sockets e vCPUs) que permitem executar instâncias de famílias e tamanhos diferentes.

Ao alocar um host dedicado em sua conta, você poderá escolher uma configuração que ofereça suporte a um tipo de instância único ou a vários tipos de instância dentro da mesma família de instâncias. O número de instâncias podem ser executadas em um host depende da configuração escolhida.

Conteúdo

- Suporte a um tipo de instância único
- Suporte a vários tipos de instância

Suporte a um tipo de instância único

É possível alocar um host dedicado que ofereça suporte somente um tipo de instância. Com essa configuração, todas as instâncias executadas no host dedicado devem ser do mesmo tipo da instância especificada no momento da alocação do host.

Por exemplo, é possível alocar um host que ofereça suporte somente ao tipo de instância `m5.4xlarge`. Nesse caso, somente instâncias `m5.4xlarge` poderão ser executadas nesse host.

O número de instâncias que é possível iniciar no host depende do número de núcleos físicos fornecidos pelo host e do número de núcleos consumidos pelo tipo de instância especificado. Por exemplo, ao alocar um host para instâncias `m5.4xlarge`, tenha em mente que o host fornece 48 núcleos físicos e cada instância `m5.4xlarge` consome 8 núcleos físicos. Isso significa que é possível iniciar até 6 instâncias nesse host (48 núcleos físicos/8 núcleos por instância = 6 instâncias).

Suporte a vários tipos de instância

É possível alocar um host dedicado que ofereça suporte a vários tipos de instância da mesma família de instâncias. Isso permite que executar diferentes tipos de instância no mesmo host, desde que elas sejam da mesma família de instâncias e o host tenha capacidade de instância suficiente.

Por exemplo, é possível alocar um host que ofereça suporte a diferentes tipos de instância dentro da família de instâncias `R5`. Nesse caso, você poderá iniciar qualquer combinação de tipos de instância `R5`, como `r5.large`, `r5.xlarge`, `r5.2xlarge` er`5.4xlarge`, nesse host até atingir a capacidade do núcleo físico do host.

As seguintes famílias de instâncias são compatíveis com hosts dedicados com suporte a vários tipos de instância:

- Uso geral:A1, M5, M5n, M6i e T3
- Otimizadas para computação: C5, C5n e C6i
- Otimizadas para memória:R5, R5n e R6i

O número de instâncias que é possível executar no host depende do número de núcleos físicos fornecidos pelo host e do número de núcleos consumidos por cada tipo de instância executado no host. Por exemplo, se você alocar um host `R5`, que fornece 48 núcleos físicos, e executar duas instâncias `r5.2xlarge` (4 núcleos x 2 instâncias) e três instâncias `r5.4xlarge` (8 núcleos x 3 instâncias), essas instâncias consumirão um total de 32 núcleos. Assim, você poderá executar qualquer combinação de instâncias `R5`, desde que não excedam os 16 núcleos restantes.

No entanto, para cada família de instâncias, há um limite no número de instâncias que podem ser executadas para cada tamanho de instância. Por exemplo, um host dedicado `R5` oferece suporte a até 2 instâncias `r5.8xlarge`, as quais usam 32 dos núcleos físicos. Nesse caso, instâncias `R5` adicionais menores podem ser usadas para preencher o host até a capacidade do núcleo ser

atingida. Para obter o número de tamanhos de instância válidos para cada família de instâncias, consulte a Tabela de configuração de hosts dedicados.

A tabela a seguir mostra exemplos de combinações de tipos de instâncias.

Família de instâncias	Combinações de exemplo de tamanhos de instância
R5	• Exemplo 1: 4 x r5.4xlarge + 4 x r5.2xlarge • Exemplo 2: 1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large
C5	• Exemplo 1: 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge • Exemplo 2: 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large
M5	• Exemplo 1: 4 x m5.4xlarge + 4 x m5.2xlarge • Exemplo 2: 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large

Considerações

Lembre-se do seguinte ao trabalhar com hosts dedicados que oferecem suporte a vários tipos de instâncias:

- Com hosts dedicados do tipo N, como C5n, M5n e R5n, não é possível combinar tamanhos de instâncias menores (`2xlarge` e menores) com tamanhos de instância maiores (`4xlarge` e maiores, incluindo `metal`). Se você precisar de tamanhos de instância menores e maiores em hosts dedicados do tipo N ao mesmo tempo, será necessário alocar hosts separados para os tamanhos de instância menores e maiores.

- Recomendamos iniciar primeiro os tamanhos de instância maiores e, em seguida, preencher a capacidade de instâncias restante com tamanhos de instância menores conforme necessário.

Traga sua própria licença

O Hosts dedicados permite usar suas licenças de software por VM, por núcleo e por soquete existentes. Quando você leva sua própria licença, é responsável por gerenciar as próprias licenças. No entanto, o Amazon EC2 tem recursos que ajudam você a manter a conformidade com a licença, como afinidade de instâncias e posicionamento direcionado.

Estas são as etapas gerais para trazer sua própria imagem de máquina com licença por volume para o Amazon EC2.

1. Verifique se os termos de licença que regem o uso de suas imagens de máquina permitem o uso de um ambiente de nuvem virtualizado. Para obter mais informações sobre o Licenciamento da Microsoft, consulte Amazon Web Services e Licenciamento da Microsoft.
2. Depois de verificar se sua imagem de máquina pode ser usada no Amazon EC2, importe-a com o VM Import/Export. Para obter informações sobre como importar sua imagem de máquina, consulte o Manual do usuário do VM Import/Export.
3. Depois de importar a imagem de máquina, será possível executar instâncias dela no Hosts dedicados ativo na sua conta.
4. Ao executar essas instâncias, dependendo do sistema operacional, talvez seja necessário ativar essas instâncias em seu próprio servidor KMS (por exemplo, Windows Server ou Windows SQL Server). Não é possível ativar a AMI do Windows importada no servidor Amazon Windows KMS.

> **Note**
>
> Para controlar como as imagens são usadas na AWS, ative a gravação de host no AWS Config. É possível usar o AWS Config para gravar alterações de configuração em um host dedicado e usar a saída como fonte de dados para geração de relatórios de licenças. Para ter mais informações, consulte Monitorar alterações de configuração.

Definição de preço e faturamento

O preço de um Host dedicado varia de acordo com a opção de pagamento.

Opções de pagamento

- Hosts dedicados sob demanda
- Dedicated Host Reservations
- Savings Plans
- Definição de preço para o Windows Server no Hosts dedicados

Hosts dedicados sob demanda

O faturamento sob demanda é automaticamente ativado quando você aloca um Host dedicado à sua conta.

O preço sob demanda para um Host dedicado varia por família de instância e por região. É cobrado por segundo (com mínimo de 60 segundos) por Host dedicado ativo, independentemente da quantidade ou do tamanho das instâncias que você optar por executar nele. Para obter mais informações sobre a definição de preço sob demanda, consulte Amazon EC2 Hosts dedicados On-Demand Pricing (Definição de preço sob demanda).

É possível liberar um Host dedicado sob demanda a qualquer momento para parar de acumular cobranças para ele. Para obter informações sobre como liberar um Host dedicado, consulte Liberar Hosts dedicados.

Dedicated Host Reservations

Os Reservas de hosts dedicados fornecem um desconto de faturamento em comparação com a execução de Hosts dedicados sob demanda. Há três opções de pagamento disponíveis para as reservas:

- Sem pagamento adiantado — as reservas sem pagamento adiantado fornecem um desconto no uso do Host dedicado durante um período de vigência e não requerem pagamento adiantado. Disponível para períodos de vigência de um e três anos. Apenas algumas famílias de instâncias oferecem suporte para o período de vigência de três anos para a opção Sem reservas antecipadas.
- Pagamento adiantado parcial — deve ser feito o pagamento adiantado de uma parte da reserva, e as horas restantes do período de vigência são cobradas com uma taxa com desconto. Disponível para períodos de vigência de um e três anos.

- Pagamento integral adiantado — fornece o menor preço. Disponível para períodos de vigência de um e três anos e abrange todo o custo do período antecipadamente, sem nenhuma outra cobrança futura.

É necessário ter Hosts dedicados ativos em sua conta para poder comprar reservas. Cada reserva pode cobrir um ou mais hosts que oferecem suporte para a mesma família de instâncias em uma única zona de disponibilidade. As reservas são aplicadas à família da instância do host e não ao tamanho da instância. Se você tiver três Hosts dedicados com diferentes tamanhos de instâncias (`m4.xlarge`, `m4.medium` e `m4.large`), poderá associar uma única reserva `m4` a todos esses Hosts dedicados. A família de instâncias e a zona de disponibilidade da reserva devem corresponder aos hosts dedicados aos quais você quer se associar.

Quando uma reserva for associada a um Host dedicado, o Host dedicado não poderá ser liberado até que o prazo da reserva termine.

Para obter mais informações sobre a definição de preço de reservas, consulte Definição de preço de Hosts dedicados do Amazon EC2.

Savings Plans

Savings Plans são um modelo de definição de preço flexível que oferece economias significativas em Instâncias on-demand. Com o Savings Plans, você se compromete com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos. Isso oferece a flexibilidade de usar Hosts dedicados que melhor atendam às suas necessidades e continuar economizando dinheiro, em vez de se comprometer com um Host dedicado específico. Para obter mais informações, consulte o Guia do usuário do AWS Savings Plans.

> **Note**
>
> Savings Plans não são compatíveis com hosts dedicados `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, e `u-24tb1.metal`.

Definição de preço para o Windows Server no Hosts dedicados

Conforme os termos de licenciamento da Microsoft, é possível trazer suas licenças de Windows Server e SQL Server para o Hosts dedicados. Não há cobrança adicional para uso de software caso você opte por trazer as próprias licenças.

Além disso, também é possível usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados. Isso é comum para cenários nos quais você tem licenças do SQL Server qualificadas para execução no Hosts dedicados, mas precisa do Windows Server para executar a workload do SQL Server. As AMIs do Windows Server fornecidas pela Amazon são compatíveis somente com os tipos de instância da geração atual. Para obter mais informações, consulte Amazon EC2 Dedicated Hosts Pricing (Definição de preço de hosts dedicados do Amazon EC2).

Instâncias T3 expansíveis em hosts dedicados

Hosts dedicados são compatíveis com instâncias expansíveis T3. As instâncias T3 apresentam um bom custo-benefício para usar seu software de licença BYOL elegível em hardware dedicado. O menor espaço de vCPU das instâncias T3 permite consolidar seus workloads em menos hosts e maximizar a utilização da licença por núcleo.

Os hosts dedicados T3 são mais adequados para executar o software BYOL com utilização de CPU baixa a moderada. Isso inclui licenças de software qualificadas por soquete, por núcleo ou por VM, como Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux e Oracle Database. Exemplos de workloads adequados a hosts dedicados T3 são bancos de dados pequenos e médios, desktops virtuais, ambientes de desenvolvimento e teste, repositórios de código e protótipos de produtos. Os hosts dedicados T3 não são recomendados para workloads com alta utilização sustentada da CPU ou para workloads que apresentem expansãos de CPU correlacionadas simultaneamente.

As instâncias T3 em hosts dedicados usam o mesmo modelo de crédito que as instâncias T3 em hardware de locação compartilhada. No entanto, eles são compatíveis apenas com o modo de crédito `standard`, não com o modo de crédito `unlimited`. No modo `standard`, instâncias T3 em hosts dedicados ganham, gastam e acumulam créditos da mesma forma que instâncias expansíveis em hardware de locação compartilhada. Elas fornecem performance de CPU de linha de base com capacidade de expansão acima do nível da linha de base. Para expansãos acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Quando os créditos acumulados estão esgotados, a utilização da CPU é reduzida para o nível de linha de base. Para mais informações sobre o modo `standard`, consulte Como funcionam as instâncias expansíveis padrão.

Os hosts dedicados T3 oferecem suporte a todos os recursos oferecidos pelos hosts dedicados do Amazon EC2, incluindo vários tamanhos de instância em um único host, grupos de recursos de host e BYOL.

Tamanhos e configurações de instância T3 compatíveis

Os hosts dedicados T3 executam instâncias T3 expansíveis de uso geral que compartilham recursos de CPU do host, fornecendo uma performance de CPU de linha de base e a capacidade de expansão para um nível mais alto quando necessário. Isso permite que os hosts dedicados T3, que têm 48 núcleos, suportem até no máximo 192 instâncias por host. Para utilizar os recursos do host de forma eficiente e fornecer a melhor performance de instância, o algoritmo de posicionamento de instância do Amazon EC2 calcula automaticamente o número de instâncias e combinações de tamanho de instância compatíveis que podem ser iniciadas no host.

Os hosts dedicados T3 oferecem suporte a vários tipos de instância no mesmo host. Todos os tamanhos de instâncias T3 são compatíveis em um host dedicado. É possível executar diferentes combinações de instâncias T3 até o limite de CPU do host.

A tabela a seguir lista os tipos de instância compatíveis, resume a performance de cada tipo de instância e indica o número máximo de instâncias de cada tamanho que pode ser lançado.

Tipo de instâ	vCPUs	Memória (GiB)	Utilização da linha de base de CPU por vCPU	Expansão da largura de banda da rede (Gbps)	Expansão da largura de banda da Amazon EBS (Mbps)	Número máximo de instâncias por host dedicado
t3.na	2	0,5	5%	5	Até 2.085	192
t3.m	2	1	10%	5	Até 2.085	192
t3.sn	2	2	20%	5	Até 2.085	192
t3.m	2	4	20%	5	Até 2.085	192
t3.la	2	8	30%	5	2.780	96
t3.xl	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Monitorar a utilização da CPU para hosts dedicados T3

É possível usar a métrica `DedicatedHostCPUUtilization` do Amazon CloudWatch para monitorar a utilização da vCPU de um host dedicado. A métrica está disponível no namespace `EC2` e na dimensão `Per-Host-Metrics`. Para ter mais informações, consulte Métricas de host dedicado.

Restrições do Hosts dedicados

Antes de alocar Hosts dedicados, observe as seguintes limitações e restrições:

- Para executar o RHEL, o SUSE Linux e o SQL Server no Hosts dedicados, é necessário trazer suas próprias AMIs. As AMIs do RHEL, SUSE Linux e SQL Server oferecidas pela AWS ou disponíveis no AWS Marketplace não podem ser usadas com os hosts dedicados. Para obter mais informações sobre como criar sua própria AMI, consulte Traga sua própria licença.

  Essa restrição não se aplica a hosts alocados para instâncias de alta memória (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`). As AMIs do RHEL e do SUSE Linux oferecidas pela AWS ou disponíveis no AWS Marketplace podem ser usadas com esses hosts.
- Há um limite para o número de hosts dedicados em execução por família de instâncias por conta da AWS por região. As cotas se aplicam somente às instâncias em execução. Se a sua instância estiver pendente, sendo interrompida ou tiver sido interrompida, ela não será contabilizada para a sua cota. Para ver as cotas da sua conta ou solicitar aumento da cota, use o console do Service Quotas.
- As instâncias que são executadas em um Host dedicado somente podem ser iniciadas em uma VPC.
- Grupos de Auto Scaling são compatíveis ao usar um modelo de execução que especifica um grupo de recursos de host. Para obter mais informações, consulte Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.
- Não há suporte para instâncias do Amazon RDS.
- O nível de uso gratuito da AWS não está disponível para hosts dedicados.
- O controle de posicionamento de instância se refere ao gerenciamento de execuções de instâncias em Hosts dedicados. Não é possível iniciar o Hosts dedicados em grupos de posicionamento.
- Se você alocar um host para um tipo de instância virtualizada, não poderá modificar o tipo de instância para um tipo de instância `.metal` depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.large`, não poderá modificar o tipo de instância para `m5.metal`.

Da mesma forma, se você alocar um host para um tipo de instância `.metal`, não poderá modificar o tipo de instância para um tipo de instância virtualizada depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.metal`, não poderá modificar o tipo de instância para `m5.large`.

Como trabalhar com o Hosts dedicados

Para usar um Host dedicado, primeiro aloque os hosts a serem usados na sua conta. Depois, execute instâncias nos hosts especificando a locação do host da instância. É necessário selecionar um host específico no qual executar a instância ou permitir que ela seja executada em qualquer host que tenha o posicionamento automático habilitado e corresponda ao seu tipo de instância. Quando uma instância é interrompida e reiniciada, a configuração Afinidade de host determina se ela será reiniciada no mesmo host ou em um host diferente.

Se você não precisar mais de um host sob demanda, poderá interromper as instâncias em execução no host, direcioná-las para execução em um host diferente e liberar o host.

Hosts dedicados também estão integrados ao AWS License Manager. Com o License Manager, é possível criar um grupo de recursos de host, que é uma coleção de Hosts dedicados gerenciados como uma única entidade. Ao criar um grupo de recursos de host, especifique as preferências de gerenciamento de host, como alocação automática e liberação automática, para os Hosts dedicados. Isso permite que você execute instâncias em Hosts dedicados sem alocar e gerenciar manualmente esses hosts. Para obter mais informações, consulte Grupos de recursos de host no Guia do usuário do AWS License Manager.

Tópicos

- Alocar Hosts dedicados
- Execute instâncias em um Host dedicado.
- Execute instâncias em um grupo de recursos de host.
- Noções básicas sobre posicionamento automático e afinidade
- Modificar posicionamento automático de Host dedicado
- Modificar os tipos de instância compatíveis
- Modificar locação e da afinidade de instâncias
- Visualização do Hosts dedicados
- Marcação de Hosts dedicados

- Monitorar Hosts dedicados
- Liberar Hosts dedicados
- Comprar Reservas de hosts dedicados
- Visualizar reservas de Host dedicado
- Atribuir tag de Reservas de hosts dedicados

Alocar Hosts dedicados

Para começar a usar o Hosts dedicados, é necessário alocar o Hosts dedicados à sua conta usando o console do Amazon EC2 ou as ferramentas da linha de comando. Depois da alocação do Host dedicado, a capacidade do Host dedicado é imediatamente disponibilizada em sua conta, e é possível começar a executar instâncias no Host dedicado.

Ao alocar um host dedicado em sua conta, você poderá escolher uma configuração que ofereça suporte a um tipo de instância único ou a vários tipos de instância dentro da mesma família de instâncias. O número de instâncias podem ser executadas no host depende da configuração escolhida. Para ter mais informações, consulte Configurações de capacidade de instância.

Console

Como alocar um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Hosts dedicados e Allocate Host dedicado (Alocar Host dedicado).
3. Em Instance family (Família de instâncias), escolha a família de instâncias do Host dedicado.
4. Especifique se o Host dedicado oferece suporte a vários tipos de instância na família de instâncias selecionada ou a um único tipo específico de instância. Faça uma das coisas a seguir.

   - Para configurar o Host dedicado para oferecer suporte a vários de tipos de instância na família de instâncias selecionada, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar) Isso permitirá executar diferentes tipos de instância da família de instâncias selecionada no Host dedicado. Por exemplo, se você escolher a família de instâncias `m5` e escolher essa opção, poderá executar instâncias `m5.xlarge` e `m5.4xlarge` no Host dedicado.

- Para configurar o Host dedicado a fim de oferecer suporte a um tipo de instância na família de instâncias selecionada, desmarque Support multiple instance types (Oferecer suporte a vários tipos de instância) e, em Instance type (Tipo de instância), escolha o tipo de instância ao qual oferecer suporte. Isso permite que você execute um único tipo de instância no Host dedicado. Por exemplo, se você escolher essa opção e especificar `m5.4xlarge` como o tipo de instância compatível, poderá executar apenas instâncias `m5.4xlarge` no Host dedicado.

5. Em Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual o Host dedicado será alocado.
6. Para permitir que o Host dedicado aceite lançamentos de instância não direcionada compatíveis com o tipo de instância, para Instance auto-placement (Autoposicionamento da instância), selecione Enable (Habilitar). Para obter mais informações sobre posicionamento automático, consulte Noções básicas sobre posicionamento automático e afinidade.
7. Para habilitar a recuperação do host para o Host dedicado, em Host recovery (Recuperação do host), selecione Enable (Habilitar). Para ter mais informações, consulte Recuperação do host.
8. Em Quantity (Quantidade), insira o número de Hosts dedicados a ser alocado.
9. (Opcional) Escolha Adicionar nova tag e digite uma chave de tag e um valor de tag.
10. Escolha Allocate.

AWS CLI

Como alocar um Host dedicado

Use o comando allocate-hosts da AWS CLI. O comando a seguir aloca um Host dedicado que oferece suporte a vários tipos de instância da família de instâncias `m5` na zona de disponibilidade `us-east-1a`. O host também tem a recuperação do host habilitada e o posicionamento automático desabilitado.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --
auto-placement "off" --host-recovery "on" --quantity 1
```

O comando a seguir aloca um Host dedicado que oferece suporte a execuções de instâncias `m4.large` não direcionadas na zona de disponibilidade `eu-west-1a`, habilita recuperação do host e aplica uma tag com uma chave de `purpose` e um valor de `production`.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Como alocar um Host dedicado

Use o comando New-EC2Host do AWS Tools for Windows PowerShell. O comando a seguir aloca um Host dedicado que oferece suporte a vários tipos de instância da família de instâncias `m5` na zona de disponibilidade `us-east-1a`. O host também tem a recuperação do host habilitada e o posicionamento automático desabilitado.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -
AutoPlacement Off -HostRecovery On -Quantity 1
```

Os comandos a seguir alocam um Host dedicado que oferece suporte a execuções de instâncias `m4.large` não destinadas na zona de disponibilidade `eu-west-1a`, habilitam recuperação do host e aplicam uma tag com uma chave de `purpose` e um valor de `production`.

O parâmetro `TagSpecification` usado para marcar um Host dedicado na criação requer um objeto que especifique o tipo de recurso a ser marcado, a chave e o valor da tag. Os comandos a seguir criam o objeto necessário.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

O comando a seguir aloca o Host dedicado e aplica a tag especificada no objeto `$tagspec`.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Execute instâncias em um Host dedicado.

Depois de alocar um Host dedicado, é possível executar instâncias nele. Você não pode executar instâncias com locação de `host` se não tiver Hosts dedicados ativos com capacidade suficiente disponível para o tipo de instância que está executando.

> **Tip**
>
> Para hosts dedicados compatíveis com vários tamanhos de instâncias, recomendamos executar primeiro os tamanhos de instância maiores e preencher a capacidade de instâncias restante com os tamanhos de instância menores, conforme necessário.

Antes de executar as instâncias, observe as limitações. Para ter mais informações, consulte Restrições do Hosts dedicados.

É possível executar uma instância em um Host dedicado usando os métodos a seguir.

Console

Para executar uma instância em um Host dedicado específico na página de Hosts dedicados

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Dedicated Hosts (Hosts dedicados), selecione um host e escolha Actions (Ações), Launch Instance(s) onto Host (Iniciar instâncias no host).
4. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.

   > **Note**
   >
   > AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.

5. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.

   > **Note**
   >
   > Se o Host dedicado oferecer suporte a um único tipo de instância, o tipo de instância com suporte será selecionado por padrão e não poderá ser alterado.
   > Se o Host dedicado oferecer suporte a vários tipos de instância, será necessário selecionar um tipo de instância na família de instâncias com suporte de acordo com a capacidade de instância disponível do Host dedicado. Recomendamos que

você execute primeiro os tamanhos de instância maiores e preencha a capacidade restante da instância com os tamanhos de instância menores, conforme necessário.

6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
7. Na seção Advanced details (Detalhes avançados), em Tenancy affinity (Afinidade de locação), faça uma das seguintes opções:

   - Selecione Off (Desativar): a instância será iniciada no host especificado, mas não é garantido que seja iniciada no mesmo host dedicado se for interrompida.
   - Selecione o ID do host dedicado: se for interrompida, a instância sempre será reiniciada nesse host específico.

   Para obter mais informações sobre afinidade, consulte Noções básicas sobre posicionamento automático e afinidade.

   > **Note**
   >
   > As opções Tenancy (Locação) e Host são pré-configuradas com base no host selecionado.

8. Configure as demais opções da instância conforme necessário. Para ter mais informações, consulte Iniciar uma instância usando parâmetros definidos.
9. Escolha Iniciar instância.

Para executar uma instância em um Host dedicado usando o assistente de execução de instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.

   > **Note**
   >
   > AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.

4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.
5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
6. Na seção Advanced details (Detalhes avançados), faça o seguinte:

   a. Em Tenancy (Locação), escolha Dedicated Host (Host dedicado).
   b. Em Target host by (Visar host por), selecione Host ID (ID do host).
   c. Em Host ID (ID do host), selecione o host no qual a instância será iniciada.
   d. Em Tenancy affinity (Afinidade de locação), faça uma destas opções:

      - Selecione Off (Desativar): a instância será iniciada no host especificado, mas não é garantido que seja iniciada no mesmo host dedicado se for interrompida.
      - Selecione o ID do host dedicado: se for interrompida, a instância sempre será reiniciada nesse host específico.

      Para obter mais informações sobre afinidade, consulte Noções básicas sobre posicionamento automático e afinidade.
7. Configure as demais opções da instância conforme necessário. Para ter mais informações, consulte Iniciar uma instância usando parâmetros definidos.
8. Escolha Iniciar instância.

AWS CLI

Como iniciar uma instância em um Host dedicado

Use o comando run-instances da AWS CLI e especifique a afinidade da instância, a locação e o host no parâmetro de solicitação `Placement`.

PowerShell

Como iniciar uma instância em um Host dedicado

Use o comando New-EC2Instance do AWS Tools for Windows PowerShell e especifique a afinidade da instância, a locação e o host no parâmetro de solicitação `Placement`.

Execute instâncias em um grupo de recursos de host.

Quando você executa uma instância em um grupo de recursos de host que tem um Host dedicado com capacidade de instância disponível, o Amazon EC2 executa a instância nesse host. Se o

grupo de recursos de host não tiver um host com capacidade de instância disponível, o Amazon EC2 alocará automaticamente um novo host no grupo de recursos de host e, depois, executará a instância nesse host. Para obter mais informações, consulte Grupos de recursos de host no Guia do usuário do AWS License Manager.

Requisitos e limites

- É necessário associar uma configuração de licença baseada em núcleo ou soquete à AMI.
- Não é possível usar as AMIs do SQL Server, do SUSE ou do RHEL fornecidas pelo Amazon EC2 com o Hosts dedicados.
- Você não pode segmentar um host específico escolhendo um ID de host e não é possível habilitar a afinidade de instâncias ao executar uma instância em um grupo de recursos de host.

É possível executar uma instância em um grupo de recursos de host usando os métodos a seguir.

Console

Como executar uma instância em um grupo de recursos de host

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.

   > **Note**
   >
   > AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.

4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.
5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
6. Na seção Advanced details (Detalhes avançados), faça o seguinte:
   a. Em Tenancy (Locação), escolha Dedicated Host (Host dedicado).
   b. Em Target host by (Visar host por), selecione Host resource group (Grupo de recursos do host).

c. Em Tenancy host resource group name (Nome do grupo de recursos do host de locação), escolha o grupo de recursos de host no qual a instância será iniciada.

d. Em Tenancy affinity (Afinidade de locação), faça uma destas opções:

- Selecione Off (Desativar): a instância será iniciada no host especificado, mas não é garantido que seja iniciada no mesmo host dedicado se for interrompida.
- Selecione o ID do host dedicado: se for interrompida, a instância sempre será reiniciada nesse host específico.

Para obter mais informações sobre afinidade, consulte Noções básicas sobre posicionamento automático e afinidade.

7. Configure as demais opções da instância conforme necessário. Para ter mais informações, consulte Iniciar uma instância usando parâmetros definidos.
8. Escolha Iniciar instância.

AWS CLI

Como executar uma instância em um grupo de recursos de host

Use o comando run-instances da AWS CLI e, no parâmetro de solicitação `Placement`, omita a opção Tenancy e especifique o ARN do grupo de recursos do host.

PowerShell

Como executar uma instância em um grupo de recursos de host

Use o comando New-EC2Instance do AWS Tools for Windows PowerShell e, no parâmetro de solicitação `Placement`, omita a opção Tenancy e especifique o ARN do grupo de recursos do host.

Noções básicas sobre posicionamento automático e afinidade

O controle de posicionamento do Hosts dedicados ocorre em nível de instância e de host.

Posicionamento automático

O posicionamento automático é configurado no nível do host. Ele permite que você gerencie se as instâncias são executadas em um host específico ou em qualquer host disponível com as configurações correspondentes.

Quando o posicionamento automático de um Host dedicado está desabilitado, ele só aceita execuções de instâncias de locação Host que especificam seu ID exclusivo de host. Trata-se da configuração padrão para novos Hosts dedicados.

Quando o posicionamento automático de um Host dedicado está habilitado, ele aceita todas as execuções de instâncias não direcionadas que correspondam à configuração do tipo de instância.

Ao executar uma instância, você precisa configurar sua locação. A execução de uma instância em um Host dedicado sem fornecer um `HostId` específico permite que você a execute em qualquer Host dedicado que tenha o posicionamento automático habilitado e corresponda ao seu tipo de instância.

Afinidade de host

A afinidade de host é configurada no nível da instância. Ela estabelece uma relação de execução entre uma instância e um Host dedicado.

Quando a afinidade é definida como `Host`, uma instância executada em um host específico sempre é reiniciada no mesmo host se for interrompida. Isso se aplica a execuções direcionadas e não direcionadas.

Quando a afinidade estiver definida como `Default` e você parar e reiniciar a instância, ela poderá ser reiniciada em qualquer host disponível. Contudo, ela tenta ser executada novamente no último Host dedicado em que estava em execução (com base no melhor esforço).

Modificar posicionamento automático de Host dedicado

É possível modificar as configurações de posicionamento automático de um Host dedicado depois de alocá-lo à sua conta da AWS, usando um dos métodos a seguir.

Console

Como modificar o posicionamento automático de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione um host e escolha Actions (Ações), Modify host (Modificar host).
4. Em Instance auto-placement (Posicionamento automático da instância), escolha Enable (Habilitar) para habilitar o posicionamento automático ou desmarque Enable (Habilitar) para desabilitar o posicionamento automático. Para ter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade.

5. Escolha Save (Salvar).

AWS CLI

Como modificar o posicionamento automático de um Host dedicado

Use o comando modify-hosts da AWS CLI. O exemplo a seguir habilita o posicionamento automático para o Host dedicado especificado.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Como modificar o posicionamento automático de um Host dedicado

Use o comando Edit-EC2Host do AWS Tools for Windows PowerShell. O exemplo a seguir habilita o posicionamento automático para o Host dedicado especificado.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modificar os tipos de instância compatíveis

O suporte para vários tipos de instância no mesmo host dedicado está disponível para as seguintes famílias de instâncias: C5, M5, R5, C5n, R5n, M5n e T3. Outras famílias de instâncias oferecem suporte apenas a um único tipo de instância no mesmo Host dedicado.

É possível alocar um Host dedicado usando os métodos a seguir.

É possível modificar um Host dedicado para alterar os tipos de instância aos quais ele oferece suporte Se ele oferecer suporte a um único tipo de instância no momento, será possível modificá-lo para oferecer suporte a vários tipos de instância dentro dessa família de instâncias. De forma semelhante, se ele oferecer suporte a vários tipos de instância, será possível modificá-lo para oferecer suporte somente a um tipo específico de instância.

Para modificar o Host dedicado para oferecer suporte a vários tipos de instância, primeiro interrompa todas as instâncias em execução no host. Essa modificação leva aproximadamente 10 minutos para ser concluída. O Host dedicado faz a transição para o estado `pending` enquanto as modificações estão em andamento. Não é possível iniciar instâncias interrompidas ou executar novas instâncias no Host dedicado enquanto ele estiver no estado `pending`.

Para modificar um Host dedicado compatível com vários tipos de instância para que ofereça suporte a um tipo específico de instância, o host não deve ter nenhuma instância em execução, ou as instâncias em execução devem ser do tipo ao qual você deseja que o host ofereça suporte. Por exemplo, para modificar um host que oferece suporte a vários tipos de instância na família de instâncias `m5` para oferecer suporte apenas a instâncias `m5.large`, o Host dedicado não deve ter nenhuma instância em execução ou ter apenas instâncias `m5.large` em execução.

Se você alocar um host para um tipo de instância virtualizada, não poderá modificar o tipo de instância para um tipo de instância `.metal` depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.large`, não poderá modificar o tipo de instância para `m5.metal`. Da mesma forma, se você alocar um host para um tipo de instância `.metal`, não poderá modificar o tipo de instância para um tipo de instância virtualizada depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.metal`, não poderá modificar o tipo de instância para `m5.large`.

É possível modificar os tipos de instância compatíveis usando um dos métodos a seguir.

Console

Como modificar os tipos de instância compatíveis de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Dedicated Host (Host dedicado).
3. Selecione o Host dedicado a ser modificado e escolha Actions (Ações), Modify host (Modificar host).
4. Dependendo da configuração atual do Host dedicado, siga um destes procedimentos:

   - Atualmente, se o Host dedicado oferecer suporte a um tipo de instância específico, o Support multiple instance types (Oferecer suporte a vários tipos de instância) não será habilitado e o Instance type (Tipo de instância) listará o tipo de instância compatível. Para modificar o host para oferecer suporte a vários tipos na família de instâncias atual, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar).

     Primeiro é necessário interromper todas as instâncias em execução no host antes de modificá-lo para oferecer suporte a vários tipos de instância.
   - Atualmente, se o Host dedicado oferecer suporte a vários tipos de instância em uma família de instâncias, Enabled (Habilitado) estará selecionado em Support multiple instance

types (Oferecer suporte a vários tipos de instância). Para modificar o host para oferecer suporte a um tipo específico de instância, em Support multiple instance types (Oferecer suporte a vários tipos de instância), desmarque Enable (Habilitar) e, em Instance type (Tipo de instância), selecione o tipo de instância específico ao qual oferecer suporte.

Não é possível alterar a família de instâncias compatível do Host dedicado.

5. Escolha Save (Salvar).

AWS CLI

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o comando modify-hosts da AWS CLI.

O comando a seguir modifica um Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias `m5`.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

O comando a seguir modifica um Host dedicado para oferecer suporte apenas a instâncias `m5.xlarge`.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o comando Edit-EC2Host do AWS Tools for Windows PowerShell.

O comando a seguir modifica um Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias `m5`.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

O comando a seguir modifica um Host dedicado para oferecer suporte apenas a instâncias `m5.xlarge`.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modificar locação e da afinidade de instâncias

É possível alterar a locação de uma instância depois de tê-la iniciado. Você também pode modificar a afinidade da instância para atingir um host específico ou permitir que ela seja iniciada em qualquer host dedicado disponível com atributos correspondentes em sua conta. Para modificar a locação ou a afinidade da instância, a instância deve estar no estado `stopped`.

Os detalhes do sistema operacional da instância, e se o SQL Server está ou não instalado, afetam quais conversões são compatíveis. Para obter mais informações sobre os caminhos de conversão de locação disponíveis para a sua instância, consulte Tenancy conversion no License Manager User Guide.

> **Note**
>
> Para instâncias T3, você deve iniciar a instância em um host dedicado para usar uma locação de `host`. Para instâncias T3, você não pode alterar a locação de `host` para `dedicated` ou `default`. Tentar fazer uma dessas alterações de locação não compatíveis gera um código de erro de `InvalidRequest`.

É possível modificar a locação e a afinidade de uma instância usando os métodos a seguir.

Console

Como modificar a locação ou a afinidade da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instances (Instâncias) e selecione a instância a ser modificada.
3. Escolha Instance state (Estado da instância), Stop (Interromper).
4. Com a instância selecionada, escolha Ações, Configurações de instância, Modificar posicionamento de instância).
5. Na página Modificar posicionamento da instância, configure o seguinte:
   - Tenancy (Locação) — escolha um dos seguintes:
     - Run a dedicated hardware instance (Executar uma instância de hardware dedicada) — executa a instância como um Instâncias dedicadas. Para ter mais informações, consulte Dedicated Instances.

- Launch the instance on a Host dedicado (Executar a instância em um dh) — executa a instância em um Host dedicado com afinidade configurável.

- Affinity (Afinidade) — escolha uma das seguintes opções:
  - This instance can run on any one of my hosts (Esta instância pode ser executada em qualquer um dos meus hosts) — A instância é executada em qualquer Host dedicado disponível em uma conta que ofereça suporte ao seu tipo de instância.
  - This instance can only run on the selected host (Esta instância só pode ser executada no host selecionado) — A instância só pode ser executada no Host dedicado selecionado em Target Host (Host de destino).
- Target Host (Host de destino) — selecione o Host dedicado no qual executar a instância. Se nenhum host de destino estiver listado, talvez não haja Hosts dedicados disponíveis e compatíveis em sua conta.

Para ter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade.

6. Escolha Save (Salvar).

AWS CLI

Como modificar a locação ou a afinidade da instância

Use o comando modify-instance-placement da AWS CLI. O exemplo a seguir altera a afinidade da instância especificada de `default` para `host` e especifica o Host dedicado com o qual a instância tem afinidade.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
 --tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

Como modificar a locação ou a afinidade da instância

Use o comando Edit-EC2InstancePlacement do AWS Tools for Windows PowerShell. O exemplo a seguir altera a afinidade da instância especificada de `default` para `host` e especifica o Host dedicado com o qual a instância tem afinidade.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
Tenancy host -HostId h-012a3456b7890cdef
```

Visualização do Hosts dedicados

É possível visualizar os detalhes de um Host dedicado e das Instâncias individuais existentes nele usando os métodos a seguir.

Console

Como visualizar os detalhes de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione um host.
4. Para obter informações sobre o host, escolha Details (Detalhes).

   Available vCPUs (vCPUs disponíveis) indica que vCPUs estão disponíveis no Host dedicado para execução de novas instâncias. Por exemplo, um Host dedicado que oferece suporte a vários tipos de instância na família de instâncias `c5` e que não tem nenhuma instância em execução nele, tem 72 vCPUs disponíveis. Isso significa que é possível executar diferentes combinações de tipos de instância no Host dedicado para consumir as 72 vCPUs disponíveis.

   Para obter informações sobre as instâncias em execução no host, escolha Running instances (Instâncias em execução).

AWS CLI

Como visualizar a capacidade de um Host dedicado

Use o comando describe-hosts da AWS CLI.

O exemplo a seguir usa o comando describe-hosts (AWS CLI) para visualizar a capacidade de instâncias disponível para um Host dedicado que oferece suporte a vários tipos de instância na família de instâncias `c5`. O Host dedicado já tem duas instâncias `c5.4xlarge` e quatro instâncias `c5.2xlarge` em execução nele.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [
    { "AvailableCapacity": 2,
      "InstanceType": "c5.xlarge",
      "TotalCapacity": 18 },
    { "AvailableCapacity": 4,
      "InstanceType": "c5.large",
      "TotalCapacity": 36 }
  ],
"AvailableVCpus": 8
```

PowerShell

Como visualizar a capacidade da instância de um Host dedicado

Use o comando Get-EC2Host do AWS Tools for Windows PowerShell.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Marcação de Hosts dedicados

É possível atribuir tags personalizadas aos Host dedicados existentes para categorizá-los de diferentes formas; por exemplo, por objetivo, proprietário ou ambiente. Isso ajuda a localizar rapidamente um host dedicado específico com base na tags personalizadas que você atribuiu. As tags de host dedicado também podem ser usadas para rastreamento de alocação de custos.

Também é possível aplicar tags aos Hosts dedicados no momento da criação. Para ter mais informações, consulte Alocar Hosts dedicados.

É possível marcar um Host dedicado usando os métodos a seguir.

Console

Como marcar um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado a ser marcado e escolha Actions (Ações), Manage tags (Gerenciar tags).

4. Na tela Manage tags (Gerenciar tags), escolha Add tag (Adicionar tag) e especifique a chave e o valor da tag.
5. (Opcional) Escolha Add tag (Adicionar tag) para adicionar outras tags ao Host dedicado.
6. Selecione Save changes (Salvar alterações).

AWS CLI

Como marcar um Host dedicado

Use o comando da AWS CLI create-tags.

O comando a seguir marca o Host dedicado especificado com `Owner=TeamA`.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

Como marcar um Host dedicado

Use o comando do AWS Tools for Windows PowerShell New-EC2Tag.

O comando `New-EC2Tag` precisa de um objeto `Tag`, que especifica o par de chave e valor a ser usado na tag do Host dedicado. Os seguintes comandos criam um objeto `Tag` denominado `$tag` com um par de chave e valor de `Owner` e `TeamA`, respectivamente:

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

O comando a seguir marca o Host dedicado especificado com o objeto `$tag`:

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

Monitorar Hosts dedicados

O Amazon EC2 monitora constantemente o estado do seu Hosts dedicados. As atualizações são comunicadas no console do Amazon EC2. É possível visualizar informações sobre um Host dedicado usando os métodos a seguir.

Console

Como visualizar o estado de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Localize o Host dedicado na lista e revise o valor na coluna State (Estado).

AWS CLI

Como visualizar o estado de um Host dedicado

Use o comando describe-hosts da AWS CLI e revise a propriedade `state` no elemento de resposta `hostSet`.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Como visualizar o estado de um Host dedicado

Use o comando Get-EC2Host do AWS Tools for Windows PowerShell e revise a propriedade `state` no elemento de resposta `hostSet`.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

A tabela a seguir explica os possíveis estados de um Host dedicado.

Estado	Descrição
`available`	A AWS não detectou nenhum problema com o host dedicado. Não estão programados manutenções ou reparos. As instâncias podem ser executadas neste host dedicado.
`released`	O Host dedicado foi liberado. O ID do host não está mais uso. Os hosts liberados não podem ser reutilizados.
`under-assessment`	A AWS está explorando um possível problema com o host dedicado. Se for necessário executar uma ação, você será notificado pelo AWS

Estado	Descrição
	Management Console ou por e-mail. As instâncias não podem ser executadas em um Host dedicado neste estado.
`pending`	O Host dedicado não pode ser usado para execução de novas instâncias. Ele está sendo modificado para oferecer suporte a vários tipos de instância, ou uma recuperação de host está em andamento.
`permanent-failure`	Uma falha irrecuperável foi detectada. Você receberá um aviso de remoção por meio de suas instâncias e por e-mail. Suas instâncias podem continuar a ser executadas. Se você interromper ou encerrar todas as instâncias de um host dedicado neste estado, a AWS desativará o host. A AWS não reinicia instâncias nesse estado. As instâncias não podem ser executadas no Hosts dedicados neste estado.
`released-permanent-failure`	A AWS liberará permanentemente os hosts dedicados que falharem e não tiverem mais instâncias em execução. O ID do Host dedicado não está mais disponível para uso.

Liberar Hosts dedicados

Todas as instâncias em execução no Host dedicado devem ser interrompidas para que você possa liberar o host. Essas instâncias podem ser migradas para outros Hosts dedicados de sua conta para que você possa continuar as usando. Estas etapas se aplicam somente a Hosts dedicados sob demanda.

É possível liberar um Host dedicado usando os métodos a seguir.

Console

Como liberar um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione o Host dedicado a ser liberado.
4. Escolha Actions (Ações), Release host (Liberar host).
5. Para confirmar, escolha Release (Liberar).

AWS CLI

Como liberar um Host dedicado

Use o comando release-hosts da AWS CLI.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Como liberar um Host dedicado

Use o comando Remove-EC2Hosts do AWS Tools for Windows PowerShell.

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Depois de liberar um Host dedicado, você não pode reutilizar o mesmo host ou ID de host, e não terá mais taxas de faturamento sob demanda cobradas para ele. O estado do Host dedicado será alterado para `released` e não será mais possível executar nenhuma instância nesse host.

> **Note**
>
> Se você tiver liberado o Hosts dedicados recentemente, poderá levar um tempo para que eles parem de contar para seu limite. Durante esse tempo, é possível receber erros de `LimitExceeded` ao tentar alocar novos Hosts dedicados. Se esse for o caso, tente alocar novos hosts novamente após alguns minutos.

As instâncias que foram interrompidas ainda estão disponíveis para uso e estão listadas na página Instances (Instâncias). Elas retêm sua configuração de alocação de `host`.

Comprar Reservas de hosts dedicados

É possível comprar reservas usando os seguintes métodos:

Console

Como comprar reservas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. Selecione Hosts dedicados, Reservas de hosts dedicados, Purchase Reserva de hosts dedicados (Comprar Reserva de hosts dedicados).
3. Na tela Encontrar ofertas, faça o seguinte:
   a. Em Família de instâncias, selecione a família de instâncias do host dedicado para a qual deseja adquirir a reserva de host dedicado.
   b. Em Opção de pagamento, selecione e configure a opção de pagamento de sua preferência.
4. Escolha Próximo.
5. Selecione os hosts dedicados aos quais deseja associar a reserva de host dedicado e, em seguida, escolha Próximo.
6. (Opcional) Atribua etiquetas à reserva de host dedicado.
7. Analise o pedido e escolha Adquirir.

AWS CLI

Como comprar reservas

1. Use o comando describe-host-reservation-offerings da AWS CLI para listar as ofertas disponíveis que atendam às suas necessidades. O exemplo a seguir lista as ofertas compatíveis com instâncias na família de instâncias `m4` e tem período de vigência de um ano.

   > **Note**
   >
   > O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

   ```
   aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4 --max-duration 31536000
   ```

   O comando retorna uma lista de ofertas que correspondem aos seus critérios. Observe o `offeringId` da oferta a ser comprada.
2. Use o comando purchase-host-reservation da AWS CLI para comprar a oferta e fornecer o `offeringId` indicado na etapa anterior. O exemplo a seguir compra a reserva especificada

e ela é associada a um host dedicado específico já atribuído à conta da AWS, e uma etiqueta é aplicada com uma chave de `purpose` e um valor de `production`.

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --
host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Como comprar reservas

1. Use o comando Get-EC2HostReservationOffering do AWS Tools for Windows PowerShell para listar as ofertas disponíveis que atendam às suas necessidades. Os seguintes exemplos listam as ofertas compatíveis com instâncias na família de instâncias `m4` e têm prazo de um ano.

   > **Note**
   >
   > O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

   ```
   PS C:\> $filter = @{Name="instance-family"; Value="m4"}
   ```

   ```
   PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
   ```

   O comando retorna uma lista de ofertas que correspondem aos seus critérios. Observe o `offeringId` da oferta a ser comprada.

2. Use o comando New-EC2HostReservation do AWS Tools for Windows PowerShell para comprar a oferta e fornecer o `offeringId` indicado na etapa anterior. O exemplo a seguir compra a reserva especificada e ela é associada a um host dedicado específico já atribuído à conta da AWS.

   ```
   PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
   HostIdSet h-013abcd2a00cbd123
   ```

Visualizar reservas de Host dedicado

É possível ver as informações sobre o Hosts dedicados que estão associadas à sua reserva, como:

- O período de vigência da reserva
- A opção de pagamento
- As datas de início e fim

É possível visualizar detalhes de suas reservas do Host dedicado usando os métodos a seguir.

Console

Como ver os detalhes de uma reserva do Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, escolha Host dedicado Reservations (Reservas de hosts dedicados) e selecione a reserva na lista fornecida.
4. Selecione Details (Detalhes) para obter informações sobre a reserva.
5. Selecione Hosts para obter informações sobre os Hosts dedicados aos quais a reserva está associada.

AWS CLI

Como ver os detalhes de uma reserva do Host dedicado

Use o comando describe-host-reservations da AWS CLI.

```
aws ec2 describe-host-reservations
```

PowerShell

Como ver os detalhes de uma reserva do Host dedicado

Use o comando Get-EC2HostReservation do AWS Tools for Windows PowerShell.

```
PS C:\> Get-EC2HostReservation
```

Atribuir tag de Reservas de hosts dedicados

É possível atribuir tags personalizadas aos Reservas de hosts dedicados para categorizá-los de diferentes maneiras, como por objetivo, proprietário ou ambiente. Isso ajuda a localizar rapidamente um Reserva de hosts dedicados específico com base na tags personalizadas que você atribuiu.

Só é possível marcar um Reserva de hosts dedicados usando as ferramentas da linha de comando.

AWS CLI

Como marcar um Reserva de hosts dedicados

Use o comando da AWS CLI create-tags.

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

Como marcar um Reserva de hosts dedicados

Use o comando do AWS Tools for Windows PowerShell New-EC2Tag.

O comando `New-EC2Tag` precisa de um parâmetro `Tag`, que especifica o par de chave e valor a ser usado na tag do Reserva de hosts dedicados. Os comandos a seguir criam o parâmetro de `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

Trabalhar com Hosts dedicados compartilhado

O compartilhamento de host dedicado permite que proprietários de hosts dedicados os compartilhem com outras contas da AWS ou em uma organização da AWS. Isso permite criar e gerenciar os hosts dedicados centralmente, e compartilhar o host dedicado entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui o host dedicado (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nos Hosts

dedicados que são compartilhadas com eles da mesma maneira que executam instâncias em Hosts dedicados alocados em sua própria conta. O proprietário é responsável pelo gerenciamento do Host dedicado e pelas instâncias executadas nele. Os proprietários não podem modificar instâncias que os consumidores executam em Hosts dedicados compartilhados. Os consumidores são responsáveis por gerenciar as instâncias que executam em Hosts dedicados compartilhados com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário do Host dedicado, e não podem modificar os Hosts dedicados que são compartilhados com eles.

Um proprietário de Host dedicado pode compartilhar um Host dedicado com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Tópicos

- Pré-requisitos para compartilhar Hosts dedicados
- Limitações para compartilhamento de Host dedicado
- Serviços relacionados
- Compartilhamento entre zonas de disponibilidade
- Compartilhar um Host dedicado
- Descompartilhar um Host dedicado compartilhado
- Identificar um Host dedicado compartilhado
- Visualizar instâncias em execução em um Host dedicado compartilhado
- Permissões de Host dedicado compartilhado
- Faturamento e medição
- Limites de Host dedicado
- Recuperação de host e compartilhamento do Host dedicado

Pré-requisitos para compartilhar Hosts dedicados

- Para compartilhar um host dedicado, é necessário ser o proprietário dele em sua conta da AWS. Não é possível compartilhar um Host dedicado que tenha sido compartilhado com você.

- Para compartilhar um host dedicado com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Limitações para compartilhamento de Host dedicado

Não é possível compartilhar Hosts dedicados que foram alocados para os seguintes tipos de instância: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`.

Serviços relacionados

AWS Resource Access Manager

O compartilhamento de host dedicado integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de seus Hosts dedicados relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da zona de disponibilidade é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de zona de disponibilidade da região `us-east-1` e é o mesmo local em cada conta da AWS.

Como visualizar os IDs de zona de disponibilidade para as zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram.
2. Os IDs de zona de disponibilidade da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar um Host dedicado

Quando um proprietário compartilha um Host dedicado, ele permite que os consumidores executem instâncias no host. Os consumidores podem executar tantas instâncias no host compartilhado quanto sua capacidade disponível permitir.

> **Important**
>
> Observe que você é responsável por garantir que possui direitos de licença apropriados para compartilhar qualquer licença BYOL no Hosts dedicados.

Se você compartilhar um Host dedicado com o posicionamento automático habilitado, lembre-se do seguinte, pois isso pode gerar uso não intencional do Host dedicado:

- Se os consumidores executarem instâncias com locação de Host dedicado e não tiverem capacidade em um Host dedicado que possuam na conta, a instância será executada automaticamente no Host dedicado compartilhado.

Para compartilhar um Host dedicado, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. É possível adicionar o Host dedicado a um recurso existente ou adicioná-lo a um novo compartilhamento de recursos.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente ao host dedicado compartilhado. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao Host dedicado compartilhado depois de aceitar o convite.

> **Note**
>
> Depois de compartilhar um Host dedicado, pode levar alguns minutos para que os consumidores tenham acesso a ele.

É possível compartilhar um Host dedicado de sua propriedade usando um dos seguintes métodos.

Amazon EC2 console

Como compartilhar um Host dedicado de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Escolha o Host dedicado a ser compartilhado e selecione Ações, Compartilhar host.
4. Selecione o compartilhamento de recursos ao qual adicionar o Host dedicado e escolha Compartilhar host.

   Pode levar alguns minutos para que os consumidores obtenham acesso ao host compartilhado.

AWS RAM console

Para compartilhar um host dedicado de sua propriedade usando o console do AWS RAM

Consulte Criar um compartilhamento de atributos no Manual do usuário do AWS RAM.

AWS CLI

Para compartilhar um host dedicado de sua propriedade usando a AWS CLI

Use o comando create-resource-share.

Descompartilhar um Host dedicado compartilhado

O proprietário do Host dedicado pode cancelar o compartilhamento de um Host dedicado compartilhado a qualquer momento. Ao cancelar o compartilhamento de um Host dedicado compartilhado, as seguintes regras são aplicadas:

- Os consumidores com os quais o Host dedicado foi compartilhado não podem mais executar novas instâncias nele.
- As instâncias de propriedade de consumidores que estavam em execução no Host dedicado no momento do cancelamento do compartilhamento continuam a ser executadas, mas são programadas para desativação. Os consumidores recebem notificações de desativação para as instâncias e têm duas semanas para agir sobre as notificações. No entanto, se o Host dedicado for compartilhado novamente com o consumidor durante o período de aviso de desativação, as desativações de instância serão canceladas.

Para cancelar o compartilhamento de um Host dedicado compartilhado de sua propriedade, é necessário removê-lo do compartilhamento de recursos. Isso pode ser feito usando um dos seguintes métodos.

Amazon EC2 console

Como cancelar o compartilhamento de um Host dedicado compartilhado de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Escolha o Host dedicado do qual cancelar o compartilhamento e escolha a guia Compartilhamento.
4. A guia Compartilhamento lista os compartilhamentos de recursos aos quais o Host dedicado foi adicionado. Selecione o compartilhamento de recursos do qual remover o Host dedicado e escolha Remover do compartilhamento de recursos.

AWS RAM console

Para cancelar o compartilhamento de um host dedicado compartilhado de sua propriedade usando o console do AWS RAM

Consulte Atualização de um compartilhamento de atributos no Guia do usuário do AWS RAM.

Command line

Para cancelar o compartilhamento de um host dedicado compartilhado de sua propriedade usando a AWS CLI

Use o comando disassociate-resource-share.

Identificar um Host dedicado compartilhado

Proprietários e consumidores podem identificar Hosts dedicados compartilhados usando um dos seguintes métodos.

Amazon EC2 console

Como identificar um Host dedicado compartilhado usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados. A tela lista Hosts dedicados de sua propriedade e Hosts dedicados compartilhados com você. A coluna Owner (Proprietário) mostra o ID de conta da AWS do proprietário do host dedicado.

Command line

Para identificar um host dedicado compartilhado usando a AWS CLI

Use o comando describe-hosts. O comando retorna os Hosts dedicados de sua propriedade e os Hosts dedicados compartilhados com você.

Visualizar instâncias em execução em um Host dedicado compartilhado

Proprietários e consumidores podem visualizar as instâncias em execução em um Host dedicado compartilhado a qualquer momento usando um dos seguintes métodos.

Amazon EC2 console

Como visualizar as instâncias em execução em um Host dedicado compartilhado usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado para o qual deseja visualizar as instâncias e escolha Instances (Instâncias). A guia lista as instâncias em execução no host. Os proprietários veem todas as instâncias em execução no host, incluindo instâncias executadas pelos consumidores. Os consumidores veem somente as instâncias que executaram no host. A coluna Owner (Proprietário) mostra o ID da conta da AWS que executou a instância.

Command line

Para visualizar as instâncias em execução em um host dedicado compartilhado usando a AWS CLI

Use o comando describe-hosts. O comando retorna as instâncias em execução em cada Host dedicado. Os proprietários veem todas as instâncias em execução no host. Os consumidores veem somente as instâncias em execução que executaram nos hosts compartilhados. `InstanceOwnerId` mostra o ID de conta da AWS do proprietário da instância.

Permissões de Host dedicado compartilhado

Permissões para proprietários

Os proprietários são responsáveis pelo gerenciamento de seus Hosts dedicados compartilhados e das instâncias executadas neles. Os proprietários podem visualizar todas as instâncias em execução no Host dedicado compartilhado, incluindo aquelas executadas pelos consumidores. No entanto, os proprietários não podem realizar ações nas instâncias que foram executadas pelos consumidores.

Permissões para consumidores

Os consumidores são responsáveis por gerenciar as instâncias que executam em um Host dedicado compartilhado. Os consumidores não podem modificar o Host dedicado compartilhado de nenhuma forma e não podem visualizar nem modificar instâncias que foram executadas por outros consumidores ou pelo proprietário do Host dedicado.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Hosts dedicados.

Os proprietários são cobrados por Hosts dedicados compartilhado. Os consumidores não são cobrados pelas instâncias que executam no Hosts dedicados compartilhado.

Reservas de hosts dedicados continuam a oferecer descontos de cobrança por Hosts dedicados compartilhados. Somente proprietários de Host dedicado podem comprar Reservas de hosts dedicados para Hosts dedicados compartilhados que possuem.

Limites de Host dedicado

Hosts dedicados compartilhados são contabilizados somente para os limites de Hosts dedicados do proprietário. Os limites de Hosts dedicados do consumidor não são afetados por Hosts dedicados

que foram compartilhados com eles. Da mesma forma, as instâncias executadas pelos consumidores em Hosts dedicados compartilhados não são contabilizadas para seus limites de instâncias.

Recuperação de host e compartilhamento do Host dedicado

A recuperação de host recupera instâncias executadas pelo proprietário do Host dedicado e pelos consumidores com os quais ele foi compartilhado. O Host dedicado de reposição é alocado na conta do proprietário. É adicionado aos mesmos compartilhamentos de recursos que o Host dedicado original e é compartilhado com os mesmos consumidores.

Para ter mais informações, consulte Recuperação do host.

Hosts dedicados no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS para o local. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que você crie e execute aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, usando recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

Você pode alocar hosts dedicados nos Outposts que você tiver em sua conta. Isso torna mais fácil para você trazer suas licenças de software e workloads existentes que exigem um servidor físico dedicado para AWS Outposts. Você também pode direcionar ativos de hardware específicos em um Outpost para ajudar a minimizar a latência entre as workloads.

Os hosts dedicados permitem que você use suas licenças de software qualificadas no Amazon EC2 para obter a flexibilidade e a economia de usar suas próprias licenças. Outras licenças de software vinculadas a máquinas virtuais, soquetes ou núcleos físicos também podem ser usadas em hosts dedicados, sujeitos aos termos de licença. Embora o Outposts sempre tenha sido um ambiente de locatário único qualificado para workloads BYOL, os hosts dedicados permitem limitar as licenças necessárias a um único host, e não a toda a implantação do Outpost.

Além disso, o uso de hosts dedicados em um Outpost oferece maior flexibilidade na implantação do tipo de instância e um controle mais granular sobre o posicionamento da instância. Você pode

segmentar um host específico para execuções de instância e usar a afinidade do host para garantir que a instância sempre seja executada nesse host, ou você pode usar o posicionamento automático para executar uma instância em qualquer host disponível que tenha configurações correspondentes e capacidade disponível.

Sumário

- Pré-requisitos
- Atributos compatíveis
- Considerações
- Alocar e usar um host dedicado em um Outpost

Pré-requisitos

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Atributos compatíveis

- Há suporte para as seguintes famílias de instâncias: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` e `i3en`.
- Os hosts dedicados no Outposts podem ser configurados para serem compatíveis com vários tamanhos de instância. A compatibilidade com vários tamanhos de instância está disponível para as seguintes famílias de instâncias: `C5`, `M5`, `R5`, `C5d`, `M5d` e `R5d`. Para ter mais informações, consulte Configurações de capacidade de instância.
- Hosts dedicados no Outposts são compatíveis com o posicionamento automático e as execuções de instâncias direcionadas. Para ter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade.
- Hosts dedicados no Outposts são compatíveis com a afinidade do host. Para ter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade.
- Hosts dedicados no Outposts são compatíveis o compartilhamento com AWS RAM. Para ter mais informações, consulte Trabalhar com Hosts dedicados compartilhado.

Considerações

- Reservas do host dedicado não são compatíveis com o Outposts.
- Grupos de recursos de host e AWS License Manager não são compatíveis com o Outposts.

- Hosts dedicados no Outposts não são compatíveis com a instâncias T3 intermitentes.
- Hosts dedicados no Outposts não são compatíveis com a recuperação do host.
- Não há compatibilidade da recuperação automática simplificada em instâncias com locação de hosts dedicados em Outposts.

Alocar e usar um host dedicado em um Outpost

Você aloca e usa hosts dedicados em Outposts da mesma forma que faria com hosts dedicados em uma região da AWS.

Pré-requisitos

Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.

Para alocar um host dedicado a um Outpost, use um destes métodos:

AWS Outposts console

1. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Outposts. Selecione o Outpost e, em seguida, escolha Actions (Ações), Allocate Dedicated Host (Alocar host dedicado).
3. Configure o host dedicado, conforme necessário. Para ter mais informações, consulte Alocar Hosts dedicados.

   > **Note**
   >
   > Availability Zone (Zona de disponibilidade) e Outpost ARN (ARN do Outpost) devem ser preenchidos previamente com a zona de disponibilidade e o ARN do Outpost selecionado.

4. Escolha Allocate.

Amazon EC2 console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Dedicated Hosts (Hosts dedicados) e Allocate Host dedicado (Alocar host dedicado).

3. Em Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade associada ao Outpost.
4. Em Outpost ARN (ARN do Outpost), insira o ARN do Outpost.
5. Para direcionar ativos de hardware específicos no Outpost, em Segmente ativos de hardware específicos no Outpost, selecione Habilitar. Para cada ativo de hardware de destino, escolha Adicionar ID do ativo e, em seguida, insira o ID do ativo de hardware.

   > **Note**
   >
   > O valor especificado para Quantidade deve ser igual ao número de IDs de ativos que você especifica. Por exemplo, se você especificar três IDs de ativos, a Quantidade também deverá ser 3.

6. Defina as configurações restantes do host dedicado, conforme necessário. Para ter mais informações, consulte Alocar Hosts dedicados.
7. Escolha Allocate.

AWS CLI

Use o comando allocate-hosts da AWS CLI. Em `--availability-zone`, especifique a zona de disponibilidade associada ao Outpost. Em `--outpost-arn`, especifique o ARN do Outpost. Opcionalmente, para `--asset-ids`, especifique os IDs dos ativos de hardware do Outpost de destino.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn
 "arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

Como iniciar uma instância em um host dedicado em um Outpost

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados. Selecione o host dedicado que você alocou na etapa anterior e escolha Actions (Ações), Launch instance onto host (Executar instância no host).
3. Defina a instância conforme necessário e, em seguida, inicie a instância. Para ter mais informações, consulte Execute instâncias em um Host dedicado..

Recuperação do host

A recuperação automática do host dedicado reinicia as instâncias em um novo host substituto quando certas condições problemática são detectadas no host dedicado. A recuperação do host reduz a necessidade de intervenção manual e diminui a carga operacional em caso de falhas inesperadas no host dedicado relativas a eventos de alimentação do host ou conectividade da rede. Outros problemas do host dedicado exigirão intervenção manual para recuperação.

Conteúdo

- Conceitos básicos de recuperação do host
- Tipos de instâncias compatíveis
- Configurar a recuperação do host
- Estados de recuperação do host
- Recuperar manualmente instâncias incompatíveis
- Serviços relacionados
- Definição de preço

Conceitos básicos de recuperação do host

O processo de recuperação do host e dos grupos de recursos do host usa verificações de integridade no nível do host para avaliar a disponibilidade do host dedicado e detectar falhas nos sistemas subjacentes. O tipo de falha do host dedicado determina se a recuperação automática do host dedicado é possível. Os exemplos de problemas que podem causar falha nas verificações de integridade no nível do host incluem:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de hardware ou software no host físico

> **Important**
>
> A recuperação automática do host dedicado não ocorre quando o host está programado para ser desativado.

Recuperação automática de host dedicado

Quando uma falha de alimentação do sistema ou de conectividade de rede é detectada no seu host dedicado, a recuperação automática do host dedicado é iniciada, e o Amazon EC2 aloca automaticamente um host dedicado substituto na mesma zona de disponibilidade do host dedicado original. O Host dedicado em substituição recebe um novo ID do host, mas retém os mesmos atributos que o Host dedicado original, como:

- Availability Zone
- Tipo de instância
- Tags
- Configurações de autoposicionamento
- Reserva

Quando o host dedicado substituto é alocado, as instâncias são recuperadas para o host dedicado substituto. As instâncias recuperadas retêm os mesmos atributos que as instâncias originais, como:

- ID da instância
- Endereços IP privados
- Endereços IP elásticos
- Anexos de volume do EBS
- Todos os metadados da instância

Além disso, a integração incorporada com o AWS License Manager automatiza o monitoramento e o gerenciamento das licenças.

> **Note**
>
> A integração com o AWS License Manager é compatível somente nas regiões em que o AWS License Manager está disponível.

Se as instâncias tiverem um relacionamento de afinidade de host com o host dedicado prejudicado, as instâncias recuperadas estabelecem afinidade do host com o host dedicado de substituição.

Quando todas as instâncias tiverem sido recuperadas para o Host dedicado de substituição, o Host dedicado prejudicado será liberado e o Host dedicado de substituição ficará disponível para uso.

Quando a recuperação do host for iniciada, o proprietário da conta da AWS será notificado por e-mail e por um evento AWS Health Dashboard. A segunda notificação é enviada após a recuperação do host ser concluída com sucesso.

Se você estiver usando o AWS License Manager para acompanhar suas licenças, o AWS License Manager alocará novas licenças para o host dedicado de substituição conforme os limites de configuração da licença. Se a configuração da licença tiver limites rígidos que serão violados em resultado da recuperação do host, o processo de recuperação não será permitido e você será notificado da falha de recuperação do host por meio de uma notificação do Amazon SNS (se as configurações de notificação foram definidas no AWS License Manager). Se a configuração da licença tiver limites suaves que serão violados como resultado da recuperação do host, a recuperação poderá continuar e você será notificado acerca da violação do limite por meio de uma notificação do Amazon SNS. Para obter mais informações, consulte Uso de configurações de licença e Configurações no License Manager no Guia do usuário do AWS License Manager.

Cenários sem recuperação automática de host dedicado

A recuperação automática do host dedicado não ocorre quando o host está programado para ser desativado. Você receberá uma notificação de retirada no AWS Health Dashboard, um evento do Amazon CloudWatch e o endereço de email do proprietário da conta da AWS recebe uma mensagem sobre a falha do host dedicado. Siga as etapas de remedição descritas na notificação de desativação dentro do prazo especificado para recuperar manualmente as instâncias restantes no host que está sendo desativado.

As instâncias interrompidas não são recuperadas para o Host dedicado de substituição. Se você tentar iniciar uma instância interrompida que mire no Host dedicado prejudicado, o início da instância falhará. Recomendamos que você modifique a instância interrompida para mirar em um a host dedicado diferente ou abrir em qualquer host dedicado disponível, com configurações correspondentes e autoposicionamento habilitado.

As instâncias com armazenamento de instâncias não são recuperadas para o Host dedicado de substituição. Como medida de remediação, o Host dedicado prejudicado será marcado para desativação e você receberá tal notificação depois de a recuperação do host ser concluída. Siga as etapas de remedição descritas na notificação de desativação dentro do prazo especificado para recuperar manualmente as instâncias restantes no Host dedicado prejudicado.

Tipos de instâncias compatíveis

A recuperação de host é compatível com as seguintes famílias de instâncias: A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2iezn, u-6tb1, u-9tb1, u-12tb1, u-18tb1 e u-24tb1.

Para recuperar instâncias não compatíveis, consulte Recuperar manualmente instâncias incompatíveis.

> **Note**
>
> A recuperação automática de host dedicado de tipos de instância metal levará mais tempo para detectar e recuperar do que os tipos de instância não metal.

Configurar a recuperação do host

É possível configurar a recuperação do host no momento da alocação do host dedicado ou após a alocação, usando o console do Amazon EC2 ou AWS Command Line Interface (CLI).

Tópicos

- Ativar a recuperação do host
- Desativar a recuperação do host
- Visualizar a configuração de recuperação do host

Ativar a recuperação do host

É possível habilitar a recuperação do host no momento da alocação do Host dedicado ou após a alocação.

Para obter mais informações sobre como habilitar a recuperação do host no momento da alocação do Host dedicado, consulte Alocar Hosts dedicados.

Como habilitar a recuperação do host após a alocação usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado para o qual habilitar a recuperação do host e escolha Actions (Ações), Modify Host Recovery (Modificar recuperação do host).

4. Para Host recovery (Recuperação do host), selecione Enable (Habilitar) e Save (Salvar).

Como habilitar a recuperação do host após a alocação usando a AWS CLI

Use o comando modify-hosts e especifique o parâmetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Desativar a recuperação do host

É possível desabilitar a recuperação do host a qualquer momento após o Host dedicado ser alocado.

Como desabilitar a recuperação do host após a alocação usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado no qual a recuperação do host será desabilitada e escolha Actions (Ações), Modify Host Recovery (Modificar recuperação do host).
4. Para Host recovery (Recuperação do host), selecione Disable (Desabilitar) e Save (Salvar).

Como desabilitar a recuperação do host após a alocação usando a AWS CLI

Use o comando modify-hosts e especifique o parâmetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Visualizar a configuração de recuperação do host

É possível ver a configuração de recuperação do host para o Host dedicado a qualquer momento.

Como visualizar a configuração de recuperação do host para um Host dedicado usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado e, na aba Description (Descrição), confira o campo Host Recovery (Recuperação do host).

Para visualizar a configuração de recuperação do host para um host dedicado usando a AWS CLI

Use o comando describe-hosts.

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

O elemento de resposta do `HostRecovery` indica se a recuperação do host está habilitada ou desabilitada.

Estados de recuperação do host

Quando a falha do Host dedicado for detectada, o Host dedicado prejudicado entra no estado `under-assessment` e todas as instâncias entram no estado `impaired`. Não é possível executar instâncias no Host dedicado prejudicado enquanto estiver no estado `under-assessment`.

Depois de o Host dedicado de substituição ser alocado, ele entra no estado `pending`. Ele continua nesse estado até que o processo de recuperação do host esteja concluído. Não é possível executar instâncias no Host dedicado de substituição enquanto ele estiver no estado `pending`. As instâncias recuperadas no Host dedicado de substituição continuam no estado `impaired` durante o processo de recuperação.

Depois de a recuperação do host ser concluída, o Host dedicado de substituição entrará no estado `available` e as instâncias recuperadas retornarão ao estado `running`. É possível abrir instâncias no Host dedicado de substituição depois de entrar no estado `available`. O Host dedicado prejudicado original é liberado permanentemente e entra no estado `released-permanent-failure`.

Se o Host dedicado prejudicado tiver instâncias incompatíveis com a recuperação do host, como instâncias com volumes compatíveis com o armazenamento de instâncias, o Host dedicado não será liberado. Em vez disso, é marcado para aposentadora e entra no estado `permanent-failure`.

Recuperar manualmente instâncias incompatíveis

A recuperação do host não é compatível com a recuperação de instâncias que usam volumes do armazenamento de instâncias. Siga as instruções abaixo para recuperar à mão todas as instâncias que não puderem ser recuperadas automaticamente.

> **Warning**
>
> Os dados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de

instância anexados a uma instância que possui um volume do EBS como dispositivo raiz. Para proteger os dados dos volumes de armazenamento de instâncias, faça backup no armazenamento persistente antes de a instância ser interrompida ou encerrada.

Recuperar manualmente instâncias compatíveis com EBS

Para instâncias compatíveis com EBS que não possam ser recuperadas automaticamente, recomendamos pará-las e iniciá-las automaticamente para recuperá-las a um novo Host dedicado. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte Início e interrupção de instâncias do Amazon EC2.

Recuperar manualmente instâncias compatíveis com armazenamento de instâncias

Para instâncias compatíveis com armazenamento de instâncias que não possam ser automaticamente recuperadas, recomendamos fazer o seguinte:

1. Abrir a instância de substituição em um novo Host dedicado a partir da AMI mais recente.
2. Migrar todos os dados necessários para a instância de substituição.
3. Encerrar a instância original no Host dedicado prejudicado.

Serviços relacionados

O Host dedicado se integra com os seguintes serviços:

- AWS License Manager: monitora licenças em seus hosts dedicados do Amazon EC2 (compatível somente nas regiões em que o AWS License Manager está disponível). Para obter mais informações, consulte o Manual do usuário do AWS License Manager.

Definição de preço

Não há cobranças adicionais para usar a recuperação do host; aplicam-se as cobranças usuais do Host dedicado. Para obter mais informações, consulte Definição de preço de hosts dedicados do Amazon EC2.

Assim que a recuperação for iniciada, você não será mais cobrado pelo Host dedicado prejudicado. A cobrança pelo host dedicado começa somente depois de entrar no estado `available`.

Se o Host dedicado prejudicado tiver sido cobrado usando a taxa sob demanda, o Host dedicado de substituição também são cobrados usando essa taxa. Se o Host dedicado prejudicado tiver um Reserva de hosts dedicados ativo, ele será transferido para o Host dedicado de substituição.

Manutenção de host

Com a manutenção de host, suas instâncias do Amazon EC2 no host dedicado degradado serão reinicializadas automaticamente em um host dedicado substituto durante um evento de manutenção programado. Isso ajuda a reduzir o tempo de inatividade das aplicações e transfere a carga pesada indiferenciada da manutenção para a AWS. A manutenção de host também é realizada para a manutenção planejada e rotineira do Amazon EC2.

A manutenção de host é compatível com todas as novas alocações de host dedicado feitas por meio do console Amazon EC2. Para qualquer host dedicado na sua Conta da AWS ou qualquer novo host dedicado alocado por meio da API AllocateHosts, você pode configurar a manutenção de host para os hosts dedicados compatíveis. Para ter mais informações, consulte the section called “Configurar manutenção de host”.

Conteúdo

- Conceitos básicos de manutenção de host
- Comparação entre manutenção de host e recuperação de host
- Tipos de instâncias compatíveis
- Instâncias em hosts dedicados
- Configurar manutenção de host
- Evento de manutenção
- Estados de manutenção de host
- Serviços relacionados
- Definição de preço

Conceitos básicos de manutenção de host

Quando é detectada a degradação de um host dedicado, um novo host dedicado é alocado. A degradação pode ser causada pela degradação do hardware subjacente ou pela detecção de certas condições problemáticas. As instâncias no host dedicado degradado estão programadas para reinicialização automática no host dedicado substituto.

O host dedicado de substituição recebe um novo ID de host, mas retém os mesmos atributos do host dedicado original. Esses atributos incluem o que se segue.

- Configurações de autoposicionamento
- Availability Zone (zona de disponibilidade)
- Reserva
- Afinidade de host
- Configurações de manutenção de host
- Configurações de recuperação de host
- Tipo de instância
- Tags

A manutenção de host está disponível em todas as Regiões da AWS para todos os hosts dedicados compatíveis. Para obter mais informações sobre hosts dedicados que não são compatíveis com manutenção de host, consulte the section called “Limitações”.

Seu host dedicado degradado é liberado após todas as suas instâncias terem sido reinicializadas em um novo host dedicado ou interrompidas. Você pode acessar as instâncias no host dedicado degradado antes do evento de manutenção programado, mas não é possível iniciar as instâncias no host dedicado degradado.

Você pode usar o host dedicado substituto para iniciar novas instâncias no host antes do evento de manutenção programado. No entanto, parte da capacidade de instância no host substituto será reservada para as instâncias que precisem ser migradas do host degradado. Não é possível executar novas instâncias nessa capacidade reservada. Para ter mais informações, consulte the section called “Instâncias em hosts dedicados”.

Limitações

- A manutenção de host não é compatível com o AWS Outposts, com o AWS Local Zones e com o AWS Wavelength Zones.
- A manutenção de host não pode ser ativada ou desativada para hosts que já estão em um grupo de recursos de host. Os hosts adicionados a um grupo de recursos de host retêm sua configuração de manutenção de host. Para obter mais informações, consulte Grupos de recursos de host.
- A manutenção de host só é compatível com determinados tipos de instância. Para ter mais informações, consulte the section called “Tipos de instâncias compatíveis”.

Comparação entre manutenção de host e recuperação de host

A seguinte tabela mostra as principais diferenças entre recuperação de host e manutenção de host.

	Recuperação do host	Manutenção de host
Acessibilidade	Inacessível	Acessível
State	`under-assessment`	`permanent-failure`
Ação	A recuperação é imediata	A manutenção é programada
Flexibilidade de agendamento	Não pode ser reagendada	Pode ser reagendada
Grupo de recursos de host	Compatível	Sem compatibilidade

Para obter mais informações sobre a recuperação de host, consulte Recuperação de host.

Tipos de instâncias compatíveis

A manutenção do host é compatível com as seguintes famílias de instâncias:

- Uso geral: `A1` | `M4` | `M5` | `M5a` | `M5n` | `M5zn` | `M6a` | `M6g` | `M6i` | `M6in` | `M7a` | `M7g` | `M7i` | `T3`
- Otimizada para computação: `C4` | `C5` | `C5a` | `C5n` | `C6a` | `C6g` | `C6gn` | `C6i` | `C6in` | `C7g` | `C7gn` | `C7i`
- Otimizadas para memória: `R4` | `R5` | `R5a` | `R5b` | `R5n` | `R6a` `R6g` | `R6i` | `R6in` | `R7a` | `R7g` | `R7iz` | `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `X2iezn`
- Computação acelerada: `G3` | `G5g` | `Inf1` | `P2` | `P3`

Instâncias em hosts dedicados

O Amazon EC2 reserva automaticamente a capacidade no host substituto para as instâncias que serão migradas automaticamente do host degradado. O Amazon EC2 não reserva capacidade no host substituto para instâncias que não possam ser migradas automaticamente, como instâncias com volumes raiz de armazenamento de instâncias. Não é possível executar novas instâncias usando a capacidade reservada.

> **Note**
>
> O console do Amazon EC2 mostra a capacidade reservada como capacidade usada. Pode parecer que as instâncias estão sendo executadas tanto no host degradado quanto no host substituto. No entanto, as instâncias continuarão sendo executadas somente no host degradado até que sejam interrompidas ou migradas para a capacidade reservada no host substituto.

Se você interromper manualmente uma instância no host degradado que possa ser migrada automaticamente, a capacidade que foi reservada para essa instância no host substituto será liberada e ficará disponível para uso.

Durante o evento da manutenção programada de host, as instâncias no host dedicado degradado serão reinicializadas automaticamente e migradas para a capacidade reservada no host dedicado substituto. As instâncias migradas retêm os mesmos atributos do host degradado, incluindo os que se seguem.

- Anexos de volume do Amazon EBS
- Endereços IP elásticos
- ID da instância
- Metadados da instância
- Endereço IP privado

Você pode interromper e iniciar uma instância no host degradado a qualquer momento antes do início do evento de manutenção programada. Essa ação reinicializará a instância em outro host, e ela não passará pela manutenção programada. Você deve atualizar a afinidade de host da instância para o novo host em que deseja reinicializar a instância. Se você interromper todas as instâncias no host degradado antes do início do evento de manutenção, o host degradado será liberado e o evento de manutenção será cancelado. Para ter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

> **Note**
>
> Os dados em qualquer volume de armazenamento local não são preservados quando você interrompe e inicia a instância.

As instâncias com um volume de armazenamento de instância como dispositivo raiz são encerradas após a data de encerramento especificada. Todos os dados em volumes de armazenamento de instância são excluídos quando as instâncias são encerradas. As instâncias encerradas são excluídas permanentemente e não podem ser iniciadas novamente. Para casos com volumes de armazenamento de instância como dispositivo raiz, recomendamos iniciar as instâncias de substituição em um host dedicado diferente usando a imagem de máquina da Amazon mais recente e migrar todos os dados disponíveis para as instâncias de substituição antes da data de encerramento especificada. Para obter mais informações, consulte Actions to take for instance retirement.

As instâncias que não podem ser reinicializadas automaticamente são interrompidas após a data especificada. Você pode iniciar essas instâncias novamente em um host diferente. As instâncias que usam um volume do Amazon EBS como dispositivo raiz continuam usando o mesmo volume do Amazon EBS após serem iniciadas em um novo host.

Você pode definir a ordem da reinicialização das instâncias reprogramando a hora de início da reinicialização de uma instância em https://console.aws.amazon.com/ec2/.

Configurar manutenção de host

Você pode configurar a manutenção de host para todos os hosts dedicados compatíveis via AWS Management Console ou AWS CLI. Para obter mais detalhes, consulte a tabela a seguir.

AWS Management Console

Para habilitar a manutenção de host para o host dedicado usando o AWS Management Console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione Host dedicado Ações > Modificar host.
4. Selecione ativado no campo Manutenção de host.

Para desabilitar a manutenção de host para o host dedicado usando o AWS Management Console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione Host dedicado Ações > Modificar host.

4. Selecione Desativado no campo Manutenção de host.

Para visualizar a configuração de manutenção de host para o host dedicado usando a AWS Management Console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o host dedicado e, na guia Descrição, revise o campo Manutenção de host.

AWS CLI

Para ativar ou desativar a manutenção de host para o novo host dedicado durante a alocação usando a AWS CLI.

Use o comando allocate-hosts.

Habilitar

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

Desabilitar

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

Para ativar ou desativar a manutenção de host para o host dedicado existente usando a AWS CLI.

Use o comando modify-hosts.

Habilitar

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

Desabilitar

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

Para visualizar a configuração de manutenção de host para o host dedicado usando a AWS CLI.

Use o comando describe-hosts.

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

> **Note**
>
> Se você desabilitar a manutenção de host, receberá uma notificação por e-mail para remover o host degradado e migrar manualmente as instâncias para outro host dentro de 28 dias. Um host substituto será alocado se você tiver uma reserva de host dedicado. Após 28 dias, as instâncias em execução no host degradado são encerradas e o host é liberado automaticamente.

Evento de manutenção

Após a detecção da degradação, um evento de manutenção é programado para 14 dias depois a fim de reinicializar as instâncias em um novo host dedicado. Você recebe uma notificação por e-mail com detalhes sobre o host degradado, o evento de manutenção programado e os horários de manutenção. Para obter mais informações, consulte Visualizar eventos programados.

Você pode reprogramar o evento de manutenção para qualquer dia até sete dias após a data do evento programado. Para obter mais informações sobre reprogramação, consulte Reprogramar um evento programado.

O evento de manutenção geralmente leva alguns minutos para ser concluído. No caso raro de um evento ser malsucedido, você recebe uma notificação por e-mail para remover as instâncias do host degradado dentro de um período de tempo especificado.

Estados de manutenção de host

O host dedicado é definido com o estado de `permanent-failure` quando a degradação é detectada. Você não pode iniciar instâncias em um host dedicado no estado de `permanent-failure`. Após a conclusão do evento de manutenção, o host degradado é liberado e colocado no estado de `released, permanent-failure`.

Após detectar a degradação em um host dedicado e antes de programar um evento de manutenção, a manutenção de host alocará automaticamente um host dedicado substituto à sua conta. Esse host substituto permanecerá em um estado `pending` até que um evento de manutenção seja programado. Após a programação do evento de manutenção, o host dedicado de substituição é alterado para o estado `available`.

Você pode usar o host dedicado substituto para iniciar novas instâncias no host antes do evento de manutenção programado. No entanto, parte da capacidade de instância no host substituto será reservada para as instâncias que precisem ser migradas do host degradado. Não é possível executar novas instâncias nessa capacidade reservada. Para ter mais informações, consulte the section called “Instâncias em hosts dedicados”.

Serviços relacionados

Host dedicado se integra com o AWS License Manager: rastreia licenças em todos os hosts dedicados do Amazon EC2 (disponível apenas nas regiões em que o AWS License Manager está disponível). Para obter mais informações, consulte o Manual do usuário do AWS License Manager.

Você deve ter licenças suficientes na Conta da AWS para o novo host dedicado. As licenças associadas ao host degradado são liberadas quando o host é liberado após a conclusão do evento de manutenção programado.

Definição de preço

Não há cobranças adicionais para usar a manutenção de host, mas as cobranças usuais do host dedicado se aplicam. Para obter mais informações, consulte Definição de preço de hosts dedicados do Amazon EC2.

Assim que a recuperação é iniciada, você deixa de ser mais cobrado pelo host dedicado degradado. A cobrança pelo host dedicado começa somente depois de entrar no estado `available`.

Se a cobrança do host dedicado degradado fosse realizada com base na taxa de sob demanda, o host dedicado substituto também será cobrado usando essa taxa. Se o host dedicado degradado tinha uma reserva de host dedicado ativa, ela será transferida para o host dedicado de substituição.

Monitorar alterações de configuração

É possível usar o AWS Config para gravar as alterações de configuração de hosts dedicados e de instâncias que são iniciadas, interrompidas ou encerradas neles. Em seguida, use as informações capturadas pelo AWS Config como fonte de dados para geração de relatórios de licenças.

O AWS Config grava individualmente as informações de configuração dos hosts dedicados e das instâncias e emparelha essas informações por meio de relacionamentos. Há três condições de geração de relatórios:

- Status de gravação do AWS Config: quando On (Ativado), o AWS Config está gravando um ou mais tipos de recursos da AWS que podem incluir hosts dedicados e instâncias dedicadas. Para capturar as informações necessárias para geração de relatórios de licenças, verifique se os hosts e as instâncias estão sendo gravados com os campos a seguir.
- Status de gravação do host — quando está Enabled (Habilitado), as informações de configuração de Hosts dedicados são gravadas.
- Instance recording status (Status de gravação da instância) — quando Enabled (Habilitado), as informações de configuração de Instâncias dedicadas são gravadas.

Se qualquer uma das três condições estiver desabilitada, o ícone do botão Edit Config Recording (Editar gravação de configuração) ficará vermelho. Para aproveitar todos os benefícios dessa ferramenta, verifique se os três métodos de gravação estão ativados. Quando os três estão ativados, o ícone fica verde. Para editar as configurações, escolha Edit Config Recording (Editar gravação de configuração). Você será direcionado à pagina Set up AWS Config (Configurar CC) no console do AWS Config, onde poderá configurar o AWS Config e começar a gravar em seus hosts, instâncias e outros tipos de recursos com suporte. Para obter mais informações, consulte Configuração do AWS Config para uso do console no Guia do desenvolvedor do AWS Config.

> **Note**
>
> O AWS Config grava seus recursos depois de descobri-los, o que pode levar vários minutos.

Depois que o AWS Config começa a gravar alterações de configuração nos hosts e nas instâncias, você obtém o histórico de configuração de qualquer host que tenha alocado ou liberado e qualquer instância que tenha executado, interrompido ou encerrado. Por exemplo, a qualquer momento no histórico de configuração de um Host dedicado, é possível pesquisar quantas instâncias são executadas nesse host, juntamente com o número de soquetes e núcleos no host. Para qualquer uma dessas instâncias, também é possível procurar o ID de sua imagem de máquina da Amazon (AMI). É possível usar essas informações para gerar relatórios de licenças para seu próprio software ligado ao servidor, que é licenciado por soquete ou por núcleo.

É possível visualizar os históricos de configuração de qualquer uma destas maneiras:

- Usando o console do AWS Config. Para cada recursos gravado, é possível visualizar uma página de linha do tempo, que fornece o histórico com detalhes de configuração. Para visualizar essa página, escolha o ícone cinza na coluna Config Timeline (Configurar linha de tempo) da página Hosts dedicados. Para obter mais informações, consulte Visualização de detalhes de configuração do console do AWS Config no Guia do desenvolvedor do AWS Config.
- Executando comandos da AWS CLI. Primeiro, é possível usar o comando list-discovered-resources para obter uma lista de todos os hosts e instâncias. Depois, é possível usar o comando get-resource-config-history para obter detalhes de configuração de um host ou instância para um intervalo de tempo específico. Para obter mais informações, consulte Visualização de detalhes de configuração usando a CLI no Guia do desenvolvedor do AWS Config.
- Usando a API do AWS Config em suas aplicações. Primeiro, é possível usar a ação ListDiscoveredResources para obter uma lista de todos os hosts e instâncias. Depois, é possível usar a ação GetResourceConfigHistory para obter detalhes de configuração de um host ou instância para um intervalo de tempo específico.

Por exemplo, para obter uma lista de todos os hosts dedicados do AWS Config, execute um comando da CLI como este:

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Para obter o histórico de configurações de um host dedicado do AWS Config, execute um comando da CLI como o a seguir.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

Para gerenciar as configurações do AWS Config usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página Hosts dedicados, escolha Edit Config Recording (Editar gravação de configuração).
3. No console do AWS Config, siga as etapas fornecidas para ativar a gravação. Para obter mais informações, consulte Configuração do AWS Config usando o console.

Para obter mais informações, consulte Visualização de detalhes de configuração no console do AWS Config.

Como ativar o AWS Config usando a linha de comando ou a API

- CLI da AWS: Visualizar detalhes da configuração (AWS CLI) no Guia do desenvolvedor do AWS Config.
- API do Amazon EC2: GetResourceConfigHistory.

Dedicated Instances

Por padrão, as instâncias EC2 são executadas em hardware de locação compartilhada. Isso significa que várias contas da AWS podem compartilhar o mesmo hardware físico.

As instâncias dedicadas são instâncias EC2 executadas em hardware dedicado a uma única conta da AWS. Isso significa que as instâncias dedicadas são isoladas fisicamente no nível de hardware do host em relação às instâncias pertencentes a outras Contas da AWS, mesmo que essas contas estejam vinculadas a uma única conta pagante. No entanto, as instâncias dedicadas podem compartilhar o hardware com outras instâncias da mesma Conta da AWS que não sejam instâncias dedicadas.

As instâncias dedicadas não oferecem visibilidade nem controle sobre o posicionamento das instâncias, além de não serem compatíveis com afinidade ao host. Se você parar e iniciar uma instância dedicada, talvez ela não seja executada no mesmo host. Da mesma forma, você não pode direcionar um host específico no qual iniciar ou executar uma instância. Além disso, as instâncias dedicadas oferecem um suporte limitado para o modelo traga a sua própria licença (BYOL).

Se você precisar de visibilidade e controle sobre o posicionamento da instância, além de compatibilidade mais abrangente com o modelo BYOL, avalie a possibilidade de usar um host dedicado. É possível usar instâncias dedicadas e hosts dedicados para iniciar instâncias do Amazon EC2 em servidores físicos dedicados. Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, há algumas diferenças básicas entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Servidor físico dedicado	Servidor físico com capacidade de instância totalmente dedicada para seu uso.	Um servidor físico dedicado a uma única conta de cliente.

	Dedicated Host	Dedicated Instance
Compartilhamento de capacidade de instância	Pode compartilhar a capacidade de instância com outras contas.	Sem compatibilidade
Faturamento	faturamento por host	Faturamento por instância
Visibilidade de soquetes, núcleos e ID de host	Fornece visibilidade do número de soquetes e núcleos físicos	Sem visibilidade
Afinidade de hosts e instâncias	permite implantar de forma consistente suas instâncias no mesmo servidor físico com o momento	Sem suporte
Posicionamento direcionado de instâncias	Proporciona visibilidade e controle adicionais sobre como as instâncias são colocadas em um servidor físico	Não suportado
Recuperação automática de instâncias	Compatível. Para ter mais informações, consulte Recuperação do host.	Compatível
Traga sua própria licença (BYOL)	Compatível	Suporte parcial *
Reservas de capacidade	Não compatível	Compatível

* O Microsoft SQL Server com Mobilidade de Licenças por meio do Software Assurance e as licenças do Windows Virtual Desktop Access (VDA) podem ser usadas com Instância dedicada.

Para obter mais informações sobre as instâncias dedicadas, consulte Dedicated Hosts.

Tópicos

- Conceitos básicos da Instâncias dedicadas
- Atributos compatíveis
- Limitações da Instâncias dedicadas
- Definição de preço para Instâncias dedicadas
- Como trabalhar com Instâncias dedicadas

Conceitos básicos da Instâncias dedicadas

Uma VPC pode ter uma locação de `default` ou `dedicated`. Por padrão, suas VPCs têm locação `default` e as instâncias lançadas em uma VPC de locação `default` têm locação `default`. Para iniciar instâncias dedicadas, faça o seguinte:

- Crie uma VPC com uma locação de `dedicated`, para que todas as instâncias na VPC sejam executadas como instâncias dedicadas. Para ter mais informações, consulte Criar uma VPC com uma locação de instância dedicada.
- Crie uma VPC com uma locação de `default` e especifique manualmente uma locação de `dedicated` para as instâncias que serão executadas como instâncias dedicadas. Para ter mais informações, consulte Executar Instâncias dedicadas em um VPC.

Atributos compatíveis

Instâncias dedicadas são compatíveis com os seguintes recursos e integrações de serviço da AWS:

Tópicos

- Instâncias reservadas
- Escalabilidade automática
- Recuperação automática
- Instâncias spot dedicadas
- Instâncias expansíveis

Instâncias reservadas

Para reservar capacidade para suas instâncias dedicadas, é possível comprar instâncias reservadas dedicadas ou reservas de capacidade. Para ter mais informações, consulte Reserved Instances e On-Demand Capacity Reservations.

Ao adquirir uma Instância reservada dedicada, você estará comprando capacidade de executar uma Instâncias dedicadas em uma VPC a uma taxa de uso muito reduzida. A redução de preço na cobrança de uso se aplica apenas quando você executa uma instância com locação dedicada. Quando você compra uma Instância reservada com locação padrão, ela se aplica somente a uma instância em execução com locação `default`. Ela não é aplicada a uma instância em execução com locação `dedicated`.

Você não pode usar o processo de modificação para alterar a locação de uma Instância reservada depois de adquiri-la. No entanto, é possível trocar uma Instância reservada convertível por uma nova Instância reservada convertível com uma locação diferente.

Escalabilidade automática

É possível usar o Amazon EC2 Auto Scaling para executar Instâncias dedicadas. Para obter mais informações, consulte Execução de instâncias do Auto Scaling em uma VPC no Guia do usuário do Amazon EC2 Auto Scaling.

Recuperação automática

É possível configurar a recuperação automática para uma instância dedicada se ela ficar impedida devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para ser reparado. Para ter mais informações, consulte Resiliência de instância.

Instâncias spot dedicadas

É possível executar uma instância spot dedicada especificando uma locação de `dedicated` ao criar uma solicitação de instâncias spot. Para ter mais informações, consulte Especificar uma locação para suas Instâncias spot.

Instâncias expansíveis

É possível aproveitar os benefícios da execução em hardware de locação dedicada com the section called “Instâncias expansíveis”. As instâncias dedicadas T3 são executadas no modo ilimitado por padrão, e elas fornecem um nível de linha de base de performance da CPU com a capacidade de

expansão para um nível de CPU mais alto quando exigido por sua workload. A performance basal da T3 e a capacidade de expansão são regidas por créditos de CPU. Devido à natureza expansível dos tipos de instância T3, recomendamos monitorar como suas instâncias T3 usam os recursos de CPU do hardware dedicado para obter a melhor performance. As instâncias dedicadas T3 destinam-se a clientes com workloads diversas que exibem comportamento aleatório da CPU, mas que, preferencialmente, têm o uso médio da CPU em ou abaixo dos usos da linha de base. Para ter mais informações, consulte the section called “Principais conceitos”.

O Amazon EC2 tem sistemas para identificar e corrigir a variabilidade na performance. No entanto, ainda é possível passar por variabilidade de curto prazo se você iniciar várias instâncias dedicadas T3 que tenham padrões correlacionados de uso da CPU. Para essas workloads mais exigentes ou correlacionadas, recomendamos o uso de instâncias dedicadas M5 ou M5a em vez de instâncias dedicadas T3.

Limitações da Instâncias dedicadas

Tenha o seguinte em mente ao usar instâncias dedicadas:

- Alguns serviços da AWS ou seus recursos não são compatíveis com uma VPC com a locação de instância definida como `dedicated`. Verifique a documentação do serviço para confirmar se há alguma limitação.
- Alguns tipos de instância não podem ser iniciados em uma VPC com a locação da instância definida como `dedicated`. Para obter mais informações sobre os tipos de instância compatíveis, consulte Instâncias dedicadas do Amazon EC2.
- Quando você iniciar uma instância dedicada compatível com o Amazon EBS, o volume do EBS não é executado em hardware de ocupante único.

Definição de preço para Instâncias dedicadas

A definição de preço de Instâncias dedicadas é diferente da definição de preço de Instâncias sob demanda. Para obter mais informações, consulte a página do produto de Instâncias dedicadas do Amazon EC2.

Como trabalhar com Instâncias dedicadas

É possível criar uma VPC com uma locação de instância `dedicated` para garantir que todas as instâncias executadas na VPC sejam Instâncias dedicadas. Como alternativa, é possível especificar a locação da instância durante a execução.

Tópicos

- Criar uma VPC com uma locação de instância dedicada
- Executar Instâncias dedicadas em um VPC
- Exibir informações de locação
- Altere a locação de uma instância
- Alterar a locação de uma VPC

Criar uma VPC com uma locação de instância dedicada

Ao criar uma VPC, você tem a opção de especificar sua locação de instância. Se você executar uma instância em uma VPC que tenha uma locação de instância de `dedicated`, a instância sempre será executada como instância dedicada em um hardware dedicado ao seu uso.

Para obter mais informações sobre como criar uma VPC e escolher as opções de locação, consulte Criar uma VPC no Guia do usuário da Amazon VPC.

Executar Instâncias dedicadas em um VPC

É possível executar uma Instâncias dedicadas usando o assistente de execução de instâncias do Amazon EC2.

Console

Para executar uma Instâncias dedicadas em uma VPC de locação padrão usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.

   > **Note**
   >
   > Escolha um tipo de instância que tenha suporte como uma Instâncias dedicadas. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.

6. Na seção Advanced details (Detalhes avançados), em Tenancy (Locação), selecione Dedicated (Dedicada).
7. Configure as demais opções da instância conforme necessário. Para ter mais informações, consulte Iniciar uma instância usando parâmetros definidos.
8. Escolha Iniciar instância.

Command line

Para configurar a opção de locação para uma instância durante a execução usando a linha de comando

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Para obter mais informações sobre a execução de uma instância com uma locação de `host`, consulte Execute instâncias em um Host dedicado..

Exibir informações de locação

Console

Para exibir as informações da locação da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Verifique a locação da instância de sua VPC na coluna Tenancy (Locação).
4. Se a coluna Locação não for exibida, selecione o ícone de configurações ( ) no canto superior direito, ative Locação e escolha Confirmar.

Para exibir as informações da locação da sua instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Verifique a locação da instância na coluna Tenancy (Locação).
4. Se a coluna Locação não for exibida, siga um destes procedimentos:

- Selecione o ícone de configurações
  ()
  no canto superior direito, ative Locação e escolha Confirmar.
- Selecione a instância. Na guia Details (Detalhes) perto da parte inferior da página, em Host and placement group (Host e grupo de posicionamento), verifique o valor de Tenancy (Locação).

Command line

Para descrever a locação da sua VPC usando a linha de comando

- describe-vpcs (AWS CLI)
- Get-EC2Vpc (AWS Tools for Windows PowerShell)

Para descrever a locação da sua instância usando a linha de comando

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Para descrever o valor da locação de uma Instância reservada usando a linha de comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Para descrever o valor da locação de uma oferta de Instância reservada usando a linha de comando

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering (AWS Tools for Windows PowerShell)

Altere a locação de uma instância

É possível alterar a locação de uma instância interrompida depois de iniciá-la. As alterações que você fizer entrarão em vigor na próxima vez que a instância for iniciada.

Os detalhes do sistema operacional da instância, e se o SQL Server está ou não instalado, afetam quais conversões são compatíveis. Para obter mais informações sobre os caminhos de conversão de locação disponíveis para a sua instância, consulte Tenancy conversion no License Manager User Guide.

> **Note**
>
> Para instâncias T3, você deve iniciar a instância em um host dedicado para usar uma locação de `host`. Você não pode alterar a locação de `host` para `dedicated` ou `default`. Tentar fazer uma dessas alterações de locação não compatíveis gera um código de erro de `InvalidRequest`.

Console

Para alterar a locação de uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Escolha Instance state (Estado da instância), Stop instance (Interromper instância), Stop (Interromper).
4. Escolha Actions (Ações), Instance Settings (Configurações da instância) e Modify Instance Placement (Modificar posicionamento da instância).
5. Na lista Tenancy (Locação), escolha se a instância será executada em um hardware dedicado ou em um Host dedicado. Escolha Save (Salvar).

Command line

Para modificar o valor da locação de uma instância usando a linha de comando

- modify-instance-placement (AWS CLI)
- Edit-EC2InstancePlacement (AWS Tools for Windows PowerShell)

Alterar a locação de uma VPC

É possível alterar a locação da instância de uma VPC de `dedicated` para `default` depois de criá-la. Alterar a locação da instância da VPC não afeta a locação de nenhuma instância existente

na VPC. Na próxima vez que você executar uma instância na VPC, ela terá a locação `default`, a menos que você especifique o contrário durante a execução.

> **Note**
>
> Você não pode alterar a locação da instância de uma VPC de `default` para `dedicated` depois de criá-la.

Você só pode modificar a locação da instância de uma VPC usando a AWS CLI, um AWS SDK ou a API do Amazon EC2.

Command line

Para modificar o atributo de locação da instância de uma VPC usando a AWS CLI

Use o comando modify-vpc-tenancy e especifique o ID da VPC e o valor da locação da instância. O único valor aceito é `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Reservas de capacidade

As reservas de capacidade permitem que você reserve capacidade computacional para as instâncias do Amazon EC2 em uma determinada zona de disponibilidade. Há dois tipos de reserva de capacidade, que atendem a casos de uso diferentes.

Tipos de reserva de capacidade

- On-Demand Capacity Reservations
- Blocos de capacidade para ML

Estes são alguns casos de uso comuns de reservas de capacidade sob demanda:

- Eventos de escalação: você pode criar reservas de capacidade sob demanda antes de eventos críticos para os negócios de modo a garantir que possa escalar quando necessário.

- Requisitos regulamentares e recuperação de desastres: use reservas de capacidade sob demanda para atender aos requisitos regulamentares de alta disponibilidade e reserve capacidade para recuperação de desastres em uma outra zona ou região de disponibilidade.

Estes são alguns casos de uso comuns de reservas de capacidade:

- Treinamento e ajuste fino de modelo de machine learning (ML): tenha acesso ininterrupto às instâncias de GPU que você reservou para concluir o treinamento e o ajuste fino do modelo de ML.
- Experimentos e protótipos de ML: executar experimentos e desenvolver protótipos que exigem instâncias de GPU por períodos curtos.

Quando usar reserva de capacidade sob demanda

Use reservas de capacidade sob demanda se você tiver requisitos rígidos de capacidade e estiver executando workloads críticas para os negócios que precisem de capacidade garantida. Com as reservas de capacidade sob demanda, você garante que sempre terá acesso à capacidade do Amazon EC2 que reservou, pelo tempo que precisar.

Quando usar blocos de capacidade para ML

Use blocos de capacidade para ML quando precisar garantir acesso ininterrupto às instâncias de GPU por um período de tempo definido, a partir de uma data futura. Os blocos de capacidade são ideais para treinar e ajustar modelos de ML, fazer pequenas execuções experimentais e lidar com picos temporários de demanda inferida no futuro. Com blocos de capacidade, você pode garantir que terá acesso aos recursos de GPU em uma data específica para executar as workloads de ML.

On-Demand Capacity Reservations

As Reservas de Capacidade sob demanda permitem que você reserve capacidade computacional para suas instâncias do Amazon EC2 por qualquer duração em uma determinada zona de disponibilidade. As reservas de capacidade reduzem o risco da impossibilidade de obter capacidade sob demanda, caso haja restrições de capacidade. Se você tem requisitos rígidos de capacidade e está executando workloads essenciais para os negócios que exigem um certo nível de garantia de capacidade a longo ou curto prazo, recomendamos que você crie uma reserva de capacidade para garantir que sempre tenha acesso à capacidade do Amazon EC2 quando precisar, pelo tempo que precisar.

É possível criar reservas de capacidade a qualquer momento, sem entrar em um termo de compromisso de um ou três anos. A capacidade torna-se disponível e a cobrança começa assim

que a reserva de capacidade é provisionada na conta. Quando você não precisar mais de garantia de capacidade, cancele a reserva de capacidade para liberar capacidade e evitar cobranças. Você também pode usar os descontos de cobrança oferecidos pelos Savings Plans e instâncias reservadas regionais para reduzir o custo de uma reserva de capacidade.

Ao criar uma Reserva de capacidade, especifique:

- A zona de disponibilidade na qual reservar a capacidade
- O número de instâncias para as quais reservar capacidade
- Os atributos da instância, incluindo o tipo de instância, a plataforma, a zona de disponibilidade e a locação

Reservas de Capacidade só podem ser usadas por instâncias que correspondam aos seus atributos. Por padrão, elas são usadas automaticamente por instâncias em execução que correspondem aos atributos. Se você não tiver nenhuma instância em execução que corresponda aos atributos da Reserva de capacidade, ela permanecerá não utilizada até você executar uma instância com atributos correspondentes.

Conteúdo

- Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans
- Plataformas compatíveis
- Cotas
- Limitações
- Definição de preços e faturamento da Reserva de capacidade
- Como trabalhar com Reservas de Capacidade
- Trabalhar com grupos de Reserva de capacidade
- As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster
- Reservas de Capacidade em zonas locais
- Reservas de Capacidade em zonas Wavelength
- Reservas de Capacidade no AWS Outposts
- Como trabalhar com Reservas de Capacidade compartilhadas
- Frotas de reserva de capacidade
- Monitoramento de reservas de capacidade

Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans

A tabela a seguir destaca as principais diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans:

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
Prazo	Nenhum compromisso é necessário. Podem ser criadas e canceladas conforme necessário.	Exige compromisso fixo de um ano ou de três anos		
Benefício da capacidade	Capacidade reservada em uma zona de disponibilidade específica.		Nenhuma capacidade reservada.	
Desconto de faturamento	Sem desconto de faturamento. †	Fornece um desconto de faturamento.		
Limites de instâncias	Seus limites instância sob demanda por região se aplicam.	O padrão é 20 por zona de disponibilidade. É possível solicitar um aumento de limite.	O padrão é 20 por região. É possível solicitar um aumento de limite.	Sem limite.

† É possível combinar Reservas de Capacidade com Savings Plans ou instâncias reservadas regionais para receber um desconto.

Para obter mais informações, consulte:

- Reserved Instances
- Guia do usuário do Savings Plans

Plataformas compatíveis

É necessário criar a reserva de capacidade com a plataforma correta para garantir que ela corresponda corretamente às suas instâncias. As Reservas de Capacidade oferecem suporte às plataformas a seguir:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL com SQL Server Standard
- RHEL com SQL Server Enterprise
- RHEL com SQL Server Web
- RHEL com HA
- RHEL com HA e SQL Server Standard
- RHEL com HA e SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows com SQL Server
- Windows com SQL Server Web
- Windows com SQL Server Standard
- Windows com SQL Server Enterprise

Quando adquire uma Reserva de capacidade, escolha uma oferta para uma plataforma que represente o sistema operacional da sua instância.

- Para distribuições SUSE Linux e RHEL, excluindo BYOL, escolha a plataforma específica. Por exemplo, a plataforma SUSE Linux ou Red Hat Enterprise Linux .

- Para todas as demais distribuições do Linux (incluindo Ubuntu), escolha uma oferta para a plataforma Linux/UNIX.
- Se você trouxer sua assinatura RHEL (BYOL) existente, deve escolher a plataforma Linux/UNIX .
- Para Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web, escolha a plataforma específica.
- Para todas as outras versões do Windows, excluindo BYOL, que não é aceito, escolha a plataforma Windows.

Cotas

O número de instâncias para as quais você tem permissão para reservar capacidade é baseado na cota de instância sob demanda de sua conta. É possível reservar capacidade para todas as instâncias permitidas pela cota, menos o número de instâncias que já estão em execução.

As cotas se aplicam somente às instâncias em execução. Se sua instância estiver pendente, sendo interrompida, tiver sido interrompida ou hibernada, ela não será contabilizada para a sua cota.

Limitações

Antes de criar Reservas de Capacidade, observe as seguintes limitações e restrições.

- Reservas de Capacidade ativas e não utilizadas entram na contagem dos limites de instância sob demanda.
- As Reservas de Capacidade não são transferíveis de uma conta da AWS para outra. Entretanto, é possível compartilhar reservas de capacidade com outras contas da AWS. Para ter mais informações, consulte Como trabalhar com Reservas de Capacidade compartilhadas.
- Os descontos de faturamento Instância reservada de zona não se aplicam às Reservas de Capacidade.
- É possível criar reservas de capacidade em grupos de posicionamento de cluster. Não há suporte para grupos de posicionamento disseminados e de partição.
- As Reservas de Capacidade não podem ser usadas com Hosts dedicados. As reservas de capacidade não podem ser usadas com instâncias dedicadas.
- [Instâncias do Windows] Não é possível usar as reservas de capacidade com o modelo de licenciamento traga a sua própria licença (BYOL).
- O Reservas de Capacidade não garante que uma instância hibernada possa retomar depois de tentar iniciá-la.

Definição de preços e faturamento da Reserva de capacidade

Tópicos

- Definição de preço
- Faturamento
- Descontos de faturamento
- Visualizar sua fatura

Definição de preço

A reserva de capacidade é cobrada pela taxa sob demanda equivalente independentemente de executar instâncias na capacidade reservada ou não. Se você não usar a reserva, ela será exibida como uma reserva não utilizada em sua fatura do Amazon EC2. Quando executa uma instância que corresponde aos atributos de uma reserva, você paga apenas pela instância e nada pela reserva. Não há cobranças antecipadas ou adicionais.

Por exemplo, se criar uma Reserva de capacidade para 20 instâncias `m4.large` do Linux e executar 15 instâncias `m4.large` do Linux na mesma zona de disponibilidade, você será cobrado por 15 instâncias ativas e por 5 instâncias não usadas na reserva.

Descontos de faturamento para Savings Plans e instâncias reservadas regionais aplicam-se a reservas de capacidade. Para ter mais informações, consulte Descontos de faturamento.

Para obter mais informações, consulte Definição de preço Amazon EC2.

Faturamento

O faturamento começa assim que a Reserva de capacidade for provisionada na conta. Ele prosseguirá enquanto a Reserva de capacidade permanecer provisionada na conta.

As Reservas de Capacidade são cobradas por granularidade por segundo. Isso significa que você é cobrado por horas parciais. Por exemplo, se uma reserva de capacidade permanecer provisionada em sua conta por `24` horas e `15` minutos, você será cobrado por `24.25` horas de reserva.

O exemplo a seguir mostra como uma Reserva de capacidade é cobrada. A Reserva de capacidade é criada para uma instância `m4.large` do Linux, que tem uma taxa sob demanda de 0,10 USD por hora de uso. Neste exemplo, a Reserva de capacidade está provisionada na conta por cinco horas. A Reserva de capacidade não é usada na primeira hora, portanto, é cobrada por uma hora não

utilizada na taxa sob demanda padrão do tipo de instância `m4.large`. Das duas às cinco horas, a Reserva de capacidade é ocupada por uma instância `m4.large`. Durante esse período, a Reserva de capacidade não acumula cobranças e, em vez disso, a conta é cobrada pela instância `m4.large` que a está ocupando. Na sexta hora, a Reserva de capacidade é cancelada, e a instância `m4.large` é executada normalmente fora da capacidade reservada. Para essa hora, ela é cobrada pela taxa sob demanda do tipo de instância `m4.large`.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Descontos de faturamento

Os descontos de faturamento para Savings Plans e instâncias reservadas regionais aplicam-se a reservas de capacidade. A AWS aplica automaticamente esses descontos às reservas de capacidade que têm atributos correspondentes. Quando uma Reserva de capacidade é usada por uma instância, o desconto é aplicado à instância. Os descontos são preferencialmente aplicados ao uso de instâncias antes de cobrir Reservas de Capacidade não utilizadas.

Os descontos de faturamento de Instâncias reservadas zonais não se aplicam às Reservas de Capacidade.

Para obter mais informações, consulte:

- Reserved Instances
- Guia do usuário do Savings Plans
- Opções de faturamento e compra

Visualizar sua fatura

É possível revisar as cobranças e taxas da sua conta no console do AWS Billing and Cost Management.

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Reservas de Capacidade.

É possível visualizar as cobranças online ou baixar um arquivo CSV. Para obter mais informações, consulte Itens de linha da reserva de capacidade no Manual do usuário do AWS Billing and Cost Management.

Como trabalhar com Reservas de Capacidade

Para começar a usar as Reservas de Capacidade, crie a reserva de capacidade na zona de disponibilidade exigida. Depois, é possível executar instâncias na capacidade reservada, visualizar a utilização da capacidade em tempo real e aumentar ou diminuir a capacidade conforme necessário.

Por padrão, as reservas de capacidade correspondem automaticamente às novas instâncias e às instâncias em execução que têm atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação). Isso significa que qualquer instância com atributos correspondentes são automaticamente executadas na Reserva de capacidade. No entanto, também é possível destinar uma Reserva de capacidade para workloads específicas. Isso permite que você controle explicitamente quais instâncias têm permissão para executar na capacidade reservada.

É possível especificar como a reserva termina. É possível escolher cancelar o(a) Reserva de capacidade ou encerrá-lo(a) automaticamente em um horário especificado. Se você especificar um horário de término, a Reserva de capacidade será cancelada dentro de uma hora do horário especificado. Por exemplo, se você especificar, 5/31/2019, 13:30:55, a Reserva de capacidade será encerrada entre 13:30:55 e 14:30:55 em 5/31/2019. Após o término da reserva, você não poderá mais destinar instâncias à Reserva de capacidade. Instâncias em execução na capacidade reservada continuam a executar sem interrupção. Se as instâncias que estão destinando uma Reserva de capacidade forem interrompidas, você não poderá reiniciá-las até que a preferência de destino na Reserva de capacidade seja removida ou que você as configure para destinar uma Reserva de capacidade diferente.

Sumário

- Criar uma Reserva de capacidade
- Iniciar instâncias em uma Reserva de capacidade existente
- Modifique uma Reserva de capacidade
- Modificar as configurações da Reserva de capacidade de uma instância
- Visualizar uma Reserva de capacidade
- Cancelar uma Reserva de capacidade

Criar uma Reserva de capacidade

Se sua solicitação para criar uma reserva de capacidade for bem-sucedida, a capacidade será disponibilizada imediatamente. A capacidade permanece reservada para seu uso enquanto a Reserva de capacidade estiver ativa, e é possível executar instâncias nela a qualquer momento. Se a Reserva de capacidade estiver aberta, as novas instâncias e as instâncias existentes que tiverem atributos correspondentes serão executadas automaticamente na capacidade da Reserva de capacidade. Se a Reserva de capacidade for `targeted`, as instâncias deverão usá-la como destino especificamente para executar na capacidade reservada.

Sua solicitação de criação de uma Reserva de capacidade poderá falhar se uma das seguintes opções for verdadeira:

- O Amazon EC2 não tem capacidade suficiente para realizar a solicitação. Tente novamente mais tarde, tente uma zona de disponibilidade diferente ou tente uma solicitação menor. Se a sua aplicação for flexível entre tipos e tamanhos de instâncias, tente diferentes atributos de instância.
- A quantidade solicitada excede o limite de instância sob demanda para a família de instâncias selecionada. Aumente o limite de instância sob demanda para a família de instâncias e tente novamente. Para ter mais informações, consulte Cotas de instância sob demanda.

Para criar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).
3. Na página Create a Reserva de capacidade (Criar uma Reserva de capacidade), defina as seguintes configurações na seção Instance details (Detalhes da instância): O tipo de instância, a plataforma, a zona de disponibilidade e a locação das instâncias que você iniciar devem corresponder ao tipo de instância, à plataforma, à zona de disponibilidade e à locação especificadas aqui, ou não será possível aplicar a reserva de capacidade. Por exemplo, se uma Reserva de capacidade aberta não corresponder, a execução de uma instância que for destinada a essa Reserva de capacidade explicitamente falhará.

    a. Instance Type (Tipo de instância) — o tipo de instância a ser executada na capacidade reservada.

    b. Launch EBS-optimized instances (Executar instâncias otimizadas para EBS) — especifique se deseja reservar a capacidade para instâncias otimizadas para EBS. Essa opção é

selecionada por padrão para alguns tipos de instância. Para ter mais informações, consulte the section called “Otimização de EBS”.

c. Platform (Plataforma) — o sistema operacional das suas instâncias. Para ter mais informações, consulte Plataformas compatíveis.

d. Availability Zone (Zona de disponibilidade) — a zona de disponibilidade na qual reservar a capacidade.

e. Tenancy (Locação) — especifique se você quer executar em hardware compartilhado (padrão) ou em uma instância dedicada.

f. (Opcional) Placement group ARN (ARN do grupo de posicionamento): o ARN do grupo de posicionamento de cluster no qual criar a nova reserva de capacidade.

   Para ter mais informações, consulte As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster.

g. Quantity (Quantidade) — o número de instâncias para as quais reservar a capacidade. Se você especificar uma quantidade que exceda seu limite de instância sob demanda restante para o tipo de instância selecionado, a solicitação será negada.

4. Defina as seguintes configurações na seção Reservation details (Detalhes da reserva):

   a. Reservation Ends (Término da reserva) — escolha somente uma das duas opções a seguir:

      - Manually (Manualmente) — reserve a capacidade até que você a cancele explicitamente.
      - Specific time (Horário específico) — cancele a reserva de capacidade automaticamente na data e na hora especificadas.

   b. Instance eligibility (Qualificação de instância) — escolha uma das seguintes opções:

      - open: (Padrão) a reserva de capacidade corresponde a qualquer instância que tenha atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação). Se você executar uma instância com atributos correspondentes, ela será colocada na capacidade reservada automaticamente.
      - targeted: a reserva de capacidade aceita somente instâncias que tenham atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação) e que visem explicitamente a reserva.

5. Escolha Request reservation (Solicitar reserva).

Para criar uma reserva de capacidade usando a AWS CLI

Use o comando create-capacity-reservation. Para ter mais informações, consulte Plataformas compatíveis.

O comando apresentado a seguir cria uma reserva de capacidade que reserva capacidade para três instâncias `m5.2xlarge` que executam AMIs do Red Hat Enterprise Linux na zona de disponibilidade `us-east-1a`.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red
 Hat Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

O comando apresentado a seguir cria uma reserva de capacidade que reserva capacidade para três instâncias `m5.2xlarge` que executam o Windows com AMIs do SQL Server na zona de disponibilidade `us-east-1a`.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

Iniciar instâncias em uma Reserva de capacidade existente

Ao executar uma instância, é possível especificar se deseja executá-la em qualquer Reserva de capacidade `open`, em uma Reserva de capacidade específica ou em um grupo de Reservas de Capacidade. Você pode iniciar uma instância somente em uma reserva de capacidade que tenha atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e capacidade suficiente. Se preferir, configure a instância para evitar a execução em um Reserva de capacidade, mesmo que você tenha uma Reserva de capacidade `open` com atributos correspondentes e capacidade disponível.

A execução de uma instância em uma Reserva de capacidade reduz a capacidade disponível pelo número de instâncias executadas. Por exemplo, se você executar três instâncias, a capacidade disponível da Reserva de capacidade será reduzida em três.

Para executar instâncias em uma Reserva de capacidade existente usando o console

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para especificar as configurações para o grupo de posicionamento e a reserva de capacidade.
2. Expanda os Detalhes avançados e faça o seguinte:

a. Em Grupo de posicionamento, selecione o grupo de posicionamento de cluster no qual deseja executar a instância.

b. Em Capacity Reservation (Reserva de capacidade), escolha uma das seguintes opções dependendo da configuração da reserva de capacidade:

- Nenhuma: impede que as instâncias sejam executadas em uma reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
- Aberta: executa as instâncias em qualquer reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas. Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.
- Destino por ID: executa as instâncias na reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.
- Destino por grupo: executa as instâncias em qualquer reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.

3. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Para iniciar uma instância em uma reserva de capacidade existente usando a AWS CLI

Use o comando run-instances e especifique o parâmetro `--capacity-reservation-specification`.

O exemplo a seguir executa uma instância `t2.micro` em qualquer Reserva de capacidade aberta que tenha atributos correspondentes e capacidade disponível:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

O exemplo a seguir executa uma instância `t2.micro` em uma Reserva de capacidade `targeted`:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

O exemplo a seguir executa uma instância `t2.micro` em um grupo de Reserva de capacidade:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
 --instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Modifique uma Reserva de capacidade

É possível alterar os atributos de uma Reserva de capacidade ativa depois de criá-la. Não é possível modificar uma Reserva de capacidade depois que ela expirar ou depois de você cancelá-la explicitamente.

Ao modificar uma Reserva de capacidade, você só pode aumentar ou diminuir a quantidade e alterar a maneira como ela é lançada. Não é possível alterar o tipo de instância, a otimização de EBS, a plataforma, a zona de disponibilidade nem a qualificação de instâncias de uma reserva de capacidade. Se for necessário modificar qualquer um desses atributos, recomendamos cancelar a reserva e, em seguida, criar uma nova com os atributos necessários.

Se você especificar uma nova quantidade que exceda seu limite de instância sob demanda restante para o tipo de instância selecionada, a atualização falhará.

Para modificar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Reservas de Capacidade, selecione a Reserva de capacidade a ser modificada e, em seguida, escolha Edit (Editar).
3. Modifique as opções Quantity (Quantidade) ou Reservation ends (Término da reserva) conforme necessário e escolha Save changes (Salvar alterações).

Para modificar uma reserva de capacidade usando a AWS CLI

Use o comando modify-capacity-reservation:

Por exemplo, o comando a seguir modifica uma Reserva de capacidade para reservar capacidade para oito instâncias.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --
instance-count 8
```

Modificar as configurações da Reserva de capacidade de uma instância

É possível modificar as configurações da Reserva de capacidade a seguir para uma instância interrompida a qualquer momento:

- Inicie em qualquer reserva de capacidade que tenha atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e capacidade disponível.
- Execute a instância em uma Reserva de capacidade específica.
- Inicie em qualquer reserva de capacidade que tenha atributos correspondentes e capacidade disponível em um grupo de reserva de capacidade
- Impeça que a instância seja iniciada em uma Reserva de capacidade.

Para modificar as configurações da Reserva de capacidade de uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instances (Instâncias) e selecione a instância a ser modificada. Interrompa a instância se ela ainda não tiver sido interrompida.
3. Escolha Ações, Configurações da instância, Modificar configurações da reserva de capacidade.
4. Para Reserva de capacidade, selecione uma das seguintes opções:
   - Open (Aberta) — executa as instâncias em qualquer Reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas. Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.
   - None (Nenhuma) — impede que as instâncias sejam executadas em uma Reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
   - Specify Capacity Reservation (Especificar reserva de capacidade) — executa as instâncias na Reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.

- Specify Capacity Reservation group (Especificar grupo de reserva de capacidade) — executa as instâncias em qualquer Reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de Reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.

Para modificar as configurações da reserva de capacidade de uma instância usando a AWS CLI

Use o comando modify-instance-capacity-reservation-attributes.

Por exemplo, o comando a seguir altera a configuração da Reserva de capacidade de uma instância para `open` ou `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationPreference=none|open
```

Por exemplo, o comando a seguir modifica uma instância para ter como destino uma Reserva de capacidade específica.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Por exemplo, o comando a seguir modifica uma instância para ter como destino um grupo de Reserva de capacidade específico.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Visualizar uma Reserva de capacidade

As Reservas de Capacidade têm estes estados possíveis:

- `active` — a capacidade está disponível para uso.
- `expired` — a Reserva de capacidade expirou automaticamente na data e hora especificadas em sua solicitação de reserva. A capacidade reservada não está mais disponível para uso.

- `cancelled`—O(A) Reserva de capacidade foi cancelado(a). A capacidade reservada não está mais disponível para uso.
- `pending` — a solicitação de Reserva de capacidade foi bem-sucedida, mas o provisionamento da capacidade ainda está pendente.
- `failed` — a solicitação da Reserva de capacidade falhou. Uma solicitação pode falhar devido a parâmetros de solicitação que não são válidos, restrições da capacidade ou restrições de limite da instância. É possível visualizar uma solicitação com falha por 60 minutos.

> **Note**
>
> Devido ao modelo de consistência eventual seguido pelas APIs do Amazon EC2, depois de criar uma reserva de capacidade, pode levar até cinco minutos para o console e o describe-capacity-reservations responder indicando que a reserva de capacidade está no estado `active`. Durante esse tempo, o console e a resposta `describe-capacity-reservations` podem indicar que a Reserva de capacidade está no estado `pending`. No entanto, a Reserva de capacidade pode já estar disponível para uso e é possível tentar iniciar instâncias nela.

Para visualizar as Reservas de Capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Reservas de Capacidade e selecione uma Reserva de capacidade para visualizar.
3. Escolha View launched instances for this reservation (Visualizar instâncias executadas para essa reserva)

Para visualizar as Reservas de Capacidade usando a AWS CLI

Use o comando describe-capacity-reservations:

Por exemplo, o comando a seguir descreve todas as Reservas de Capacidade.

```
aws ec2 describe-capacity-reservations
```

Saída de exemplo.

```
{
```

```
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```


Cancelar uma Reserva de capacidade

É possível cancelar uma Reserva de capacidade a qualquer momento se não precisar mais da capacidade reservada. Quando você cancela uma Reserva de capacidade, a capacidade é liberada imediatamente e não é mais reservada para seu uso.

É possível cancelar Reservas de Capacidade vazias e Reservas de Capacidade que têm instâncias em execução. Se você cancelar uma reserva de capacidade que tenha instâncias em execução, as instâncias continuarão a ser executadas normalmente fora da reserva da capacidade em tarifas padrão de instância sob demanda ou em uma tarifa com desconto, se você tiver um Savings Plan ou uma instância reservada regional correspondente.

Depois que você cancela uma Reserva de capacidade, as instâncias que a usavam como destino não podem mais ser executadas. Modifique essas instâncias para que elas tenham outra Reserva de capacidade como destino, sejam executadas em uma Reserva de capacidade aberta com atributos correspondentes e capacidade suficiente ou evitem a execução em uma Reserva de capacidade. Para ter mais informações, consulte Modificar as configurações da Reserva de capacidade de uma instância.

Para cancelar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Reservas de Capacidade e selecione a Reserva de capacidade a ser cancelada.
3. Escolha Cancel reservation (Cancelar reserva), Cancel reservation (Cancelar reserva).

Para cancelar uma reserva de capacidade usando a AWS CLI

Use o comando cancel-capacity-reservation:

Por exemplo, o comando a seguir cancela uma Reserva de capacidade com um ID `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Trabalhar com grupos de Reserva de capacidade

É possível usar o AWS Resource Groups para criar coleções lógicas de Reservas de Capacidade, chamadas grupos de recursos. Um grupo de recursos é um agrupamento lógico de recursos da AWS que estão todos na mesma região da AWS. Para obter mais informações sobre grupos de recursos, consulte O que são grupos de recursos? no Guia do usuário do AWS Resource Groups.

É possível incluir reservas de capacidade de sua propriedade em sua conta e reservas de capacidade compartilhadas com você por outras contas da AWS em um único grupo de recursos. Além disso, é possível incluir reservas de capacidade com atributos diferentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) em um único grupo de recursos.

Ao criar grupos de recursos para reservas de capacidade, é possível direcionar instâncias para um grupo de reservas de capacidade em vez de uma reserva de capacidade individual. As instâncias direcionadas a um grupo de reservas de capacidade correspondem a qualquer reserva de capacidade no grupo que tenha atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e capacidade disponível. Se o grupo não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas usando a capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a correspondência da instância será automática e ela será movida para sua capacidade reservada.

Para evitar o uso não intencional de Reservas de Capacidade em um grupo, configure as Reservas de Capacidade no grupo para aceitar somente as instâncias que se dirigem explicitamente à reserva de capacidade. Para fazer isso, defina Instance eligibility (Qualificação de instâncias) como targeted (direcionadas) ou Only instances that specify this reservation (Somente instâncias que especificam essa reserva) (novo console) ao criar a Reserva de capacidade usando o console do Amazon EC2. Ao usar a AWS CLI, especifique `--instance-match-criteria targeted` ao criar a reserva de capacidade. Isso garante que somente as instâncias explicitamente direcionadas ao grupo, ou a uma Reserva de capacidade no grupo, possam ser executadas no grupo.

Se uma Reserva de capacidade em um grupo for cancelada ou expirar enquanto tiver instâncias em execução, as instâncias serão automaticamente movidas para outra Reserva de capacidade no grupo que tenha atributos correspondentes e capacidade disponível. Se não houver Reservas de Capacidade restantes no grupo que tenham atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a instância será automaticamente movida para sua capacidade reservada.

Tópicos

- Criar um grupo de reserva de capacidade
- Adicionar uma reserva de capacidade a um grupo
- Visualizar as reservas de capacidade em um grupo
- Visualizar os grupos aos quais uma reserva de capacidade pertence
- Remover uma reserva de capacidade de um grupo
- Excluir um grupo de reserva de capacidade

Criar um grupo de reserva de capacidade

Como criar um grupo para reservas de capacidade

Use o comando create-group da AWS CLI. Para `name`, forneça um nome descritivo para o grupo e, para `configuration`, especifique dois parâmetros de solicitação `Type`:

- `AWS::EC2::CapacityReservationPool` para garantir que o grupo de recursos possa ser direcionado para execuções de instâncias
- `AWS::ResourceGroups::Generic` com `allowed-resource-types` definido como `AWS::EC2::CapacityReservation` para garantir que o grupo de recursos aceite apenas Reservas de Capacidade

Por exemplo, o comando a seguir cria um grupo chamado `MyCRGroup`.

```
aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Veja a seguir um exemplo de saída.

```
{
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
```

```
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Adicionar uma reserva de capacidade a um grupo

Se você adicionar uma reserva de capacidade compartilhada com você a um grupo e essa reserva de capacidade não for compartilhada, ela será automaticamente removida do grupo.

Como adicionar uma Reserva de capacidade a um grupo

Use o comando group-resources da AWS CLI. Para `group`, especifique o nome do grupo ao qual adicionar as Reservas de Capacidade e, para `resources`, especifique ARNs de Reservas de Capacidade a serem adicionadas. Para adicionar várias Reservas de Capacidade, separe os ARNs com um espaço. Para obter os ARNs do Reservas de Capacidade para adicionar, use o comando describe-capacity-reservations da AWS CLI e especifique os IDs das Reservas de Capacidade.

Por exemplo, o comando a seguir adiciona duas Reservas de Capacidade a um grupo chamado `MyCRGroup`.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Veja a seguir um exemplo de saída.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Visualizar as reservas de capacidade em um grupo

Como visualizar as Reservas de Capacidade em um grupo específico

Use o comando list-group-resources da AWS CLI. Para `group`, especifique o nome do grupo.

Por exemplo, o comando a seguir lista as Reservas de Capacidade em um grupo chamado `MyCRGroup`.

```
aws resource-groups list-group-resources --group MyCRGroup
```

Veja a seguir um exemplo de saída.

```
{
    "QueryErrors": [],
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

> **Note**
>
> A saída do comando inclui reservas de capacidade de sua propriedade e reservas de capacidade compartilhadas com você.

Visualizar os grupos aos quais uma reserva de capacidade pertence

AWS CLI

Como visualizar os grupos aos quais uma reserva de capacidade específica foi adicionada

Use o comando get-groups-for-capacity-reservation da AWS CLI.

Por exemplo, o comando a seguir lista os grupos aos quais a Reserva de capacidade `cr-1234567890abcdef1` foi adicionada.

```
aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

Veja a seguir um exemplo de saída.

```
{
    "CapacityReservationGroups": [
        {
            "OwnerId": "123456789012",
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/
MyCRGroup"
        }
    ]
}
```

> **Note**
>
> Se você especificar uma reserva de capacidade compartilhada com você, o comando retornará apenas os grupos de reserva de capacidade de sua propriedade.

Amazon EC2 console

Como visualizar os grupos aos quais uma reserva de capacidade específica foi adicionada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade, selecione a Reserva de capacidade a ser visualizada e escolha View (Visualizar).

   Os grupos aos quais a Reserva de capacidade foi adicionada são listados no cartão Groups (Grupos).

> **Note**
>
> Se você escolher uma reserva de capacidade compartilhada com você, o console exibirá apenas os grupos de reserva de capacidade de sua propriedade.

Remover uma reserva de capacidade de um grupo

Como remover uma Reserva de capacidade de um grupo

Use o comando ungroup-resources da AWS CLI. Para `group`, especifique o ARN do grupo do qual remover a Reserva de capacidade e, para `resources`, especifique os ARNs das Reservas de Capacidade a serem removidas. Para remover várias Reservas de Capacidade, separe os ARNs com um espaço.

O exemplo a seguir remove duas Reservas de Capacidade de um grupo chamado `MyCRGroup`.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Veja a seguir um exemplo de saída.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Excluir um grupo de reserva de capacidade

Para excluir um grupo

Use o comando delete-group da AWS CLI. Para `group`, forneça o nome do grupo a ser excluído.

Por exemplo, o comando a seguir exclui um grupo chamado `MyCRGroup`.

```
aws resource-groups delete-group --group MyCRGroup
```

Veja a seguir um exemplo de saída.

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
```

```
        "Name": "MyCRGroup"
    }
}
```

As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster

É possível criar reservas de capacidade em um grupo de posicionamento de cluster para reservar a capacidade computacional do Amazon EC2 para suas workloads. Os grupos de posicionamento de cluster oferecem o benefício de baixa latência de rede e alta throughput de rede.

Criar uma reserva de capacidade em um grupo de posicionamento de cluster garante que você tenha acesso à capacidade de computação nos grupos de posicionamento de cluster quando precisar dela, pelo tempo necessário. Isso é ideal para reservar capacidade para workloads de alta performance (HPC) que exigem escalabilidade computacional. Isso permite que você diminua a escala do cluster, garantindo que a capacidade permaneça disponível para seu uso, para que você possa escalar o backup quando necessário.

Tópicos

- Limitações
- Trabalhar com reservas de capacidade em grupos de posicionamento de cluster

Limitações

Lembre-se do seguinte ao criar reservas de capacidade em grupos de posicionamento de cluster:

- Se uma reserva de capacidade existente não estiver em um grupo de posicionamento, não será possível modificar a reserva de capacidade para reservar capacidade em um grupo de posicionamento. Para reservar capacidade em um grupo de posicionamento, crie a reserva de capacidade no grupo de posicionamento.
- Depois de criar uma reserva de capacidade em um grupo de posicionamento, você não poderá modificá-la para reservar capacidade fora do grupo de posicionamento.
- É possível aumentar sua capacidade reservada em um grupo de posicionamento modificando uma reserva de capacidade existente no grupo de posicionamento ou criando reservas de capacidade adicionais no grupo de posicionamento. No entanto, você aumenta suas chances de obter um erro de capacidade insuficiente.
- Não é possível compartilhar reservas de capacidade que foram criadas em um grupo de posicionamento de cluster.

- Não é possível excluir um grupo de posicionamento de cluster que tenha reservas de capacidade `active`. É necessário cancelar todas as reservas de capacidade no grupo de posicionamento de cluster antes de excluí-las.

Trabalhar com reservas de capacidade em grupos de posicionamento de cluster

Para começar a usar reservas de capacidade com grupos de posicionamento de cluster, execute as etapas a seguir.

> **Note**
>
> Se você quiser criar uma reserva de capacidade em um grupo de posicionamento de cluster existente, pule a Etapa 1. Em seguida, para as Etapas 2 e 3, especifique o ARN do grupo de posicionamento de cluster existente. Para obter mais informações sobre como encontrar o ARN do grupo de posicionamento de cluster existente, consulte Visualizar informações sobre um grupo de posicionamento.

Tópicos

- Etapa 1: (condicional) crie um grupo de posicionamento de cluster para uso com uma reserva de capacidade
- Etapa 2: crie uma reserva de capacidade em um grupo de posicionamento de cluster
- Etapa 3: inicie as instâncias no grupo de posicionamento de cluster

Etapa 1: (condicional) crie um grupo de posicionamento de cluster para uso com uma reserva de capacidade

Execute esta etapa somente se precisar criar um novo grupo de posicionamento de cluster. Para usar um grupo de posicionamento de cluster existente, ignore esta etapa e, em seguida, para as Etapas 2 e 3, use o ARN desse grupo de posicionamento de cluster. Para obter mais informações sobre como encontrar o ARN do grupo de posicionamento de cluster existente, consulte Visualizar informações sobre um grupo de posicionamento.

É possível criar um grupo de posicionamento de cluster usando um dos métodos a seguir.

Console

Para criar um grupo de posicionamento de cluster usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups (Grupos de posicionamento) e Create placement group (Criar grupo de posicionamento).
3. Em Name (Nome), especifique um nome descritivo para o grupo de posicionamento.
4. Em Placement strategy (Estratégia de posicionamento), escolha Cluster.
5. Escolha Criar grupo.
6. Na tabela Grupos de posicionamento, na coluna ARN do grupo, anote o ARN do grupo de posicionamento em cluster que você criou. Você precisará dela para a próxima etapa.

AWS CLI

Como criar um grupo de posicionamento de cluster usando a AWS CLI

Use o comando create-placement-group. Em `--group-name`, especifique um nome descritivo para o grupo de posicionamento, e para `--strategy`, especifique `cluster`.

O exemplo a seguir cria um grupo de posicionamento chamado `MyPG` que usa a estratégia de posicionamento `cluster`.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Anote o ARN do grupo de posicionamento retornado na saída do comando, pois você precisará dele na próxima etapa.

Etapa 2: crie uma reserva de capacidade em um grupo de posicionamento de cluster

Você cria uma reserva de capacidade em um grupo de posicionamento de cluster da mesma forma que você cria qualquer reserva de capacidade. No entanto, você também deve especificar o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade. Para ter mais informações, consulte Criar uma Reserva de capacidade.

Considerações

- O grupo de posicionamento de cluster especificado deve estar no estado `available`. Se o grupo de posicionamento de cluster estiver no estado `pending`, `deleting` ou `deleted`, a solicitação falha.
- A reserva de capacidade e o grupo de posicionamento de cluster devem estar na mesma zona de disponibilidade. Se a solicitação para criar a reserva de capacidade especificar uma zona de disponibilidade diferente da do grupo de posicionamento de cluster, a solicitação falhará.
- É possível criar reservas de capacidade somente para tipos de instância com suporte para grupos de posicionamento de cluster. Se você especificar um tipo de instância sem suporte, a solicitação falhará. Para ter mais informações, consulte Regras e limitações do grupo de posicionamento de cluster.
- Se você criar uma reserva de capacidade `open` em um grupo de posicionamento de cluster e existirem instâncias em execução que tenham atributos correspondentes (ARN de grupo de posicionamento, tipo de instância, zona de disponibilidade, plataforma e locação), essas instâncias serão executadas automaticamente na reserva de capacidade.
- Sua solicitação de criação de uma Reserva de capacidade poderá falhar se uma das seguintes opções for verdadeira:
  - O Amazon EC2 não tem capacidade suficiente para realizar a solicitação. Tente novamente mais tarde, tente uma zona de disponibilidade diferente ou tente uma capacidade menor. Se a sua workload for flexível entre tipos e tamanhos de instâncias, tente diferentes atributos de instância.
  - A quantidade solicitada excede o limite de instância sob demanda para a família de instâncias selecionada. Aumente o limite de instância sob demanda para a família de instâncias e tente novamente. Para ter mais informações, consulte Cotas de instância sob demanda.

É possível criar a reserva de capacidade no grupo de posicionamento de cluster usando um dos métodos a seguir.

Console

Para criar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).

3. Na página Criar uma reserva de capacidade, especifique o tipo de instância, a plataforma, a zona de disponibilidade, a locação, a quantidade e a data de término conforme necessário.
4. Em Grupo de posicionamento, especifique o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.
5. Escolha Create (Criar).

Para ter mais informações, consulte Criar uma Reserva de capacidade.

AWS CLI

Para criar uma reserva de capacidade usando a AWS CLI

Use o comando create-capacity-reservation. Em `--placement-group-arn`, especifique o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.

```
$ aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone az \
    --instance-count quantity \
    --placement-group-arn placement_group_ARN
```

Para ter mais informações, consulte Criar uma Reserva de capacidade.

Etapa 3: inicie as instâncias no grupo de posicionamento de cluster

Você inicia uma instância em uma reserva de capacidade em um grupo de posicionamento de cluster da mesma forma que você inicia uma instância em qualquer reserva de capacidade. No entanto, você também deve especificar o ARN do grupo de posicionamento de cluster no qual iniciar a instância. Para ter mais informações, consulte Criar uma Reserva de capacidade.

Considerações

- Se a reserva de capacidade for `open`, não é necessário especificar a reserva de capacidade na solicitação de início da instância. Se a instância tiver atributos (ARN de grupo de posicionamento, tipo de instância, zona de disponibilidade, plataforma e locação) que correspondam a uma reserva de capacidade no grupo de posicionamento de cluster especificado, a instância será iniciada automaticamente na reserva de capacidade.

- Se a reserva de capacidade aceitar somente iniciar instâncias-alvo, você deverá especificar a reserva de capacidade-alvo além do grupo de posicionamento de cluster na solicitação.
- Se a reserva de capacidade estiver em um grupo de reserva de capacidade, você deverá especificar a reserva de capacidade-alvo além do grupo de posicionamento de cluster na solicitação. Para ter mais informações, consulte Trabalhar com grupos de Reserva de capacidade.

É possível iniciar uma instância em uma reserva de capacidade em um grupo de posicionamento de cluster usando um dos métodos a seguir.

Console

Para executar instâncias em uma Reserva de capacidade existente usando o console

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para especificar as configurações para o grupo de posicionamento e a reserva de capacidade.
2. Expanda os Detalhes avançados e faça o seguinte:
   a. Em Grupo de posicionamento, selecione o grupo de posicionamento de cluster no qual deseja executar a instância.
   b. Em Capacity Reservation (Reserva de capacidade), escolha uma das seguintes opções dependendo da configuração da reserva de capacidade:
      - Aberta: para executar as instâncias em qualquer reserva de capacidade open no grupo com posicionamento em cluster que tenha atributos correspondentes e capacidade suficiente.
      - Destino por ID: para executar as instâncias em uma reserva de capacidade que aceite somente execuções direcionadas de instância.
      - Destino por grupo: para executar as instâncias em qualquer reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado.
3. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

AWS CLI

Para iniciar instâncias em uma reserva de capacidade existente usando a AWS CLI

Use o comando run-instances. Se você precisar ter como alvo uma reserva de capacidade ou um grupo de reserva de capacidade especifico, especifique o parâmetro `--capacity-reservation-specification`. Em `--placement`, especifique o parâmetro `GroupName` e, em seguida, especifique o nome do grupo de posicionamento que você criou nas etapas anteriores.

O comando a seguir inicia uma instância em uma reserva de capacidade `targeted` em um grupo de posicionamento de cluster.

```
$ aws ec2 run-instances \
    --image-id ami_id \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnetid \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

Reservas de Capacidade em zonas locais

Uma zona local é uma extensão de uma região da AWS que está geograficamente próxima de seus usuários. Os recursos criados em uma zona local podem atender usuários locais com comunicações de latência muito baixa. Para obter mais informações, consulte Local ZonesAWS. .

É possível estender uma VPC de sua região da AWS pai para uma zona local criando uma sub-rede nessa zona local. Quando você criar uma sub-rede em uma zona local, sua VPC também será estendida para essa zona local. A sub-rede na zona local funciona da mesma forma que outras sub-redes na VPC.

Ao usar zonas locais, é possível colocar Reservas de Capacidade em vários locais que estão mais próximos de seus usuários. Você cria e usa Reservas de Capacidade em zonas locais da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os

mesmos recursos e comportamento de correspondência de instâncias são aplicados. Para obter mais informações sobre os modelos de preços com suporte nas zonas locais, consulte Perguntas frequentes sobre AWS zonas locais.

Considerações

Não é possível usar grupos de Reserva de capacidade em uma zona local.

Para usar uma reserva de capacidade em uma zona local

1. Habilite a zona local para usar em sua conta da AWS. Para ter mais informações, consulte Optar por zonas locais.
2. Crie uma reserva de capacidade na zona local. Para Availability Zone (Zona de disponibilidade), escolha a zona local. A zona local é representada por um código de região da AWS seguido por um identificador que indica o local, por exemplo, `us-west-2-lax-1a`. Para ter mais informações, consulte Criar uma Reserva de capacidade.
3. Crie uma sub-rede na zona local. Para Availability Zone (Zona de disponibilidade), escolha a zona local. Para obter mais informações, consulte Criar uma sub-rede em sua VPC no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet (Sub-rede), escolha a sub-rede na zona local (por exemplo `subnet-123abc | us-west-2-lax-1a`) e em Capacity Reservation (Reserva de capacidade), escolha a especificação (`open` ou indique seu ID) necessária para a reserva de capacidade que você criou na zona local. Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

Reservas de Capacidade em zonas Wavelength

O AWS Wavelength permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. É possível estender um Amazon Virtual Private Cloud (VPC) para uma ou mais zonas do Wavelength. Em seguida, é possível usar recursos da AWS como instâncias do Amazon EC2 para executar aplicações que exigem latência ultrabaixa e uma conexão com produtos da AWS na região. Para obter mais informações, consulte Zonas AWS Wavelength.

Ao criar Reservas de Capacidade sob demanda, é possível escolher a zona de Wavelength e executar instâncias de Reserva de capacidade em uma zona de Wavelength especificando a sub-rede associada à zona de Wavelength. Uma zona do Wavelength é representada por um código de

região da AWS seguido por um identificador que indica o local, por exemplo, `us-east-1-wl1-bos-wlz-1`.

As zonas de Wavelength não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte Zonas do Wavelength disponíveis no Guia do desenvolvedor da AWS Wavelength.

Considerações

Não é possível usar grupos de Reserva de capacidade em uma zona de Wavelength.

Para usar uma Reserva de capacidade em uma zona de Wavelength

1. Habilite a zona do Wavelength para uso em sua conta da AWS. Para ter mais informações, consulte the section called “Habilitar zonas de Wavelength”.
2. Crie uma Reserva de capacidade na zona de Wavelength. Para Availability Zone ((Zona de disponibilidade), escolha a Wavelength. O Wavelength é representado por um código de região da AWS seguido por um identificador que indica o local, por exemplo `us-east-1-wl1-bos-wlz-1`. Para ter mais informações, consulte Criar uma Reserva de capacidade.
3. Depois, crie uma sub-rede na zona de Wavelength. Para Availability Zone (Zona de disponibilidade), escolha a zona de Wavelength. Para obter mais informações, consulte Criar uma sub-rede em sua VPC no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet ((Sub-rede), escolha a sub-rede na Wavelength (por exemplo `subnet-123abc | us-east-1-wl1-bos-wlz-1`) e em Reserva de capacidade, escolha a especificação (`open` ou indique seu ID) necessária para a Reserva de capacidade que você criou na Wavelength. Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

Reservas de Capacidade no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

É possível criar Reservas de Capacidade nos Outposts que criou na sua conta. Isso permite que você reserve capacidade computacional em um Outpost em seu local. Você cria e usa Reservas de Capacidade em Outposts da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os mesmos recursos e comportamento de correspondência de instâncias são aplicados.

Também é possível compartilhar Reservas de Capacidade em Outposts com outros contas da AWS na organização usando o AWS Resource Access Manager. Para obter mais informações sobre o compartilhamento de Reservas de Capacidade, consulte Como trabalhar com Reservas de Capacidade compartilhadas.

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Considerações

- Não é possível usar grupos de reserva de capacidade em um Outpost.

Para usar um grupo de reserva de capacidade em um Outpost

1. Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.
2. Crie uma reserva de capacidade no Outpost.
    a. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
    b. No painel de navegação, selecione Outposts e, em seguida, escolha Actions (Ações), Create Capacity Reservation (Criar reserva de capacidade).
    c. Configure a reserva de capacidade conforme necessário e escolha Create (Criar). Para ter mais informações, consulte Criar uma Reserva de capacidade.

> **Note**
>
> O menu suspenso Instance Type (Tipo de instância) lista somente os tipos de instância que são compatíveis com o Outpost selecionado, e o menu suspenso Availability Zone (Zona de disponibilidade) lista somente a zona de disponibilidade à qual o Outpost selecionado está associado.

3. Iniciar uma instância na reserva de capacidade Em Subnet (Sub-rede), escolha a sub-rede criada na Etapa 1 e, em Capacity Reservation (Reserva de capacidade), selecione a reserva de capacidade criada na Etapa 2. Para obter mais informações, consulte Executar uma instância no Outpost no Manual do usuário do AWS Outposts.

Como trabalhar com Reservas de Capacidade compartilhadas

O compartilhamento de reserva de capacidade permite que os proprietários de reservas de capacidade compartilhem sua capacidade reservada com outras contas da AWS em um departamento da AWS. Isso permite criar e gerenciar as Reservas de Capacidade centralmente e compartilhar a capacidade reservada entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui a Reserva de capacidade (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nas Reservas de Capacidade que são compartilhadas com eles da mesma maneira que executam instâncias em Reservas de Capacidade que possuem em sua própria conta. O proprietário da Reserva de capacidade é responsável pelo gerenciamento da Reserva de capacidade e pelas instâncias que executa nela. Os proprietários não podem modificar as instâncias que os consumidores executam nas Reservas de Capacidade que compartilharam. Os consumidores são responsáveis por gerenciar as instâncias que executam em Reservas de Capacidade compartilhadas com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário da Reserva de capacidade.

O proprietário de uma Reserva de capacidade pode compartilhar uma Reserva de capacidade com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Tópicos

- Pré-requisitos para compartilhar Reservas de Capacidade
- Serviços relacionados
- Compartilhamento entre zonas de disponibilidade
- Compartilhar uma Reserva de capacidade
- Parar de compartilhar uma Reserva de capacidade
- Identificar e exibir uma reserva de capacidade compartilhada
- Exibir uso de Reserva de capacidade compartilhado
- Permissões de Reserva de capacidade compartilhada
- Faturamento e medição
- Limites de instâncias

Pré-requisitos para compartilhar Reservas de Capacidade

- Para compartilhar uma reserva de capacidade, é necessário ser o proprietário dela em sua conta da AWS. Não é possível compartilhar uma Reserva de capacidade que tenha sido compartilhada com você.
- Só é possível compartilhar Reservas de Capacidade para instâncias de locação compartilhada. Não é possível compartilhar Reservas de Capacidade para instâncias de locação dedicada.
- O compartilhamento de Reserva de capacidade não está disponível para contas novas da AWS ou para contas da AWS que tenham um histórico limitado de faturamento.
- Para compartilhar uma reserva de capacidade com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Serviços relacionados

O compartilhamento de reserva de capacidade integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de suas Reservas de Capacidade relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O AZ ID é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de AZ da região `us-east-1` e é o mesmo local em cada conta da AWS.

Para visualizar os IDs de AZs das zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram.
2. Os IDs de AZs da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar uma Reserva de capacidade

Quando compartilha uma reserva de capacidade de sua propriedade com outras contas da AWS, você permite que elas iniciem instâncias em sua capacidade reservada. Se você compartilhar uma Reserva de capacidade aberta, lembre-se do seguinte, pois isso pode resultar em uso não intencional da Reserva de capacidade:

- Se os consumidores tiverem instâncias em execução que correspondam aos atributos da Reserva de capacidade, tenham o parâmetro `CapacityReservationPreference` definido como `open` e ainda não estejam em execução na capacidade reservada, eles usarão a Reserva de capacidade compartilhada automaticamente.
- Se os consumidores iniciarem instâncias que tenham atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e tiverem o parâmetro `CapacityReservationPreference` definido como `open`, as instâncias serão iniciadas automaticamente na reserva de capacidade compartilhada.

Para compartilhar uma Reserva de capacidade, é necessário adicioná-la um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Ao compartilhar uma Reserva de capacidade usando o console do Amazon EC2, você a adiciona a um compartilhamento de recursos existente. Para adicionar a reserva de capacidade a um novo compartilhamento de recursos, crie o compartilhamento de recursos usando o console do AWS RAM.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado em sua organização, os consumidores da organização receberão acesso à reserva de capacidade se os pré-requisitos de compartilhamento forem atendidos. Se a reserva de capacidade estiver compartilhada com contas externas, eles receberão um convite para ingressar no compartilhamento de recursos e acesso à reserva de capacidade compartilhada após aceitar o convite.

> **Important**
>
> Antes de executar instâncias em uma reserva de capacidade que seja compartilhada com você, verifique se tem acesso à reserva de capacidade compartilhada exibindo-a no console ou descrevendo-a usando o comando describe-capacity-reservations da AWS CLI. Se conseguir exibir a reserva de capacidade compartilhada no console ou descrevê-la usando a AWS CLI, ela está disponível para seu uso e é possível executar instâncias nela. Se tentar executar instâncias na reserva de capacidade e ela não estiver acessível devido a uma falha de compartilhamento, as instâncias serão executadas na capacidade sob demanda.

É possível compartilhar uma reserva de capacidade de sua propriedade usando o console do Amazon EC2, o console do AWS RAM ou a AWS CLI.

Para compartilhar uma Reserva de capacidade de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Escolha a Reserva de capacidade a ser compartilhada e escolha Actions (Ações), Share reservation (Compartilhar reserva).
4. Selecione o compartilhamento de recursos ao qual adicionar a Reserva de capacidade e escolha Share Reserva de capacidade (Compartilhar Reserva de capacidade).

Pode levar alguns minutos para que os consumidores obtenham acesso à Reserva de capacidade compartilhada.

Para compartilhar uma reserva de capacidade de sua propriedade usando o console do AWS RAM

Consulte Criar um compartilhamento de recursos no Manual do usuário do AWS RAM.

Para compartilhar uma reserva de capacidade de sua propriedade usando a AWS CLI

Use o comando create-resource-share.

Parar de compartilhar uma Reserva de capacidade

O proprietário da Reserva de capacidade pode parar de compartilhar a Reserva de capacidade a qualquer momento. As seguintes regras se aplicam:

- As instâncias de propriedade de consumidores que estavam em execução na capacidade compartilhada na hora do cancelamento do compartilhamento continuam sendo executadas normalmente fora da capacidade reservada, e a capacidade é restaurada para a Reserva de capacidade sujeita à disponibilidade da capacidade do Amazon EC2.
- Os consumidores com quem a Reserva de capacidade era compartilhada não podem mais executar novas instâncias na capacidade reservada.

Para interromper o compartilhamento de uma Reserva de capacidade que você possui, remova-a do compartilhamento de recursos. Isso pode ser feito usando o console do Amazon EC2, o console do AWS RAM ou a AWS CLI.

Como interromper o compartilhamento de uma Reserva de capacidade que você possui usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a Reserva de capacidade e escolha a guia Sharing (Compartilhamento).
4. A guia Sharing (Compartilhamento) lista os compartilhamentos de recursos aos quais a Reserva de capacidade foi adicionada. Selecione o compartilhamento de recursos do qual remover a Reserva de capacidade e escolha Remove from resource share (Remover do compartilhamento de recursos).

Para interromper o compartilhamento de uma reserva de capacidade que você possui usando o console do AWS RAM

Consulte Atualização de um compartilhamento de atributos no Guia do usuário do AWS RAM.

Para interromper o compartilhamento de uma reserva de capacidade que você possui usando o AWS CLI

Use o comando disassociate-resource-share.

Identificar e exibir uma reserva de capacidade compartilhada

> **Important**
>
> Antes de executar instâncias em uma reserva de capacidade que seja compartilhada com você, verifique se tem acesso à reserva de capacidade compartilhada exibindo-a no console ou descrevendo-a usando a AWS CLI. Se conseguir exibir a reserva de capacidade compartilhada no console ou descrevê-la usando a AWS CLI, ela está disponível para seu uso e é possível executar instâncias nela. Se tentar executar instâncias na reserva de capacidade e ela não estiver acessível devido a uma falha de compartilhamento, a instância será executada na capacidade sob demanda.

Usando o console do Amazon EC2 e a AWS CLI, os proprietários e consumidores podem identificar e exibir reservas de capacidade compartilhadas.

Para identificar uma Reserva de capacidade compartilhada usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade. A tela lista as Reservas de Capacidade de sua propriedade e as Reservas de Capacidade que são compartilhadas com você. A coluna Owner (Proprietário) mostra o ID da conta da AWS do proprietário da Reserva de capacidade. O `(me)` ao lado do ID da conta da AWS indica que você é o proprietário.

Para identificar uma reserva de capacidade compartilhada usando a AWS CLI

Use o comando describe-capacity-reservations. O comando retorna as Reservas de Capacidade de sua propriedade e as Reservas de Capacidade que são compartilhadas com você. O `OwnerId` mostra o ID da conta da AWS do proprietário da Reserva de capacidade.

Exibir uso de Reserva de capacidade compartilhado

O proprietário de uma reserva de capacidade compartilhada pode visualizar seu uso a qualquer momento usando o console do Amazon EC2 e a AWS CLI.

Para visualizar o uso da Reserva de capacidade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a Reserva de capacidade da qual visualizar o uso e escolha a guia Usage (Uso).

   A coluna AWS account ID (ID da conta da) mostra os IDs das contas dos consumidores que estão usando a reserva de capacidade no momento. A coluna Launched instances (Instâncias executadas) mostra o número de instâncias que cada consumidor está executando na capacidade reservada no momento.

Para visualizar o uso da reserva de capacidade usando a AWS CLI

Use o comando get-capacity-reservation-usage. `AccountId` mostra o ID da conta que está usando a Reserva de capacidade. `UsedInstanceCount` mostra o número de instâncias de consumidor que estão executando na capacidade reservada no momento.

Permissões de Reserva de capacidade compartilhada

Permissões para proprietários

Os proprietários são responsáveis por gerenciar e cancelar suas Reservas de Capacidade compartilhadas. Os proprietários não podem modificar instâncias em execução na Reserva de capacidade compartilhada que sejam de propriedade de outras contas. Os proprietários continuam responsáveis pelo gerenciamento das instâncias que executam na Reserva de capacidade compartilhada.

Permissões para consumidores

Os consumidores são responsáveis pelo gerenciamento de suas instâncias que estão em execução na Reserva de capacidade compartilhada. Os consumidores não podem modificar a Reserva de capacidade compartilhada de nenhuma forma e não podem visualizar nem modificar instâncias que são de propriedade de outros consumidores ou do proprietário da Reserva de capacidade.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Reservas de Capacidade.

O proprietário da Reserva de capacidade é cobrado pelas instâncias que executa na Reserva de capacidade e pela capacidade reservada não utilizada. Os consumidores são cobrados pelas instâncias que executam na Reserva de capacidade compartilhada.

Se o proprietário da reserva de capacidade pertencer a uma conta de pagador diferente e a reserva de capacidade estiver coberta por uma instância reservada regional ou por um Savings Plan, o proprietário da reserva de capacidade continuará sendo cobrado pela instância reservada regional ou pelo Savings Plan. Nesses casos, o proprietário da reserva de capacidade paga pela instância reservada regional ou pelo Savings Plan, e os consumidores são cobrados pelas instâncias que executam na reserva de capacidade compartilhada.

Limites de instâncias

Todo o uso da Reserva de capacidade é contado em relação aos limites de instância sob demanda do proprietário da Reserva de capacidade. Isso inclui:

- Capacidade reservada não utilizada
- Uso por instâncias de propriedade do proprietário da Reserva de capacidade
- Uso por instâncias de propriedade de consumidores

As instâncias executadas na capacidade reservada por consumidores são contadas em relação ao limite de instância sob demanda do proprietário da Reserva de capacidade. Os limites de instâncias dos consumidores são a soma de seus próprios limites de instância sob demanda e a capacidade disponível nas Reservas de Capacidade compartilhadas que podem acessar.

Frotas de reserva de capacidade

Umafrota de reserva de capacidade sob demanda é um grupo de reservas de capacidade.

Uma solicitação de frota de reserva de capacidade contém todas as informações de configuração necessárias para iniciar uma frota de reserva de capacidade. Com uma só solicitação, é possível reservar grandes quantidades de capacidade do Amazon EC2 para sua workload em vários tipos de instância, até uma capacidade de destino especificada.

Após criar uma frota de reserva de capacidade, é possível gerenciar coletivamente as reservas de capacidade na frota modificando ou cancelando a frota de reserva de capacidade.

Tópicos

- Funcionamento das frotas de reserva de capacidade
- Considerações
- Definição de preço
- Conceitos de frota de reserva de capacidade
- Trabalhar com frotas de reserva de capacidade
- Exemplo de configurações de frota de reserva de capacidade
- Uso de funções vinculadas aos serviços para a frota de reserva de capacidade

Funcionamento das frotas de reserva de capacidade

Quando você cria uma frota de reserva de capacidade, a frota tenta criar reservas individuais de capacidade para atender à capacidade total de destino especificada na solicitação de frota.

O número de instâncias para as quais a frota reserva capacidade depende da capacidade total de destino e dos pesos de tipo de instância especificados por você. O tipo de instância para o qual ela reserva capacidade depende da estratégia de alocação e das prioridades de tipo de instância usadas por você.

Se não houver capacidade suficiente no momento de criação da frota e ela não conseguir atingir imediatamente sua capacidade total de destino, a frota tentará criar assíncronamente reservas de capacidade até que tenha reservado a quantidade de capacidade solicitada.

Quando a frota atinge sua capacidade total de destino, ela tenta manter essa capacidade. Se houver o cancelamento de uma reserva de capacidade na frota, dependendo da configuração da frota, ela criará automaticamente uma ou mais reservas de capacidade para substituir a capacidade perdida e manter a capacidade total de destino.

Não é possível gerenciar as reservas de capacidade na frota individualmente. Elas devem ser gerenciadas coletivamente modificando a frota. Quando você modifica uma frota, as reservas de capacidade na frota são atualizadas automaticamente para refletir as alterações.

Atualmente, as frotas de reserva de capacidade são compatíveis com os critérios `open` de correspondência de instâncias, e todas as reservas de capacidade executadas por uma frota usam automaticamente esses critérios de correspondência de instâncias. Com esse critério, novas instâncias e instâncias existentes que têm atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação) são executadas automaticamente nas reservas de

capacidade criadas por uma frota. As frotas de reserva de capacidade não são compatíveis com critérios `target` de correspondência de instâncias.

Considerações

Ao trabalhar com frotas de reserva de capacidade, lembre-se do seguinte:

- Uma frota de reserva de capacidade pode ser criada, modificada, visualizada e cancelada usando a AWS CLI e API da AWS.
- Não é possível gerenciar as reservas de capacidade em uma frota individualmente. Elas devem ser gerenciadas coletivamente modificando ou cancelando a frota.
- Uma frota de reserva de capacidade não pode abranger regiões.
- Uma frota de reserva de capacidade não pode abranger zonas de disponibilidade.
- Reservas de capacidade criadas por uma frota de reserva de capacidade são marcadas automaticamente com a seguinte etiqueta gerada da AWS:
  - Chave – `aws:ec2-capacity-reservation-fleet`
  - Valor – *`fleet_id`*

  É possível usar essa etiqueta para identificar reservas de capacidade que foram criadas por uma frota de reserva de capacidade.

Definição de preço

Não há cobranças adicionais pelo uso de frotas de reserva de capacidade. Você recebe cobranças pelas reservas de capacidade individuais criadas por suas frotas de reserva de capacidade. Para mais informações sobre o faturamento de reservas de capacidade, consulte Definição de preços e faturamento da Reserva de capacidade.

Conceitos de frota de reserva de capacidade

Este tópico descreve alguns dos conceitos sobre as frotas de reserva de capacidade.

Tópicos

- Capacidade total de destino
- Estratégia de alocação
- Peso do tipo de instância
- Prioridade do tipo de instância

Capacidade total de destino

A capacidade total de destino define a quantidade total de capacidade computacional que a frota de reserva de capacidade reserva. Você especifica a capacidade total de destino ao criar a frota de reserva de capacidade. Após a criação da frota, o Amazon EC2 cria automaticamente reservas de capacidade para reservar capacidade até a capacidade total de destino.

O número de instâncias para as quais a frota de reserva de capacidade reserva a capacidade é determinado pela capacidade total de destino e pelo peso do tipo de instância que você especificar para cada tipo de instância na frota de reserva de capacidade (`total target capacity/instance type weight = number of instances`).

É possível atribuir uma capacidade total de destino com base em unidades que são significativas para sua workload. Por exemplo, se sua workload exigir um determinado número de vCPUs, será possível atribuir a capacidade total de destino com base no número necessário de vCPUs. Se sua workload exigir `2048` vCPUs, especifique uma capacidade total de destino de `2048` e, em seguida, atribua pesos de tipo de instância com base no número de vCPUs fornecidas pelos tipos de instância na frota. Para ver um exemplo, consulte Peso do tipo de instância.

Estratégia de alocação

A estratégia de alocação para sua frota de reserva de capacidade determina como ela atenderá a solicitações de capacidade reservada das especificações de tipo de instância na configuração da frota de reserva de capacidade.

Atualmente, só há compatibilidade com a estratégia de alocação `prioritized`. Com essa estratégia, a frota de reserva de capacidade cria reservas de capacidade usando as prioridades que você atribuiu a cada uma das especificações de tipo de instância na configuração da frota de reserva de capacidade. Valores mais baixos de prioridade indicam maior prioridade para uso. Por exemplo, digamos que você crie uma frota de reserva de capacidade que use os seguintes tipos de instância e prioridades:

- `m4.16xlarge` – prioridade = 1
- `m5.16xlarge` – prioridade = 3
- `m5.24xlarge` – prioridade = 2

Primeiramente a frota tenta criar reservas de capacidade para `m4.16xlarge`. Se o Amazon EC2 tiver capacidade insuficiente da `m4.16xlarge`, a frota tenta criar reservas de capacidade para

m5.24xlarge. Se o Amazon EC2 tiver capacidade insuficiente da m5.24xlarge, a frota cria reservas de capacidade para m5.16xlarge.

Peso do tipo de instância

O peso do tipo de instância é um peso que você atribui a cada tipo de instância na frota de reserva de capacidade. O peso determina quantas unidades de capacidade cada instância do tipo específico de instância são contabilizadas na capacidade total de destino da frota.

É possível atribuir pesos com base em unidades que são significativas para sua workload. Por exemplo, se sua workload exigir um determinado número de vCPUs, será possível atribuir pesos com base no número de vCPUs fornecidas por cada tipo de instância na frota de reserva de capacidade. Nesse caso, se você criar uma frota de reserva de capacidade usando instâncias m4.16xlarge e m5.24xlarge, você atribuiria pesos que correspondem ao número de vCPUs para cada instância da seguinte forma:

- m4.16xlarge – 64 vCPUs, peso = 64 unidades
- m5.24xlarge – 96 vCPUs, peso = 96 unidades

O peso do tipo de instância determina o número de instâncias para as quais a frota de reserva de capacidade reserva a capacidade. Por exemplo, se uma frota de reserva de capacidade com uma capacidade de destino total de 384 unidades usar os tipos e pesos de instância do exemplo anterior, a frota poderia reservar capacidade para 6 instâncias m4.16xlarge (384 de capacidade total de destino/64 de tipo de instância com peso = 6 instâncias), ou 4 instâncias m5.24xlarge (384/96 = 4).

Se você não atribuir pesos de tipo de instância ou se atribuir um peso de tipo de instância de 1, a capacidade total de destino é baseada puramente na contagem de instâncias. Por exemplo, se uma frota de reserva de capacidade com uma capacidade total de destino de 384 unidades usar os tipos de instância do exemplo anterior, mas omitir os pesos ou especificar um peso de 1 para ambos os tipos de instância, a frota poderia reservar capacidade para 384 instâncias m4.16xlarge ou 384 instâncias m5.24xlarge.

Prioridade do tipo de instância

A prioridade do tipo de instância é um valor que você atribui aos tipos de instância na frota. As prioridades são usadas para determinar quais dos tipos de instância especificados para a frota devem ter o uso priorizado.

Valores mais baixos de prioridade indicam uma maior prioridade para uso.

Trabalhar com frotas de reserva de capacidade

Tópicos

- Antes de começar
- Estados de frota de reserva de capacidade
- Criar uma frota de reserva de capacidade
- Visualizar uma frota de reserva de capacidade
- Modificar uma frota de reserva de capacidade
- Cancelar uma frota de reserva de capacidade

Antes de começar

Antes de criar uma frota de reserva de capacidade:

1. Determine a quantidade de capacidade computacional necessária para sua workload.
2. Decida os tipos de instância e zonas de disponibilidade que deseja usar.
3. Atribua uma prioridade a cada tipo de instância com base em suas necessidades e preferências. Para ter mais informações, consulte Prioridade do tipo de instância.
4. Crie um sistema de ponderação de capacidade que faça sentido para sua workload. Atribua um peso a cada tipo de instância e determine sua capacidade total de destino. Para ter mais informações, consulte Peso do tipo de instância e Capacidade total de destino.
5. Determine se precisa da reserva de capacidade indefinidamente ou apenas por um período de tempo específico.

Estados de frota de reserva de capacidade

Uma frota de reserva de capacidade pode estar em um dos seguintes estados:

- `submitted` – A solicitação de frota de reserva de capacidade foi enviada e o Amazon EC2 está se preparando para criar as reservas de capacidade.
- `modifying` – A frota de reserva de capacidade está sendo modificada. A frota permanece nesse estado até que a modificação esteja concluída.
- `active` – A frota de reserva de capacidade atingiu sua capacidade de destino total e está tentando manter essa capacidade. A frota permanece nesse estado até que seja alterada ou excluída.

- `partially_fulfilled` – A frota de reserva de capacidade atingiu parcialmente sua capacidade total de destino. Não há capacidade suficiente do Amazon EC2 para satisfazer a capacidade total de destino. A frota está tentando atingir sua capacidade total de destino de maneira assíncrona.
- `expiring` – A frota de reserva de capacidade atingiu sua data de término e está em processo de expiração. Uma ou mais de suas reservas de capacidade ainda podem estar ativas.
- `expired` – A frota de reserva de capacidade atingiu sua data de término. A frota e suas reservas de capacidade expiraram. A frota não pode criar novas reservas de capacidade.
- `cancelling` – A frota de reserva de capacidade está em processo de cancelamento. Uma ou mais de suas reservas de capacidade ainda podem estar ativas.
- `cancelled` – A frota de reserva de capacidade foi cancelada manualmente. A frota e suas reservas de capacidade estão canceladas e a frota não pode criar novas reservas de capacidade.
- `failed` – A frota de reserva de capacidade não conseguiu reservar capacidade para os tipos de instância especificados.

Criar uma frota de reserva de capacidade

Quando você cria uma frota de reserva de capacidade, ela cria automaticamente reservas de capacidade para os tipos de instância especificados na solicitação de frota, até a capacidade total de destino especificada. O número de instâncias para as quais a frota de reserva de capacidade reserva capacidade depende da capacidade total de destino e dos pesos de tipo de instância que você especifica na solicitação. Para ter mais informações, consulte Peso do tipo de instância e Capacidade total de destino.

Ao criar a frota, especifique os tipos de instância a serem usados e uma prioridade para cada um desses tipos de instância. Para ter mais informações, consulte Estratégia de alocação e Prioridade do tipo de instância.

> **Note**
>
> A função AWSServiceRoleForEC2CapacityReservationFleet vinculada a serviço é criada automaticamente em sua conta na primeira vez que você cria uma frota de reserva de capacidade. Para ter mais informações, consulte Uso de funções vinculadas aos serviços para a frota de reserva de capacidade.

Atualmente, as frotas de reserva de capacidade são compatíveis apenas com os critérios `open` de correspondência de instâncias.

Só é possível criar uma frota de reserva de capacidade usando a linha de comando.

Para criar uma frota de reserva de capacidade

Use o comando create-capacity-reservation-fleet da AWS CLI.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Veja a seguir o conteúdo de `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "instance_type",
        "InstancePlatform":"platform",
        "Weight": instance_type_weight,
        "AvailabilityZone":"availability_zone",
        "AvailabilityZoneId" : "az_id",
        "EbsOptimized": true|false,
        "Priority" : instance_type_priority
    }
]
```

Saída esperada.

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
}
```

Exemplo

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
```

```
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Saída de exemplo.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Visualizar uma frota de reserva de capacidade

É possível visualizar as informações de configuração e capacidade de uma frota de reserva de capacidade a qualquer momento. A visualização de uma frota também fornece detalhes sobre as reservas de capacidade individuais que estão na frota.

Só é possível visualizar uma frota de reserva de capacidade usando a linha de comando.

Para visualizar uma frota de reserva de capacidade

Use o comando describe-capacity-reservation-fleets da AWS CLI.

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Saída esperada

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
```

```
}
```

Exemplo

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Exemplo de saída

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Modificar uma frota de reserva de capacidade

É possível modificar a qualquer momento a capacidade total de destino e a data de uma frota de reserva de capacidade. Ao modificar a capacidade total de destino de uma frota de reserva de capacidade, a frota cria automaticamente novas reservas de capacidade ou modifica ou cancela as reservas de capacidade existentes na frota para atender à nova capacidade total de destino. Quando você modifica a data de término da frota, as datas de término de todas as reservas de capacidade individuais são atualizadas de maneira adequada.

Após modificar uma frota, o status dela muda para `modifying`. Não é possível tentar fazer modificações adicionais em uma frota enquanto ela estiver no estado `modifying`.

Você não pode modificar a locação, a zona de disponibilidade, os tipos de instância, as plataformas de instância, as prioridades ou os pesos usados por uma frota de reserva de capacidade. Se precisar alterar qualquer um desses parâmetros, talvez seja necessário cancelar a frota existente e criar uma nova com os parâmetros necessários.

Só é possível modificar uma frota de reserva de capacidade usando a linha de comando.

Para modificar uma frota de reserva de capacidade

Use o comando modify-capacity-reservation-fleet da AWS CLI.

> **Note**
>
> Não é possível especificar `--end-date` e `--remove-end-date` no mesmo comando.

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

Saída esperada

```
{
    "Return": true
}
```

Exemplo: modificar a capacidade total de destino

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

Exemplo: modificar a data de término

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

Exemplo: remover a data de término

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

Exemplo de saída

```
{
    "Return": true
}
```

Cancelar uma frota de reserva de capacidade

Quando não precisar mais de uma frota de reserva de capacidade e da capacidade que ela reserva, é possível cancelá-la. Quando você cancela uma frota, o status muda para `cancelled` e ela não poderá mais criar novas reservas de capacidade. Além disso, todas as reservas de capacidade individuais na frota são canceladas e as instâncias que estavam em execução anteriormente na capacidade reservada continuam a ser executadas normalmente com capacidade compartilhada.

Só é possível cancelar uma frota de reserva de capacidade usando a linha de comando.

Para cancelar uma frota de reserva de capacidade

Use o comando cancel-capacity-reservation-fleet da AWS CLI.

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Saída esperada

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
              "Code": "code",
                    "Message": "message"
          }
         ]
     }
    ]
}
```

Exemplo: cancelamento bem-sucedido

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Exemplo de saída

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
```

```
    ],
    "FailedFleetCancellations": []
}
```

Exemplo de configurações de frota de reserva de capacidade

Tópicos

- Exemplo 1: reservar capacidade com base em vCPUs

Exemplo 1: reservar capacidade com base em vCPUs

O exemplo a seguir cria uma frota de reserva de capacidade que usa dois tipos de instância: `m5.4xlarge` e `m5.12xlarge`.

Ele usa um sistema de ponderação com base no número de vCPUs fornecidas pelos tipos de instância especificados. A capacidade total de destino é de `480` vCPUs. O tipo `m5.4xlarge` fornece 16 vCPUs e tem um peso de 16, enquanto o `m5.12xlarge` fornece 48 vCPUs e tem um peso de 48. Este sistema de ponderação configura a frota de reserva de capacidade para reservar capacidade para 30 instâncias `m5.4xlarge` (480/16 = 30) ou 10 instâncias `m5.12xlarge` (480/48 = 10).

A frota está configurada para priorizar a capacidade de `m5.12xlarge` e obtém prioridade de `1`, enquanto `m5.4xlarge` obtém uma prioridade mais baixa de `2`. Isso significa que a frota tentará reservar primeiramente a capacidade de `m5.12xlarge`, e só tentará reservar `m5.4xlarge` se o Amazon EC2 tiver capacidade insuficiente de `m5.12xlarge`.

A frota reserva a capacidade para `Windows` instâncias e a reserva expira automaticamente em `October 31, 2021` às `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 480 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Veja a seguir o conteúdo de `instanceTypeSpecification.json`.

```
[
```

```
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

Uso de funções vinculadas aos serviços para a frota de reserva de capacidade

A frota de reserva de capacidade sob demanda usa funções vinculadas a serviço do AWS Identity and Access Management (IAM). Uma função vinculada a serviço é um tipo exclusivo de função do IAM vinculada diretamente à frota de reserva de capacidade. As funções vinculadas a serviço são predefinidas pela frota de reserva de capacidade e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada a serviço facilita a configuração da frota de reserva de capacidade porque você não precisa adicionar as permissões necessárias manualmente. A frota de reserva de capacidade define as permissões das funções vinculadas a serviço e, exceto se definido de outra forma, somente a frota de reserva de capacidade pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos da frota de reserva de capacidade, pois você não pode remover por engano as permissões para acessar os recursos.

Permissões de funções vinculadas aos serviços para a frota de reserva de capacidade

A frota de reserva de capacidade usa a função vinculada a serviço chamada AWSServiceRoleForec2CapacityReservationFleet para criar, descrever, modificar e cancelar em

seu nome reservas de capacidade que foram criadas anteriormente por uma frota de reserva de capacidade.

A função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet confia nas seguintes entidades para assumir a função: `capacity-reservation-fleet.amazonaws.com`.

A função usa a política AWSEC2CapacityReservationFleetRolePolicy, que inclui as seguintes permissões:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para a frota de reserva de capacidade

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria uma frota de reserva de capacidade usando o comando `create-capacity-reservation-fleet` da AWS CLI ou a API `CreateCapacityReservationFleet`, a função vinculada a serviço é criada automaticamente para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria uma frota de reserva de capacidade, a frota de reserva de capacidade cria a função vinculada a serviço para você novamente.

Editar uma função vinculada ao serviço para a frota de reserva de capacidade

A frota de reserva de capacidade não permite que você edite a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para a frota de reserva de capacidade

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, é necessário excluir os recursos de sua função vinculada a serviço antes que seja possível exclui-la manualmente.

> **Note**
>
> Se o serviço da frota de reserva de capacidade estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet

1. Use o comando `delete-capacity-reservation-fleet` da AWS CLI ou a API `DeleteCapacityReservationFleet` para excluir as frotas de reserva de capacidade em sua conta.
2. Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas aos serviços para frota de reserva de capacidade

A frota de reserva de capacidade é compatível com o uso de funções vinculadas a serviço em todas as regiões nas quais o serviço esteja disponível. Para mais informações, consulte Regiões e endpoints da AWS.

Monitoramento de reservas de capacidade

É possível usar os seguintes recursos para monitorar as reservas de capacidade:

Tópicos

- Monitorar as reservas de capacidade usando métricas do CloudWatch
- Monitorar as reservas de capacidade usando o EventBridge
- Notificações de utilização

Monitorar as reservas de capacidade usando métricas do CloudWatch

Com as métricas do CloudWatch, é possível monitorar as Reservas de Capacidade e identificar a capacidade não utilizada configurando os alarmes do CloudWatch para notificá-lo quando os limites de uso forem atingidos. Isso pode ajudá-lo a manter um volume constante de Reserva de capacidade e atingir um nível mais alto de utilização.

As Reservas de Capacidade sob demanda enviam dados de métricas ao CloudWatch a cada cinco minutos. Não há suporte para métricas de Reservas de Capacidade que estejam ativas por menos de cinco minutos.

Para obter mais informações sobre como visualizar métricas no console do CloudWatch, consulte Usar as métricas do Amazon CloudWatch. Para obter mais informações sobre como criar alarmes, consulte Criar alarmes do Amazon CloudWatch.

Tópicos

- Métricas de uso da Reserva de capacidade
- Dimensões de métricas da Reserva de capacidade
- Visualizar métricas do CloudWatch nas Reservas de Capacidade

Métricas de uso da Reserva de capacidade

O namespace `AWS/EC2CapacityReservations` inclui as seguintes métricas de uso que é possível usar para monitorar e manter a capacidade sob demanda dentro dos limites especificados para sua reserva.

Métrica	Descrição
`UsedInstanceCount`	O número de instâncias que estão em uso no momento. Unidade: contagem
`AvailableInstanceCount`	O número de instâncias disponíveis. Unidade: contagem
`TotalInstanceCount`	O número total de instâncias reservadas. Unidade: contagem
`InstanceUtilization`	A porcentagem de instâncias de capacidade reservada que estão em uso no momento.

Métrica	Descrição
	Unidade: percentual

Dimensões de métricas da Reserva de capacidade

É possível usar as seguintes dimensões para refinar as métricas listadas na tabela anterior.

Dimensão	Descrição
`CapacityReservationId`	Essa dimensão globalmente exclusiva filtra os dados solicitados somente para a reserva de capacidade identificada.

Visualizar métricas do CloudWatch nas Reservas de Capacidade

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, pelas várias dimensões com suporte. É possível usar os procedimentos a seguir para visualizar as métricas de suas Reservas de Capacidade.

Para visualizar as métricas da Reserva de capacidade usando o console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que a Reserva de capacidade reside. Para obter mais informações, consulte Regiões e endpoints.
3. No painel de navegação, selecione Metrics (Métricas).
4. Para Todas as métricas, escolha Reservas de Capacidade do EC2.
5. Escolha a dimensão da métrica Por reserva de capacidade. As métricas serão agrupadas por `CapacityReservationId`.
6. Para classificar a métrica, use o cabeçalho da coluna. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica.

Para visualizar métricas da reserva de capacidade (AWS CLI)

Use o comando list-metrics a seguir:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Monitorar as reservas de capacidade usando o EventBridge

O AWS Health envia eventos para o Amazon EventBridge quando uma reserva de capacidade em sua conta está abaixo de 20% do uso em determinados períodos. Com o EventBridge, é possível estabelecer regras que acionam ações programáticas em resposta a tais eventos. Por exemplo, você pode criar uma regra que vai cancelar automaticamente uma reserva de capacidade quando a utilização estiver abaixo de 20% em um período de sete dias.

Os eventos no EventBridge são representados como objetos JSON. Os campos que são exclusivos do evento estão contidos na seção "detalhes" do objeto JSON. O campo "evento" contém o nome do evento. O campo "resultados" contém o status concluído da ação que acionou o evento. Para obter mais informações, consulte Padrões de eventos do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Não há suporte a este recurso na AWS GovCloud (US).

Conteúdo

- Eventos
- Criar uma regra de EventBridge

Eventos

O AWS Health enviará os eventos a seguir quando o uso de capacidade para uma reserva de capacidade estiver abaixo de 20%.

Eventos

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION
- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

Veja a seguir um exemplo de evento gerado quando uma reserva de capacidade recém-criada está abaixo de 20% do uso da capacidade em um período de 24 horas.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

Veja a seguir um exemplo de evento gerado quando uma ou mais reservas de capacidade estão abaixo de 20% do uso da capacidade em um período de sete dias.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
```

```
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
            }
        ]
    }
}
```

Criar uma regra de EventBridge

Para receber notificações por e-mail quando a utilização da reserva de capacidade estiver abaixo de 20%, crie um tópico do Amazon SNS e, em seguida, crie uma regra do EventBridge para o evento `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`.

Para criaro tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, selecione Topics (Tópicos) e Create topic (Criar tópico).
3. Em Tipo, escolha Padrão.
4. Em Nome, digite um nome para o novo tópico.
5. Escolha Criar tópico.
6. Selecione Criar assinatura.
7. Em Protocolo, escolha E-mail e, em seguida, para Endpoint, insira o endereço de e-mail que receberá as notificações.
8. Selecione Criar assinatura.
9. O endereço de e-mail inserido acima receberá uma mensagem de e-mail com a seguinte linha de assunto: `AWS Notification - Subscription Confirmation`. Siga as instruções para confirmar sua assinatura.

Como criar a regra do EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Rules (Regras) e Create rule (Criar regras).
3. Em Nome, digite um nome para a nova regra.
4. Em Tipo de Regra, escolha Regra com Padrão de Evento.
5. Escolha Próximo.
6. Em Padrão de evento, faça o seguinte:
    a. Em Fonte do evento, selecione Serviços da AWS.
    b. Em Serviço da AWS, escolha AWS Health.
    c. Em Tipo de evento, escolha Notificação de subutilização de ODCR do EC2.
7. Escolha Próximo.
8. Em Destino 1, faça o seguinte:
    a. Em Tipos de destino, escolha Serviço da AWS.
    b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS).
    c. Em Tópico, escolha o tópico criado anteriormente.

9. Selecione Próximo e, em seguida, Próximo novamente.
10. Escolha Criar Regra.

Notificações de utilização

O AWS Health enviará o e-mail e as notificações do AWS Health Dashboard a seguir quando a utilização da capacidade para reservas de capacidade em sua conta estiver abaixo de 20%.

- Notificações individuais para cada reserva de capacidade recém-criada que esteve abaixo de 20% de utilização nas últimas 24 horas.
- Uma notificação resumida para todas as reservas de capacidade que estiveram abaixo de 20% de utilização nos últimos sete dias.

As notificações por e-mail e as notificações do AWS Health Dashboard serão enviadas para o endereço de e-mail associado à conta da AWS que tem as reservas de capacidade como propriedade. As notificações incluem as seguintes informações:

- O ID da reserva de capacidade.
- A zona de disponibilidade da reserva de capacidade.
- A taxa de utilização média para a reserva de capacidade.
- O tipo de instância e a plataforma (sistema operacional) da reserva de capacidade.

Além disso, quando a utilização da capacidade de uma reserva de capacidade em sua conta estiver abaixo de 20% em um período de 24 horas e sete dias, o AWS Health enviará eventos para o EventBridge. Com o EventBridge, é possível criar regras que ativam ações automáticas, como o envio de notificações por e-mail ou o acionamento de funções do AWS Lambda, em resposta a esses eventos. Para ter mais informações, consulte Monitorar as reservas de capacidade usando o EventBridge.

Blocos de capacidade para ML

Os blocos de capacidade para ML permitem que você reserve para uma data futura as instâncias de GPU com grande procura para lidar com suas workloads de machine learning (ML) de curta duração. As instâncias que são executadas em um bloco de capacidade são automaticamente colocadas próximas umas das outras nos UltraClusters do Amazon EC2 para redes sem bloqueio de baixa latência com escala de petabits.

Com blocos de capacidade, você pode ver quando a capacidade da instância de GPU está disponível em datas futuras e agendar um bloco de capacidade para começar na hora que for melhor para você. Quando você reserva um bloco de capacidade, garante capacidade previsível de instâncias de GPU e pagando apenas pelo tempo que precisar. Recomendamos blocos de capacidade quando você precisa de GPUs para lidar com workloads de ML durante dias ou semanas seguidos e não deseja pagar por uma reserva enquanto as instâncias de GPU não estão em uso.

Estes são alguns casos de uso comuns de blocos de capacidade.

- Treinamento e ajuste fino de modelo de ML: tenha acesso ininterrupto às instâncias de GPU que você reservou para realizar treinamento e ajuste fino do modelo de ML.
- Experimentos e protótipos de ML: executar experimentos e desenvolver protótipos que exigem instâncias de GPU por períodos curtos.

Atualmente, há blocos de capacidade disponíveis para instâncias `p5.48xlarge` e `p4d.24xlarge`. As instâncias `p5.48xlarge` estão disponíveis nas regiões Leste dos EUA (Ohio) e Leste dos EUA (Norte da Virgínia). As instâncias `p4d.24xlarge` estão disponíveis nas regiões Leste dos EUA (Ohio) e Oeste dos EUA (Oregon). Você pode reservar um bloco de capacidade para uma hora de início em até oito semanas no futuro.

Você pode usar blocos de capacidade para reservar instâncias `p5` e `p4d` com as seguintes opções de duração da reserva e quantidade de instâncias.

- Durações de reserva para incrementos de 1 dia em um total de até 14 dias
- Opções de quantidade de instâncias de reserva de 1, 2, 4, 8, 16, 32 ou 64 instâncias

Para reservar um bloco de capacidade, você começa especificando suas necessidades de capacidade, incluindo o tipo de instância, o número de instâncias, a quantidade de tempo, a primeira data de início e a última data de término de que precisa. Depois, você vê uma oferta disponível do bloco de capacidade que atende às suas especificações. A oferta do bloco de capacidade inclui detalhes como hora de início, zona de disponibilidade e preço da reserva. O preço de oferta de um bloco de capacidade depende da disponibilidade e da demanda no momento em que a oferta é feita. Depois que você reserva um bloco de capacidade, o preço não muda mais. Para ter mais informações, consulte Preços e faturamento de blocos de capacidade.

Quando você compra uma oferta de bloco de capacidade, a reserva é criada para a data e o número de instâncias selecionados. Quando sua reserva de bloco de capacidade começa, você

pode direcionar as inicializações de instância especificando o ID da reserva nas solicitações de inicialização.

Você pode usar todas as instâncias reservadas até 30 minutos antes da hora de término do bloco de capacidade. Trinta minutos antes do fim da reserva do bloco de capacidade, começamos a encerrar todas as instâncias em execução no bloco de capacidade. Usamos esse tempo para limpar as instâncias antes de entregar o bloco de capacidade ao próximo cliente. Os últimos 30 minutos da reserva não são incluídos na cobrança do bloco de capacidade. Emitimos um evento por meio do EventBridge 10 minutos antes do início do processo de encerramento. Para ter mais informações, consulte Monitorar blocos de capacidade com o EventBridge.

Tópicos

- Plataformas compatíveis
- Considerações
- Recursos relacionados
- Preços e faturamento de blocos de capacidade
- Trabalhar com blocos de capacidade
- Monitorar blocos de capacidade

Plataformas compatíveis

Atualmente, os blocos de capacidade para ML são compatíveis com instâncias `p5.48xlarge` e `p4d.24xlarge` com locação padrão. Quando você usa o AWS Management Console para comprar um bloco de capacidade, a opção de plataforma padrão é a Linux/UNIX. Quando você usa a AWS Command Line Interface (AWS CLI) ou o AWS SDK para comprar um bloco de capacidade, as seguintes opções de plataforma estão disponíveis:

- Linux/UNIX
- Red Hat Enterprise Linux
- RHEL com HA
- SUSE Linux
- Ubuntu Pro

Considerações

Antes de usar os blocos de capacidade, considere os seguintes detalhes e limitações.

- Os blocos de capacidade começam e terminam às 11h30, Horário Universal Coordenado (UTC).
- O processo de encerramento de instâncias em execução em um bloco de capacidade começa às 11h, Horário Universal Coordenado (UTC) no último dia da reserva.
- Os blocos de capacidade podem ser reservados para uma hora de início em até oito semanas no futuro.
- Não é permitido modificar nem cancelar blocos de capacidade.
- Os blocos de capacidade não podem ser compartilhados entre contas da AWS nem dentro da sua organização da AWS.
- Os blocos de capacidade não podem ser usados em um grupo de reserva de capacidade.
- O número total de instâncias que podem ser reservadas em blocos de capacidade entre todas as contas da sua organização da AWS não pode ultrapassar 64 instâncias em uma determinada data.
- Para usar um bloco de capacidade, as instâncias devem ser direcionadas especificamente para o ID da reserva.
- As instâncias em um bloco de capacidade não contam para seus limites de instâncias sob demanda.
- Para instâncias P5 usando uma AMI personalizada, verifique se você tem os softwares e a configuração necessários para EFA.
- No momento, os blocos de capacidade não podem ser usados com grupos de nós gerenciados pelo Amazon EKS ou com o Karpenter. Para obter mais informações sobre como criar um grupo de nós autogerenciado do Amazon EKS, consulte Blocos de capacidade para ML no Guia do usuário do Amazon EKS.

Recursos relacionados

Após criar um bloco de capacidade, você poderá fazer o seguinte com ele:

- Iniciar instâncias no bloco de capacidade. Para ter mais informações, consulte Iniciar instâncias em blocos de capacidade.
- Crie um grupo do Amazon EC2 Auto Scaling. Para obter mais informações, consulte Usar blocos de capacidade para workloads de machine learning no Guia do usuário do Amazon EC2 Auto Scaling.

> **Note**
>
> Se você usa o Amazon EC2 Auto Scaling ou o Amazon EKS, é possível programar a escalabilidade para ser executada no início da reserva do bloco de capacidade. Com o escalamento programado, o AWS gerencia automaticamente as novas tentativas para que você não precise se preocupar em implementar uma lógica de repetições para lidar com falhas transitórias.

- Melhore os fluxos de trabalho de ML com o AWS ParallelCluster. Para obter mais informações, consulte Aprimorar fluxos de trabalho de ML com o AWS ParallelCluster e blocos de capacidade do Amazon EC2 para ML.

Para obter mais informações sobre o AWS ParallelCluster, consulte O que é o AWS ParallelCluster.

Preços e faturamento de blocos de capacidade

Tópicos

- Definição de preço
- Faturamento

Definição de preço

Com os blocos de capacidade para ML do Amazon EC2, você só paga pelo que reserva. O preço de um bloco de capacidade depende da disponibilidade e da demanda de blocos de capacidade no momento da compra. Você pode ver o preço de uma oferta de bloco de capacidade antes de fazer a reserva. O preço do bloco de capacidade é cobrado à vista no momento em que a reserva é feita. Quando você pesquisa um bloco de capacidade em um intervalo de datas, retornamos a oferta de bloco de capacidade com o menor preço disponível. Depois que você reservou um bloco de capacidade, o preço não muda mais.

Quando você usa um bloco de capacidade, paga pelo sistema operacional que usa quando as instâncias estão em execução. Para obter mais informações sobre os preços de sistemas operacionais, consulte Amazon EC2 Capacity Blocks for ML Pricing.

Faturamento

O preço de uma oferta de bloco de capacidade é cobrado à vista. O pagamento é faturado para a sua conta da AWS dentro de 12 horas após a compra de um bloco de capacidade. Enquanto

seu pagamento é processado, o recurso de reserva do bloco de capacidade permanece em um estado `payment-pending`. Se o pagamento não puder ser processado em 12 horas, o bloco de capacidade será liberado e o estado da reserva passará a ser `payment-failed`.

Depois que o pagamento é processado com sucesso, o estado do recurso do bloco de capacidade passa de `payment-pending` para `scheduled`. Você recebe uma fatura que reflete o pagamento antecipado à vista. Na fatura, você pode associar o valor pago ao ID da reserva do bloco de capacidade.

Quando a reserva do bloco de capacidade começa, você é cobrado com base apenas no sistema operacional que usa enquanto as instâncias estão em execução na reserva. Você pode ver o uso e as cobranças associadas até a data de fechamento da sua fatura mensal de uso no AWS Cost and Usage Report.

> **Note**
>
> Os descontos dos Savings Plans e das instâncias reservadas não se aplicam aos blocos de capacidade.

Visualizar sua fatura

Você pode visualizar sua conta no console do AWS Billing and Cost Management. O pagamento antecipado do bloco de capacidade aparece no mês em que você adquiriu a reserva.

Depois que sua reserva começa, sua fatura mostra linhas separadas para o tempo usado e não usado da reserva do bloco. Você pode usar esses itens de linha para ver quanto tempo foi usado de sua reserva. Você só verá uma cobrança por uso na linha de tempo usado se usar um sistema operacional premium. Para ter mais informações, consulte Definição de preço. Não há custo adicional por tempo não usado.

Para obter mais informações, consulte Exibição da sua fatura no Guia do usuário do AWS Billing and Cost Management.

Se o bloco de capacidade começar em um mês diferente do mês em que você adquiriu a reserva, o preço inicial e o uso da reserva aparecerão em meses de cobrança diferentes. No AWS Cost and Usage Report, o ID da reserva do bloco de capacidade está listado no item da linha Reservation/ReservationARN do pagamento antecipado e o LineItem/ResourceID na fatura mensal fechada para que você possa associar o uso ao preço pago antecipadamente correspondente.

Trabalhar com blocos de capacidade

Para começar a usar os blocos de capacidade, primeiro você precisa encontrar e comprar um bloco de capacidade disponível que corresponda ao tamanho, à duração e as datas de reserva de que precisa. Depois, quando a reserva começar, você poderá usar o bloco de capacidade iniciando instâncias direcionadas ao ID da reserva. Trinta minutos antes do vencimento da reserva, começamos a encerrar todas as instâncias que ainda estão em execução no bloco de capacidade.

Os blocos de capacidade são fornecidos como reservas de capacidade `targeted` em uma única zona de disponibilidade. Para executar instâncias em um bloco de capacidade, você deve especificar o ID da reserva ao iniciá-las. Se você mesmo interromper as instâncias e o bloco de capacidade expirar, não poderá reiniciá-las até direcioná-las a outro bloco de capacidade no estado `active`.

Por padrão, os blocos de capacidade oferecem conectividade de rede de baixa latência e alto throughput entre as instâncias do bloco de capacidade, portanto, não há necessidade de usar um grupo de posicionamento de cluster com um bloco de capacidade.

Tópicos

- Pré-requisitos
- Encontrar e comprar blocos de capacidade
- Iniciar instâncias em blocos de capacidade
- Visualizar blocos de capacidade

Pré-requisitos

Você deverá usar o Região da AWS correspondente ao tipo de instância que deseja usar. Para ter mais informações, consulte Regiões.

Os blocos de capacidade com instâncias `p5.48xlarge` estão disponíveis nas Regiões da AWS apresentadas a seguir.

Nome da região	Código da região
Leste dos EUA (Ohio)	us-east-2
Leste dos EUA (N. da Virgínia)	us-east-1

Os blocos de capacidade com instâncias `p4d.24xlarge` estão disponíveis nas Regiões da AWS apresentadas a seguir.

Nome da região	Código da região
Leste dos EUA (Ohio)	us-east-2
Oeste dos EUA (Oregon)	us-west-2

> **Note**
>
> Tamanhos de blocos de capacidade de 64 instâncias não são compatíveis com todos os tipos de instância em todas as Regiões da AWS.

Encontrar e comprar blocos de capacidade

Para reservar um bloco de capacidade, primeiro, você precisa encontrar um bloco de tempo durante o qual a capacidade esteja disponível e que atenda às suas necessidades. Para encontrar um bloco de capacidade disponível para reserva, você especifica:

- O número de instâncias de que você precisa
- O tempo durante o qual você precisa das instâncias
- O intervalo de datas quando você precisa da reserva

Para pesquisar uma oferta disponível de bloco de capacidade, você especifica a duração da reserva e o número de instâncias. Você deve selecionar uma das opções a seguir.

- Para duração da reserva: até 14 dias em incrementos de 1 dia
- Para número de instâncias: 1, 2, 4, 8, 16, 32 ou 64 instâncias

Se houver um bloco de capacidade disponível que atenda às suas especificações, retornaremos os detalhes de uma única oferta de bloco de capacidade. Os detalhes da oferta incluem a hora de início da reserva, a zona de disponibilidade da reserva e o preço da reserva. Para ter mais informações, consulte Definição de preço.

Você pode comprar a oferta de bloco de capacidade exibida ou modificar os critérios de pesquisa para ver as outras opções disponíveis. Não há prazo de validade predefinido para a oferta, mas as ofertas só estão disponíveis por ordem de chegada.

Ao comprar uma oferta de bloco de capacidade, você recebe uma resposta imediata confirmando que o bloco de capacidade foi reservado. Após a confirmação, você verá uma nova reserva de capacidade em sua conta com um tipo de reserva de `capacity-block` e uma `start-date` definida como a hora de início da oferta que você comprou. A reserva do bloco de capacidade é criada em um estado de `payment-pending`. Depois que o pagamento antecipado é processado com sucesso, o estado da reserva passa a ser `scheduled`. Para ter mais informações, consulte Faturamento.

Você usar um dos métodos a seguir para encontrar e comprar um bloco de capacidade.

Console

Para encontrar e comprar um bloco de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma Região da AWS. Essa escolha é importante porque os tamanhos de blocos de capacidade de 64 instâncias não são compatíveis com todos os tipos de instância em todas as regiões.
3. No painel de navegação, escolha Reservas de capacidade, Comprar blocos de capacidade.
4. Em Atributos de capacidade, você pode definir os parâmetros da pesquisa de bloco de capacidade. Por padrão, a plataforma é Linux. Se você quiser selecionar outro sistema operacional, use a AWS CLI. Para ter mais informações, consulte Plataformas compatíveis.
5. Em Capacidade total, selecione o número de instâncias que você deseja reservar.
6. Em Duração, insira o número de dias durante os quais você precisa da reserva.
7. Em Intervalo de datas para pesquisar blocos de capacidade, insira a data de início mais cedo e a data de término mais tarde que forem possíveis para a reserva.
8. Escolha Encontrar blocos de capacidade.
9. Se houver um bloco de capacidade disponível que atenda às suas especificações, você verá uma oferta em Blocos de capacidade recomendados. Se houver várias ofertas que atendam às suas especificações, a oferta de bloco de capacidade disponível de menor preço será exibida. Para ver outras ofertas de blocos de capacidade, ajuste as entradas da pesquisa e escolha Localizar blocos de capacidade novamente.

10. Quando encontrar uma oferta do bloco de capacidade que você queira comprar, escolha Avançar.
11. (Opcional) Na página Adicionar tags, escolha Adicionar nova tag.
12. A página Revisar e comprar lista a data de início e a data de término, a duração, o número total de instâncias e o preço.

> **Note**
>
> Os blocos de capacidade não podem ser modificados nem cancelados depois que você os reserva.

13. Na janela pop-up Comprar um bloco de capacidade, digite confirmar e depois escolha Comprar.

AWS CLI

Para encontrar um bloco de capacidade usando a AWS CLI

Use o comando `describe-capacity-block-offerings`.

O exemplo a seguir pesquisa um bloco de capacidade que tenha 16 instâncias `p5.48xlarge` com um intervalo de datas começando em `2023-08-14` e terminando em `2023-10-22` e uma duração de 48 horas. O número instâncias deve ser um inteiro de um conjunto predefinido de opções: 1, 2, 4, 8,16, 32 ,64. A duração da capacidade deve ser um inteiro múltiplo de 24 entre 24 e 336, indicando o número de dias em horas.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \
  --instance-count 16 --start-date-range 2023-08-14T00:00:00Z \
  --end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Para comprar um bloco de capacidade usando a AWS CLI

Use o comando `purchase-capacity-block` e especifique o ID da oferta do bloco de capacidade que você deseja comprar e a plataforma da instância.

```
aws ec2 purchase-capacity-block \
  --capacity-block-offering-id cbr-0123456789abcdefg \
  --instance-platform Linux/UNIX
```

Iniciar instâncias em blocos de capacidade

Depois que reservar um bloco de capacidade, você poderá visualizar a reserva do bloco de capacidade em sua conta da AWS. Você poderá visualizar a `start-date` e a `end-date` para saber quando sua reserva começará e terminará. Antes do início de uma reserva do bloco de capacidade, a capacidade disponível aparece como zero. Você pode ver quantas instâncias estarão disponíveis em seu bloco de capacidade pelo valor da tag da chave de tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Quando uma reserva de bloco de capacidade começa, o estado da reserva passa de `scheduled` para `active`. Emitimos um evento por meio do Amazon EventBridge para notificar você de que o bloco de capacidade está disponível para uso. Para ter mais informações, consulte Monitorar blocos de capacidade.

Para usar o bloco de capacidade, você deve especificar o ID da reserva do bloco de capacidade ao iniciar as instâncias. A inicialização de uma instância em uma reserva de capacidade reduz a capacidade disponível de acordo com o número de instâncias iniciadas. Por exemplo, se a capacidade de instância comprada for de oito instâncias e você executar quatro instâncias, a capacidade disponível será reduzida em quatro.

Se você encerrar uma instância em execução no bloco de capacidade antes que a reserva termine, poderá iniciar uma nova instância em seu lugar. Quando você interrompe ou encerra uma instância em um bloco de capacidade, são necessários vários minutos para limpar sua instância antes que você possa executar outra instância para substituí-la. Durante esse tempo, a instância ficará em um estado de Interrompendo ou `shutting-down`. Depois que esse processo é concluído, o estado da sua instância passa para `stopped` ou `terminated`. Em seguida, a capacidade disponível no bloco de capacidade é atualizada para mostrar outra instância disponível para uso.

As etapas a seguir explicam como iniciar instâncias em um bloco de capacidade no estado `active` usando o AWS Management Console ou a AWS CLI.

Para obter informações sobre a configuração de um grupo de nós do EKS para usar automaticamente um bloco de capacidade quando ele começar, consulte Capacity Blocks for ML no Amazon EKS User Guide.

Para obter informações sobre como iniciar instâncias em um bloco de capacidade usando a Frota do EC2, consulte Tutorial : iniciar instâncias em blocos de capacidade.

Para obter informações sobre como criar um modelo de inicialização que direcione para um bloco de capacidade, consulte Executar uma instância a partir de um modelo de execução

Você pode usar um dos métodos a seguir para iniciar instâncias em um bloco de capacidade.

Console

Para iniciar instâncias em uma reserva de capacidade existente usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma região para a reserva do bloco de capacidade.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Nome e tags, você pode nomear e aplicar tags à instância. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2
5. Em Imagens de aplicação e sistema operacional, selecione uma imagem de máquina da Amazon (AMI).
6. Em Tipo de instância, selecione o tipo de instância que corresponde à sua reserva de bloco de capacidade.
7. Em Par de chaves (login), escolha um par de chaves existente ou selecione Criar um novo par de chaves para criar um novo. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.
8. Em Network settings (Configurações de rede), use as configurações padrão ou escolha Edit (Editar) para definir as configurações de rede, conforme necessário.

   > **Important**
   >
   > A instância não pode ser iniciada em uma sub-rede em uma zona de disponibilidade diferente da zona de disponibilidade em que o bloco de capacidade está localizado.

9. Em Detalhes avançados, configure a solicitação de instância spot como se segue.
   a. Em Opção de compra (tipo de mercado), selecione Blocos de capacidade.
   b. Em Reserva de capacidade, selecione Direcionar por ID.
   c. Selecione o ID de reserva de capacidade da sua reserva de bloco de capacidade.
10. No painel Summary (Resumo), para Number of instances (Número de instâncias), insira o número de instâncias a serem executadas.
11. Escolha Iniciar instância.

AWS CLI

Para iniciar instâncias em uma reserva de capacidade existente usando a AWS CLI

- Use o comando `run-instances` e especifique um `MarketType` de `capacity-block` na estrutura de `instance-market-options`. Você também deve especificar o parâmetro `capacity-reservation-specification`.

  O exemplo a seguir inicia uma única instância `p5.48xlarge` em um bloco de capacidade ativo com os atributos e a capacidade disponível correspondentes.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \
  --instance-type p5.48xlarge --key-name MyKeyPair \
  --subnet-id subnet-1234567890abcdef1 \
  --instance-market-options MarketType='capacity-block'
  --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Visualizar blocos de capacidade

Os blocos de capacidade têm os seguintes status:

- `payment-pending`: o pagamento antecipado ainda não foi processado.
- `payment-failed`: não foi possível processar o pagamento no prazo de 12 horas. O bloco de capacidade foi liberado.
- `scheduled`: o pagamento foi processado e a reserva do bloco de capacidade ainda não começou.
- `active`: a capacidade reservada está disponível para seu uso.
- `expired`: a reserva do bloco de capacidade expirou automaticamente na data e hora especificadas na solicitação da reserva. A capacidade reservada não está mais disponível para uso.

Você pode usar um dos métodos a seguir para visualizar sua reserva de capacidade.

Console

Para visualizar os blocos de capacidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Reservas de Capacidade.
3. Na página Visão geral das reservas de capacidade, você vê uma tabela de recursos com detalhes sobre todos os seus recursos de reserva de capacidade. Para encontrar suas reservas de blocos de capacidade, selecione Blocos de capacidade na lista suspensa acima de ID da reserva de capacidade. Na tabela, você pode ver informações sobre os blocos de capacidade, como datas de início e término, duração e status.
4. Para obter mais detalhes sobre um bloco de capacidade, selecione o ID da reserva do bloco de capacidade que você deseja visualizar. A página Detalhes da reserva de capacidade exibe todas as propriedades da reserva e o número de instâncias que estão em uso ou que estão disponíveis no bloco de capacidade.

> **Note**
>
> Antes do início de uma reserva do bloco de capacidade, a capacidade disponível aparece como zero. Você pode ver quantas instâncias estarão disponíveis quando a reserva de bloco de capacidade começar usando o seguinte valor de tag para a chave de tag: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Para visualizar os blocos de capacidade usando a AWS CLI

Por padrão, quando você usa o comando describe-capacity-reservations, as reservas de capacidade sob demanda e as reservas de blocos de capacidade são listadas. Para visualizar somente as reservas do bloco de capacidade, filtre usando `capacity-block` para o parâmetro `capacity-reservation-type`.

Por exemplo, o comando a seguir descreve uma ou mais reservas de capacidade na Região da AWS atual.

```
aws ec2 describe-capacity-reservations -reservation-type capacity-block
```

Saída de exemplo.

```
{
    "CapacityReservations": [
        {
```

```
            "CapacityReservationId": "cr-12345678",
            "EndDateType": "limited",
            "ReservationType": "capacity-block"
            "AvailabilityZone": "eu-east-2a",
            "InstanceMatchCriteria": "targeted",
            "EphemeralStorage": false,
            "CreateDate": "2023-11-29T14:22:45Z",
            "StartDate": "2023-12-15T12:00:00Z",
            "EndDate": "2023-08-19T12:00:00Z",
            "AvailableInstanceCount": 0,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 16,
            "State": "payment-pending",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "p5.48xlarge"
        },
        ...
```

Monitorar blocos de capacidade

Tópicos

- Monitorar blocos de capacidade com o EventBridge
- Registrar em log chamadas de API de blocos de capacidade com o AWS CloudTrail

Monitorar blocos de capacidade com o EventBridge

Quando a reserva do bloco de capacidade começa, o Amazon EC2 emite um evento por meio do EventBridge que indica que a capacidade está pronta para ser usada. Quarenta minutos antes do término da reserva do bloco de capacidade, você recebe outro evento do EventBridge informando que todas as instâncias em execução na reserva começarão a ser encerradas em dez minutos. Para obter mais informações sobre eventos do EventBridge, consulte Eventos do Amazon EventBridge.

As seguintes estruturas de eventos para eventos emitidos para blocos de capacidade:

Bloco de capacidade fornecido

O exemplo a seguir mostra um evento para o bloco de capacidade fornecido.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
```

```
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Aviso de expiração do bloco de capacidade

O exemplo a seguir mostra um evento para aviso de expiração do bloco de capacidade.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Registrar em log chamadas de API de blocos de capacidade com o AWS CloudTrail

Os blocos de capacidade são integrados ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS em blocos de capacidade. O CloudTrail captura chamadas de API para blocos de capacidade como eventos. As chamadas capturadas incluem chamadas do console de blocos de capacidade e chamadas de código para as operações de API de blocos de capacidade. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail a um bucket do Amazon S3, incluindo eventos para blocos de capacidade. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas

pelo CloudTrail, você pode determinar a solicitação que foi feita para os blocos de capacidade, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre blocos de capacidade no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre alguma atividade nos blocos de capacidade, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS em Histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para ter um registro contínuo de eventos na Conta da AWS, incluindo os para blocos de capacidade, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Como receber arquivos de log do CloudTrail de várias regiões e Como receber arquivos de log do CloudTrail de várias contas

Todas os blocos de capacidade são registrados em log pelo CloudTrail e são documentados na Amazon EC2 API Reference. Por exemplo, as chamadas para as ações `CapacityBlockScheduled` e `CapacityBlockActive` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management

- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para mais informações, consulte Elemento userIdentity do CloudTrail.

Entender as entradas nos arquivos de log de capacidade

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto não são exibidos em uma ordem específica.

Os seguintes exemplos mostram entradas no log do CloudTrail para:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Alguns campos foram ocultados nos exemplos por questão de privacidade dos dados.

TerminateCapacityBlocksInstances

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
```

```
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/
i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/
i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```

CapacityBlockPaymentFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockScheduled

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
```

```
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```

CapacityBlockActive

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
```

```
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```

CapacityBlockExpired

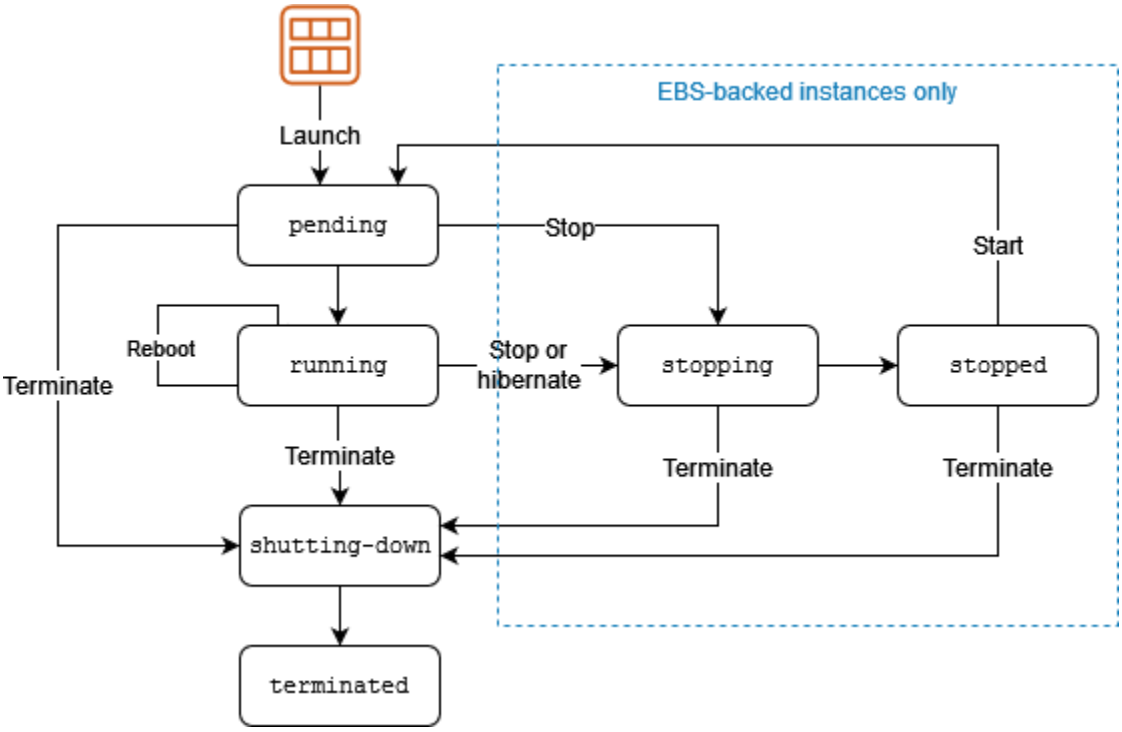
```
{
  "eventVersion": "1.05",
```

```
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```


Ciclo de vida da instância

Uma instância do Amazon EC2 passa por diferentes estados do momento em que você a inicia até seu encerramento.

A ilustração a seguir representa as transições entre os estados da instância. Observe que você não pode parar e o iniciar uma instância com armazenamento de instâncias. Para obter mais informações sobre instâncias baseadas em armazenamento de instâncias, consulte Armazenamento para o dispositivo raiz.



A tabela apresentada a seguir fornece uma breve descrição de cada estado da instância e indica se o uso da instância é faturado. Alguns recursos da AWS, como volumes do Amazon EBS e endereços IP elásticos, incorrem em cobranças independentemente do estado da instância. Para obter mais informações, consulte Evitar cobranças inesperadas no Manual do usuário do AWS Billing.

Estado da instância	Descrição	Faturamento para uso da instância
`pending`	A instância está se preparando para entrar no estado `running`. Uma instância entra no estado `pending` quando ela é executada ou quando é iniciada após estar no estado `stopped`.	Não faturado

Estado da instância	Descrição	Faturamento para uso da instância
running	A instância está em execução e pronta para uso.	Faturado
stopping	A instância está se preparando para ser interrompida.	Não faturado
stopped	A instância está desativada e não pode ser usada. A instância pode ser iniciada a qualquer momento.	Não faturado
shutting-down	A instância está se preparando para ser encerrada.	Não faturado
terminated	A instância foi permanentemente excluída e não pode ser iniciada.	Não faturado **Note** As instâncias reservadas que foram aplicadas a instâncias encerradas são faturadas até o final do prazo de acordo com a opção de pagamento. Para ter mais informações, consulte Reserved Instances.

Conteúdo

- Execução da instância
- Interrupção e início de instância (somente instâncias baseadas no Amazon EBS)
- Hibernação de instância (somente instâncias baseadas no Amazon EBS)
- Reinicialização da instância

- Encerramento de instância
- Diferenças entre reinicialização, interrupção, hibernação e encerramento
- Executar sua instância
- Início e interrupção de instâncias do Amazon EC2
- Hibernar sua instância do Amazon EC2
- Reinicializar a instância
- Encerramento de instâncias do Amazon EC2
- Desativação da instância
- Resiliência de instância

Execução da instância

Quando você executa uma instância, ela entra no estado `pending`. O tipo de instância que você especificou na execução determina o hardware de computador host para sua instância. Usamos a imagem de máquina da Amazon (AMI) especificada na execução para inicializar a instância. Depois de a instância estar pronta para você, ela entra no estado `running`. É possível se conectar à instância em execução e usá-la da forma como usaria um computador bem à sua frente.

Assim que sua instância fizer a transição para o estado `running`, você será cobrado por cada segundo, com o mínimo de um minuto, que mantiver a instância em execução, mesmo se a instância permanecer ociosa e você não se conectar a ela.

Interrupção e início de instância (somente instâncias baseadas no Amazon EBS)

Se sua instância falhar na verificação de status ou não estiver executando suas aplicações como esperado, e se o volume do dispositivo raiz de sua instância for um volume do Amazon EBS, será possível parar e iniciar a instância para tentar corrigir o problema.

Quando você para sua instância, ela entra no estado `stopping` e, em seguida, no estado `stopped`. Você não é cobrado pelas taxas de uso ou transferência de dados da sua instância quando ela é `stopped`. Cobranças são geradas pelo armazenamento de qualquer volume do Amazon EBS. Quando sua instância estiver no estado `stopped`, será possível modificar determinados atributos da instância, inclusive o tipo de instância.

Quando você inicia a instância, ela entra no estado `pending` e é movida para um novo computador host (embora em alguns casos ela permaneça no host atual). Quando você interrompe e inicia instância, perde todos os dados nos volumes de armazenamento de instância anexados ao computador host anterior.

Sua instância retém o endereço IPv4 privado, o que significa que um endereço IP elástico associado ao endereço IPv4 privado ou à interface de rede permanece associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Toda vez que você faz a transição de uma instância de `stopped` para `running`, a cobrança é feita por segundo quando a instância está em execução, com no mínimo um minuto por início de instância.

Para obter mais detalhes sobre como interromper e iniciar instâncias, consulte Início e interrupção de instâncias do Amazon EC2.

Hibernação de instância (somente instâncias baseadas no Amazon EBS)

Ao hibernar uma instância, sinalizamos para o sistema operacional para executar hibernação (suspend-to-disk), o que salva o conteúdo da memória da instância (RAM) no volume raiz do Amazon EBS. Persistimos o volume raiz do Amazon EBS e todos os volumes de dados do Amazon EBS da instância anexados. Quando você inicia a instância, o volume raiz do Amazon EBS é restaurado para seu estado anterior, e o conteúdo da RAM é recarregado. Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

Quando você hiberna a instância, ela entra no estado `stopping` e, em seguida, no estado `stopped`. Não cobramos pelo uso de uma instância hibernada quando ela está no estado `stopped`, mas cobramos quando ela está no estado `stopping`, ao contrário de quando você interrompe uma instância sem hiberná-la. Não cobramos pelo uso de taxas de transferência de dados, mas cobramos pelo armazenamento de qualquer volume do Amazon EBS, incluindo armazenamento dos dados da RAM.

Quando você inicia a instância hibernada, ela entra no estado `pending` e a movemos para um novo computador host (embora em alguns casos, ela permaneça no host atual).

Sua instância retém o endereço IPv4 privado, o que significa que um endereço IP elástico associado ao endereço IPv4 privado ou à interface de rede ainda estará associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.

Reinicialização da instância

É possível reinicializar sua instância usando o console do Amazon EC2, uma ferramenta da linha de comando e a API do Amazon EC2. Recomendamos que você use o Amazon EC2 para reinicializar sua instância em vez de executar o comando de reinicialização do sistema operacional pela sua instância.

A reinicialização de uma instância equivale a reinicialização de um sistema operacional. A instância permanece no mesmo computador host e mantém seu nome DNS público, endereço IP privado e todos os dados em seus volumes de armazenamento de instância. Normalmente demora alguns minutos para a reinicialização ser concluída, mas o tempo necessário para reinicialização depende da configuração da instância.

Reiniciar uma instância não inicia uma novo período de faturamento de instância; o faturamento por segundo continua sem a cobrança mínima de um minuto.

Para ter mais informações, consulte Reinicializar a instância.

Encerramento de instância

Ao perceber que não necessita mais de uma instância, pode encerrá-la. Assim que o estado de uma instância de mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Se você ativou a proteção de encerramento, não poderá encerrar a instância usando o console, a CLI ou a API.

Depois de encerrar uma instância, ela permanecerá visível no console por um curto período, quando será automaticamente excluída. Também é possível descrever uma instância encerrada usando a CLI e a API. Recursos (como tags) são gradualmente dissociados da instância encerrada, portanto podem não ser visíveis na instância encerrada após um breve período. Você não pode se conectar nem recuperar uma instância encerrada.

Cada instância baseada no Amazon EBS é compatível com o atributo `InstanceInitiatedShutdownBehavior`, que controla se a instância é interrompida ou encerrada quando você inicia o desligamento de dentro da própria instância (por exemplo, ao usar o comando shutdown no Linux). O comportamento padrão é interromper a instância. É possível modificar a configuração desse atributo enquanto a instância estiver sendo executada ou parada.

Cada volume do Amazon EBS oferece suporte ao atributo `DeleteOnTermination`, que controla se o volume é excluído ou preservado ao encerrar a instância à qual ela está associada. O padrão é excluir o volume do dispositivo raiz e preservar todos os outros volumes do EBS.

Para ter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Diferenças entre reinicialização, interrupção, hibernação e encerramento

A tabela a seguir resume as principais diferenças entre reinicialização, parada, hibernação e encerramento da sua instância.

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
Computador host	A instância permanece no mesmo computador host	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nenhum
Endereços IPv4 privados e públicos	Esses endereços permanecem iguais	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	Nenhum
Endereços IP	O endereço IP elástico permanece	O endereço IP elástico permanece	O endereço IP elástico permanece	O endereço IP elástico está

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
elásticos (IPv4)	associado à instância	associado à instância	associado à instância	dissociado da instância
Endereço IPv6	A instância mantém seu endereço IPv6	A instância mantém seu endereço IPv6	A instância mantém seu endereço IPv6	Nenhum
Volumes de armazenamento de instâncias	Os dados são preservados	Os dados são apagados	Os dados são apagados	Os dados são apagados
Volume do dispositivo raiz	O volume é preservado	O volume é preservado	O volume é preservado	O volume é excluído por padrão
RAM (conteúdo da memória)	A RAM é apagada	A RAM é apagada	A RAM é salva em um arquivo no volume raiz	A RAM é apagada

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
Faturamento	O momento de faturamento da instância não sofre alterações.	As cobranças de uma instância são interrompidas assim que o estado mudar para `stopping`. Toda vez que uma instância faz a transição de `stopped` para `running`, nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	Você incorre em cobranças quando a instância está no estado `stopping`, mas não incorre em cobranças quando a instância está no estado `stopped`. Toda vez que uma instância faz a transição de `stopped` para `running`, nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	Você deixa de incorrer em cobranças para uma instância assim que o estado é alterado para `shutting-down` .

Os comandos de desligamento do sistema operacional sempre encerra uma instância com armazenamento de instâncias. É possível controlar se os comandos de desativação do sistema operacional param ou encerram uma instância baseada no Amazon EBS. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.

Executar sua instância

Uma instância é um servidor virtual na Nuvem AWS. Você executa uma instância a partir de uma imagem de máquina da Amazon (AMI). A AMI fornece o sistema operacional, o servidor de aplicações e as aplicações para sua instância.

Ao se cadastrar na AWS, será possível começar a usar o Amazon EC2 gratuitamente usando o Nível gratuito da AWS. É possível usar o nível gratuito para iniciar e usar uma instância `t2.micro` gratuitamente por 12 meses (em regiões onde `t2.micro` não estiver disponível, será possível usar uma instância `t3.micro` no nível gratuito). Se você executar uma instância que não esteja no nível gratuito, serão cobradas as taxas de uso padrão do Amazon EC2 para a instância. Para obter mais informações, consulte Definição de preço do Amazon EC2.

É possível executar uma instância usando os métodos a seguir.

Método	Documentação
[Console do Amazon EC2] Use o assistente de execução de instância para especificar os parâmetros de execução.	Inicie uma instância usando o assistente de inicialização de instância
[Console do Amazon EC2] Crie um modelo de execução e execute a instância a partir desse modelo.	Executar uma instância a partir de um modelo de execução
[Console do Amazon EC2] Use uma instância existente como base.	Executar uma instância usando parâmetros de uma instância existente
[Console do Amazon EC2] Use uma AMI comprada do AWS Marketplace.	Executar uma instância AWS Marketplace
[AWS CLI] Use uma AMI selecionada.	Usar o Amazon EC2 pela CLI da AWS
[AWS Tools for Windows PowerShell] Use uma AMI selecionada.	Amazon EC2 pela AWS Tools for Windows PowerShell
[AWS CLI] Use a EC2 Fleet para provisionar capacidade em diferentes tipos de instância do EC2 e zonas de disponibilidade, e em modelos de compra de instância sob demanda, instância reservada e instância spot.	EC2 Fleet
[AWS CloudFormation] Use um modelo de AWS CloudFormation para especificar uma instância.	AWS::EC2::Instance no Manual do usuário do AWS CloudFormation

Método	Documentação
[AWS SDK] Use um SDK específico de idioma da AWS para executar uma instância.	AWS SDK para .NET AWS SDK para C++ AWS SDK for Go AWS SDK for Java AWS SDK for JavaScript AWS SDK for PHP V3 AWS SDK for Python AWS SDK para Ruby V3

Note

Para iniciar uma instância do EC2 em uma sub-rede somente IPv6, você deve usar instâncias desenvolvidas no AWS Nitro System.

Note

Ao iniciar uma instância somente de IPv6, é possível que o DHCPv6 não forneça imediatamente a instância com o servidor de nomes DNS IPv6. Durante esse atraso inicial, talvez a instância não consiga determinar domínios públicos.
Para instâncias em execução no Amazon Linux 2, se você quiser atualizar imediatamente o arquivo /etc/resolv.conf com o servidor de nomes DNS IPv6, execute a diretiva cloud-init seguinte ao iniciá-las:

```
#cloud-config
bootcmd:
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver
 fd00:ec2::253,' /etc/resolv.conf
```

Outra opção é alterar o arquivo de configuração e refazer a imagem da sua AMI para que o arquivo obtenha o endereço do servidor de nomes DNS IPv6 de forma imediata na inicialização.

Ao executar a instância, é possível executá-la em uma sub-rede associada a um dos seguintes recursos:

- Uma zona de disponibilidade – esta opção é o padrão.
- Uma zona local: para executar uma instância em uma zona local, é necessário optar pela zona local e criar uma sub-rede na zona. Para obter mais informações, consulte Get started with Local Zones.
- Uma zona de Wavelength: para executar uma instância em uma zona de Wavelength, opte pela zona de Wavelength e crie uma sub-rede na zona. Para obter informações sobre como iniciar uma instância em uma zona do Wavelength, consulte Get started with AWS Wavelength.
- Um Outpost – para executar uma instância em um Outpost, é necessário criar um Outpost. Para obter informações sobre como criar um Outpost, consulte Get started with AWS Outposts.

Após executar a instância, é possível conectar-se a ela e usá-la. Para começar, o estado da instância é `pending`. Quando o estado de instância for `running`, a instância terá começado a inicialização. Pôde passar um breve tempo antes de você se conectar à instância. Observe que os tipos de instância bare metal podem levar mais tempo para serem executados.

A instância recebe um nome DNS público que é possível usar para contatar a instância pela Internet. A instância também recebe um nome DNS privado que outras instâncias na mesma VPC podem usar para contatar a instância.

Quando você tiver terminado com uma instância, encerre-a. Para ter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta

É possível iniciar uma instância usando o assistente de inicialização de instância. O assistente de lançamento de instâncias especifica todos os parâmetros de início necessários para iniciar uma instância. Quando o assistente de execução de instância fornece um valor padrão, é possível aceitá-

lo ou especificar seu próprio valor. Se você aceitar os valores padrão, será possível iniciar uma instância selecionando apenas um par de chaves.

> **Important**
>
> Quando você executa uma instância que não esteja dentro do Nível gratuito da AWS, será cobrado pelo tempo que a instância é executada, mesmo se ela permanecer inativa.

Tópicos

- Iniciar rapidamente uma instância
- Iniciar uma instância usando parâmetros definidos
- Inicie uma instância usando o assistente de inicialização de instância

Iniciar rapidamente uma instância

Para configurar uma instância rapidamente para fins de teste, siga estas etapas. Você selecionará o sistema operacional e o par de chaves e aceitará os valores padrão. Para obter informações sobre todos os parâmetros do assistente de lançamento de instância, consulte Iniciar uma instância usando parâmetros definidos.

Para iniciar rapidamente uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, a região atual AWS é exibida [por exemplo, Leste dos EUA (Ohio)]. Selecione uma região na qual a instância será iniciada. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre regiões, enquanto outros não podem. Para ter mais informações, consulte Localizações de recursos.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.
5. Em Application and OS Images (Amazon Machine Image), (Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Quick Start (Início rápido) e depois escolha o sistema operacional da sua instância.
6. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.

7. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

Iniciar uma instância usando parâmetros definidos

Exceto pelo par de chaves, o assistente de lançamento de instâncias fornece valores padrão para todos os parâmetros. É possível aceitar qualquer um ou todos os padrões ou configurar uma instância especificando seus próprios valores para cada parâmetro. Os parâmetros são agrupados no assistente de lançamento de instância. As instruções a seguir orientam você por cada grupo de parâmetros.

Parâmetros para configuração de instâncias

- Iniciar a execução da instância
- Nome e tags
- Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon)
- Tipo de instância
- Par de chaves (login)
- Configurações de rede
- Configurar armazenamento
- Detalhes avançados
- Resumo

Iniciar a execução da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, a região atual AWS é exibida [por exemplo, Leste dos EUA (Ohio)]. Selecione uma região na qual a instância será iniciada. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre regiões, enquanto outros não podem. Para ter mais informações, consulte Localizações de recursos.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).

Nome e tags

O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar. É possível marcar a instância, os volumes e as interfaces de rede. Para instâncias spot,

é possível marcar apenas a solicitação de instância spot. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2.

A especificação de um nome de instância e de tags adicionais é opcional.

- Em Name (Nome), insira um nome descritivo para a instância. Se você não especificar um nome, a instância poderá ser identificada por seu ID, que é gerado automaticamente quando você inicia a instância.
- Para adicionar mais tags, selecione Add additional tag (Adicionar outra tag). Escolha Add tag (Adicionar tag), insira uma chave e um valor, e selecione o tipo de recurso a aplicar a tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon)

Uma imagem de máquina da Amazon (AMI) contém as informações necessárias para criar uma instância. Por exemplo, uma AMI pode conter o software que é necessário para atuar como um servidor Web, como o Linux, o Apache e seu site.

É possível encontrar uma AMI adequada da seguinte forma: Caso contrário, escolha Cancel (Cancelar) (no canto superior direito) para retornar ao assistente de lançamento de instâncias sem escolher uma AMI.

Barra de pesquisa

Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa de AMI e pressione Enter. Escolha Select para selecionar uma AMI.

Recents (Recentes)

As AMIs que você usou recentemente.

Escolha Recently launched (Iniciadas recentemente) ou Currently in use (Atualmente em uso) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Minhas AMIs

As AMIs privadas que você possui, ou as AMI privadas que foram compartilhadas com você.

Escolha Owned by me (De minha propriedade) ou Shared with me (Compartilhado comigo) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Início rápido

As AMIs são agrupadas por sistema operacional (SO) para ajudá-lo a começar rapidamente.

Em primeiro lugar, selecione o sistema operacional de que precisa e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI. Para selecionar uma AMI qualificada para o nível gratuito, confira se a AMI está marcada como Free tier eligible (Qualificada para o nível gratuito).

Browse more AMIs (Procurar mais AMIs)

Selecione Browse more AMIs (Procurar mais AMIs) para navegar pelo catálogo completo de AMIs.

- Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa e pressione Enter.
- Para encontrar uma AMI usando um parâmetro do Systems Manager, escolha o botão de seta à direita da barra de pesquisa e escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager). Para ter mais informações, consulte Encontrar uma AMI usando um parâmetro do Systems Manager.
- Para pesquisar por categoria, escolha Quickstart AMIs (AMIS de início rápido), My AMIs (Minhas AMIs), AWS Marketplace AMIs ou Community AMIs (AMIs da comunidade).

  O AWS Marketplace é uma loja online onde é possível comprar software executado na AWS, inclusive AMIs. Para obter mais informações sobre como executar uma instância pelo AWS Marketplace, consulte Executar uma instância AWS Marketplace. Em Community AMIs (AMIs da comunidade), é possível encontrar AMIs que membros da comunidade AWS disponibilizaram para outras pessoas usarem. AMIs da Amazon ou de um parceiro verificado estão marcadas como Provedor verificado.
- Para filtrar a lista de AMIs, marque uma ou mais caixas de seleção em Refine results (Refinar resultados) do lado esquerdo da tela. As opções de filtro são diferentes dependendo da categoria de pesquisa selecionada.
- Verifique Root device type (Tipo de dispositivo raiz) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: ebs (baseadas no Amazon EBS) ou instance-store (baseadas no armazenamento de instâncias). Para ter mais informações, consulte Armazenamento para o dispositivo raiz.
- Verifique o Virtualization type (Tipo de virtualização) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: hvm ou paravirtual. Por exemplo, alguns tipos de instância

exigem HVM. Para obter mais informações sobre os tipos de virtualização do Linux, consulte Tipos de virtualização de AMI.

- Verifique o modo de inicialização listado para cada AMI. Observe quais AMIs usam o modo de inicialização de que você precisa: legacy-bios, uefi ou uefi-preferred. Para ter mais informações, consulte Modos de inicialização do Amazon EC2.
- Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).

Aviso ao alterar a AMI

Se você modificar a configuração de volumes ou grupos de segurança associados à AMI selecionada e escolher uma AMI diferente, será exibida uma janela para avisar que algumas das configurações atuais serão alteradas ou removidas. Você pode revisar as alterações nos grupos de segurança e nos volumes. Além disso, é possível visualizar quais volumes serão adicionados e excluídos ou visualizar apenas os volumes que serão adicionados.

Tipo de instância

O tipo de instância define a configuração do hardware e o tamanho da instância. Os tipos de instâncias maiores têm mais CPU e memória. Para obter mais informações, consulte Tipos de instância do Amazon EC2.

- Em Instance type (Tipo de instância), selecione o tipo de instância da instância.

  Nível gratuito – Se sua conta da AWS tiver menos de 12 meses, você poderá usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro (ou o tipo de instância t3.micro em regiões nas quais o tipo t2.micro estiver indisponível). Se um tipo de instância for qualificada para o nível gratuito, ela será rotulada Free tier eligible (Qualificada ao nível gratuito). Para obter mais informações sobre t2.micro e t3.micro, consulte Instâncias expansíveis.
- Compare instance types (Comparar tipos de instâncias): é possível comparar diferentes tipos de instâncias pelos seguintes atributos: número de vCPUs, arquitetura, quantidade de memória (GiB), quantidade de armazenamento (GB), tipo de armazenamento e performance de rede.
- Obter conselho: você pode obter orientações e sugestões de tipos de instância no seletor de tipo de instância do EC2 Amazon Q. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma nova workload.

Par de chaves (login)

Em Key pair name (Nome do par de chaves), escolha um par de chaves existente ou escolha Create new key pair (Criar um novo par de chaves) para criar um novo. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

> **Important**
>
> Se você escolher a opção Proceed without key pair (Not recommended) (Prosseguir sem par de chaves, não recomendado), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir que os usuários façam login de outro modo.

Configurações de rede

Defina as configurações de rede, conforme necessário.

- VPC: escolha uma VPC existente para sua instância. Você pode escolher a VPC padrão ou uma VPC criada por você. Para ter mais informações, consulte the section called “Nuvens privadas virtuais”.
- Subnet (Sub-rede): é possível executar uma instância em uma sub-rede associada a uma zona de disponibilidade, a uma zona local, a uma zona Wavelength ou a um Outpost.

  Para iniciar a instância em uma zona de disponibilidade, selecione a sub-rede na qual a instância será iniciada. Para criar uma nova sub-rede, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Quando tiver concluído, retorne ao assistente de inicialização da instância e escolha o ícone Refresh (Atualizar) para carregar sua sub-rede na lista.

  Para executar a instância em uma sub-rede somente IPv6, a instância deve ser desenvolvida no Nitro System.

  Para iniciar a instância em uma zona local, selecione uma sub-rede que você criou na zona local.

  Para iniciar uma instância em um Outpost, selecione uma sub-rede em uma VPC associada ao Outpost.
- Auto-assign Public IP (Autoatribuir IP público): especifique se sua instância recebe um endereço IPv4 público. Por padrão, as instâncias em uma sub-rede padrão recebem um endereço IPv4 público, e as instâncias em uma sub-rede não padrão, não. Selecione Enable (Habilitar) ou

Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Para ter mais informações, consulte Endereços IPv4 públicos.

- Firewall (security groups) (Firewall, grupos de segurança): use um grupo de segurança para definir regras de firewall da sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. Para obter mais informações sobre grupos de segurança, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.

  Se adicionar uma interface de rede, especifique o mesmo grupo de segurança na interface de rede.

  Selecione ou crie um grupo de segurança da seguinte forma:

  - Para selecionar um grupo de segurança existente para sua VPC, escolha Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança em Common security groups (Grupos de segurança comuns).
  - Para criar um novo grupo de segurança para sua VPC, escolha Create security group (Criar grupo de segurança). O assistente de inicialização de instância define automaticamente o grupo de segurança launch-wizard-x e fornece as seguintes caixas de seleção para adicionar regras de grupo de segurança rapidamente:

    (Linux) Permitir tráfego SSH de: cria uma regra de entrada para permitir que você se conecte à instância ao usar SSH (porta 22).

    (Windows) Permitir tráfego RDP de: cria uma regra de entrada para permitir que você se conecte à instância por RDP (porta 3389).

    Especifique se o tráfego vem de Anywhere (Qualquer lugar), Custom (Personalizado) ou My IP (Meu IP).

    Allow HTTPs traffic from the internet (Permitir tráfego HTTPS da Internet): cria uma regra de entrada que abre a porta 443 (HTTPS) para permitir o tráfego da Internet de qualquer lugar. Se sua instância for um servidor Web, essa regra será necessária.

    Allow HTTP traffic from the internet (Permitir tráfego HTTPS da Internet): cria uma regra de entrada que abre a porta 80 (HTTP) para permitir o tráfego da Internet de qualquer lugar. Se sua instância for um servidor Web, essa regra será necessária.

    É possível editar essas regras e adicionar regras de acordo com suas necessidades.

Para editar ou adicionar uma regra, escolha Edit (Editar) no canto superior direito. Para adicionar uma regra, escolha Add security group rule (Adicionar regra do grupo de segurança). Em Type (Tipo), selecione o tipo de tráfego da rede. O campo Protocol (Protocolo) é preenchido automaticamente com o protocolo para abrir para o tráfego de rede. Em Source type (Tipo de origem), escolha o tipo da origem. Para permitir que o assistente de inicialização da instância adicione o endereço IP público de seu computador, escolha My IP (Meu IP). No entanto, se você estiver se conectando por meio de um ISP ou por trás de um firewall sem um endereço IP estático, precisará encontrar o intervalo de endereços IP usado pelos computadores clientes.

> **Warning**
>
> Regras que habilitam todos os endereços IP (`0.0.0.0/0`) a acessar a instância por SSH ou RDP são aceitáveis se você for iniciar, por pouco tempo, uma instância de teste e interrompê-la ou terminá-la em breve, mas não são segurar para ambientes de produção. É necessário autorizar apenas um endereço IP específico ou um intervalo de endereços a acessar a instância.

- Advanced network configuration (Configuração avançada de rede): disponível apenas se você escolher uma sub-rede.

  Interface de rede

  - Device index (Índice do dispositivo): o índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância suportam várias placas de rede.
  - Network Interface (Interface de rede): selecione New interface (Nova interface), para deixar o Amazon EC2 criar uma interface nova, ou selecione uma interface de rede existente que esteja disponível.
  - Description (Descrição): (opcional) uma descrição da nova interface de rede.
  - Subnet (Sub-rede): a sub-rede na qual criar a nova interface de rede. Para a interface de rede principal (`eth0`), essa é a sub-rede na qual a instância será executada. Se você tiver inserido uma interface de rede existente para `eth0`, a instância será executada na sub-rede na qual a interface de rede está localizada.
  - Grupos de segurança: um ou mais grupos de segurança na VPC aos quais associar a interface de rede.

- Primary IP (IP principal): um endereço IPv4 privado no intervalo de sua sub-rede. Deixe em branco para que o Amazon EC2 escolha um endereço IPv4 privado para você.
- IP secundário: um ou mais endereços IPv4 privados adicionais do intervalo de endereços da sua sub-rede. Escolha Manually assign (Atribuir manualmente) e insira um endereço IP. Escolha Add IP (Adicionar IP) para adicionar outro endereço IP. Ou escolha Automatically assign (Atribuir automaticamente), para deixar que o Amazon EC2 escolha um para você, e insira um valor para indicar o número de endereços IP a serem adicionados.
- (Somente para IPv6) IPv6 IPs (IPs IPv6): um endereço IPv6 no intervalo da sub-rede. Escolha Manually assign (Atribuir manualmente) e insira um endereço IP. Escolha Add IP (Adicionar IP) para adicionar outro endereço IP. Ou escolha Automatically assign (Atribuir automaticamente), para deixar que o Amazon EC2 escolha um para você, e insira um valor para indicar o número de endereços IP a serem adicionados.
- IPv4 Prefixes (Prefixos IPv4): os prefixos IPv4 para a interface de rede.
- IPv6 Prefixes (Prefixos IPv6): os prefixos IPv6 para a interface de rede.
- (Pilha dupla e somente IPv6) Atribuir IP IPv6 primário: (Opcional) se você estiver iniciando uma instância em uma sub-rede de pilha dupla ou somente IPv6, terá a opção de Atribuir IP IPv6 primário. A atribuição de um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Escolha Habilitar se essa instância depender do seu endereço IPv6 permanecer inalterado. Quando a instância é executada, a AWS atribuirá automaticamente um endereço IPv6 associado à ENI anexada à sua instância como o endereço IPv6 principal. Após habilitar um endereço GUA IPv6 para ser um IPv6 primário, não será possível desabilitá-lo. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se tornará o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada. Se você tiver vários endereços IPv6 associados a uma ENI anexada à sua instância e habilitar um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à ENI se tornará o endereço IPv6 primário.
- Delete on termination (Excluir no encerramento): se a interface de rede deve ser excluída quando a instância for excluída.
- Elastic Fabric Adapter: indica se a interface de rede é um Elastic Fabric Adapter. Para ter mais informações, consulte Elastic Fabric Adapter.
- ENA Express: o ENA Express tem a tecnologia Scalable Reliable Datagram (SRD) da AWS. A tecnologia SRD usa um mecanismo de pulverização de pacotes para distribuir carga e evitar congestionamento de rede. A ativação do ENA Express permite que as instâncias compatíveis se comuniquem usando SRD além do tráfego TCP normal, quando possível. O assistente de

inicialização de instâncias não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar na lista.

- UDP do ENA Express: se habilitou o ENA Express, tem a opção de usá-lo para tráfego UDP. O assistente de inicialização de instâncias não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar.

Escolha Adicionar interface de rede para adicionar mais interfaces de rede. Outras interfaces de rede podem residir em uma sub-rede diferente da mesma VPC ou em uma sub-rede em outra VPC que você possua (desde que a sub-rede esteja na mesma zona de disponibilidade da sua instância). Se optar por adicionar mais uma interface de rede que resida na sub-rede de outra VPC, você verá a opção Sub-redes multi-VPC ao selecionar uma sub-rede. Se você selecionar uma sub-rede em outra VPC, o rótulo Multi-VPC aparecerá ao lado da interface de rede que você adicionou. Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança. Observe que, se anexar uma ENI adicional de outra VPC, você deverá escolher um grupo de segurança para a ENI dessa VPC.

Para ter mais informações, consulte Interfaces de rede elástica. Se você especificar mais de uma interface de rede, sua instância não poderá receber um endereço IPv4 público. Além disso, se você especificar uma interface de rede existente para eth0, não poderá substituir a configuração de IPv4 pública da sub-rede usando Auto-assign Public IP (Atribuir IP público automaticamente). Para ter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância.

Configurar armazenamento

A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume raiz. É possível especificar volumes adicionais a serem anexados à instância.

É possível usar a exibição Simple (Simples) ou Advanced (Avançada). Com a visualização Simple (Simples), especifique o tamanho e o tipo de volume. Para especificar todos os parâmetros de volume, use a exibição Advanced (Avançada), no canto superior direito do cartão.

Usando a exibição Advanced (Avançada), é possível configurar cada volume da seguinte forma:

- Storage type (Tipo de armazenamento): selecione os volumes do Amazon EBS ou de armazenamento de instância para associar à instância. Os tipos de volume disponíveis na lista dependem do tipo de instância escolhido. Para obter mais informações, consulte Armazenamento de instâncias do Amazon EC2 e Volumes do Amazon EBS.

- Device Name (Nome do dispositivo): selecione na lista de nomes de dispositivo disponíveis para o volume.
- Snapshot: selecione o snapshot ao qual o volume será restaurado. Também é possível pesquisar snapshots públicos e compartilhados que estão disponíveis, inserindo texto no campo Snapshot.
- Size (GiB) (Tamanho): para volumes do EBS, especifique um tamanho de armazenamento. Se você tiver selecionado uma AMI e uma instância que estejam qualificadas para o nível gratuito, tenha em mente que para permanecer no nível gratuito, seu armazenamento total deverá ficar abaixo de 30 GiB.
- Volume Type (Tipo de volume): para volumes do EBS, selecione um tipo de volume. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.
- IOPS: se tiver selecionado um tipo de volume Provisioned IOPS SSD, será possível inserir o número de operações de E/S por segundo (IOPS) ao qual o volume pode oferecer suporte.
- Delete on termination (Excluir ao término): em volumes do Amazon EBS, escolha Yes (Sim), para excluir o volume quando a instância associada for terminada, ou escolha No (Não) para manter o volume. Para ter mais informações, consulte Preservação de dados quando uma instância for encerrada.
- Encrypted: (Criptografado): se o tipo de instância oferecer suporte à criptografia do EBS, será possível escolher Yes (Sim) para habilitar criptografia para o volume. Se você tiver habilitado a criptografia por padrão nessa região, a criptografia estará habilitada para você. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.
- KMS Key (Chave do KMS): se você selecionou Yes (Sim) para Encrypted (Criptografado), deve selecionar uma chave gerenciada pelo cliente a ser usada para criptografar o volume. Se tiver habilitado a criptografia por padrão nessa região, a chave gerenciada pelo cliente padrão será selecionada para você. É possível selecionar uma chave diferente ou especificar o ARN de qualquer chave gerenciada pelo cliente que você tenha criado.
- Sistemas de arquivos: monte um sistema de arquivos Amazon EFS ou Amazon FSx na instância. Para obter mais informações sobre a montagem de um sistema de arquivos do Amazon EFS, consulte Uso do Amazon EFS com instâncias do Linux. Para obter mais informações sobre a montagem de um sistema de arquivos do Amazon FSx, consulte Use o Amazon FSx com o Amazon EC2

Detalhes avançados

Em Advanced details (Detalhes avançados), expanda a seção para visualizar os campos e especifique quaisquer parâmetros adicionais para a instância.

- Purchasing option (Opção de compra): escolha Request Spot Instances (Solicitar instâncias spot) para solicitar instâncias spot pelo preço spot, limitado ao preço sob demanda, e escolha Customize(Personalizar) para alterar as configurações padrão da instância spot. É possível definir o preço máximo (não recomendado) e alterar o tipo de solicitação, a duração da solicitação e o comportamento de interrupção. Se você não solicitar uma instância spot, o Amazon EC2 iniciará uma instância sob demanda por padrão. Para ter mais informações, consulte Criar uma solicitação de instância spot.
- Diretório de ingresso em domínio: selecione o diretório do AWS Directory Service (domínio) ao qual sua instância será associada após a inicialização. Se selecionar um domínio, é necessário selecionar a função do IAM com as permissões necessárias. Para obter mais informações sobre o ingresso em domínio de instâncias do Linux, consulte Seamlessly join a Linux EC2 instance to your AWS Managed Microsoft AD directory. Para obter mais informações sobre o ingresso em domínio de instâncias do Windows, consulte Seamlessly join a Windows EC2 instance to your AWS Managed Microsoft AD directory.
- IAM instance profile (Perfil da instância do IAM): um perfil de instância do AWS Identity and Access Management (IAM) a ser associado à instância. Para ter mais informações, consulte Funções do IAM para Amazon EC2.
- Hostname type (Tipo de nome do host): selecione se o nome do host do sistema operacional convidado da instância incluirá o nome do recurso ou o nome do IP. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.
- Hostname DNS (Nome de host DNS): determina se as consultas de DNS para o nome do recurso ou nome do IP (de acordo com o que você selecionou em Hostname type [Tipo de nome do host]) serão respondidas com o endereço IPv4 (registro A), o endereço IPv6 (registro AAAA) ou ambos. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.
- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.
- Stop - Hibernate behavior (Comportamento Parar - Hibernar): para habilitar a hibernação, escolha Enable (Habilitar). Esse campo só está disponível se a instância atender aos pré-requisitos de hibernação. Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.

- Termination protection (Proteção contra término): para evitar o término acidental, escolha Enable (Habilitar). Para ter mais informações, consulte Habilitar a proteção contra encerramento.
- Stop protection (Proteção contra interrupção): para prevenir interrupções acidentais, escolha Enable (Habilitar). Para ter mais informações, consulte Habilitar a proteção contra interrupção.
- Detailed CloudWatch monitoring (Monitoramento detalhado do CloudWatch): escolha Enable (Habilitar) para ativar o monitoramento detalhado da instância usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para ter mais informações, consulte Monitorar instâncias usando o CloudWatch.
- Elastic GPU: o Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.
- Elastic inference (Inferência elástica): uma aceleradora de inferência elástica a ser anexada à instância de CPU do EC2. Para obter mais informações, consulte Trabalhando com o Amazon Elastic Inference no Guia do desenvolvedor do Amazon Elastic Inference.

  > **Note**
  >
  > A partir de 15 de abril de 2023, a AWS não integrará novos clientes ao Amazon Elastic Inference (EI) e ajudará os clientes atuais a migrar suas workloads para opções que ofereçam melhores preço e desempenho. Depois de 15 de abril de 2023, os novos clientes não poderão executar instâncias com aceleradores Amazon EI no Amazon SageMaker, Amazon ECS ou Amazon EC2. No entanto, os clientes que tenham usado o Amazon EI pelo menos uma vez durante os últimos 30 dias serão considerados clientes atuais e poderão continuar usando o serviço.

- Credit specification (Especificação de crédito): escolha Unlimited (Ilimitado) para permitir que as aplicações ultrapassem linha de base pelo tempo que for necessário. Esse campo só é válido para instâncias T. Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Instâncias expansíveis.
- Placement group name (Nome do grupo de posicionamento): especifique um grupo de posicionamento no qual a instância será executada. É possível selecionar um grupo de posicionamento existente ou crie um novo. Nem todos os tipos de instância oferecem suporte ao lançamento de uma instância em um grupo de posicionamento. Para ter mais informações, consulte Grupos de posicionamento.
- EBS-optimized instance (Instância otimizada para EBS): uma instância otimizada para Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade dedicada adicional para E/S

do Amazon EBS. Se o tipo de instância oferecer suporte a esse recurso, escolha Enable (Habilitar) para habilitá-lo. Aplicam-se cobranças adicionais. Para ter mais informações, consulte the section called “Otimização de EBS”.

- Capacity Reservation (Reserva de capacidade): especifique se deseja iniciar a instância em qualquer reserva de capacidade aberta (Open, Aberta), uma reserva de capacidade específica (Target by ID, Alvo por ID) ou um grupo de reservas de capacidade (Target by group, Alvo por grupo). Para especificar que nenhuma reserva de capacidade deva ser usada, escolha None (Nenhuma). Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.
- Tenancy (Locação): escolha se a instância deve ser executada em hardware compartilhado (Shared (Compartilhado)), isolado, hardware dedicado (Dedicated (Dedicado)) ou em um Host dedicado (Dedicated host (Host dedicado)). Se você optar por executar a instância em um Host dedicado, poderá especificar se deseja executar a instância em um grupo de recursos de host ou poderá segmentar um Host dedicado específico. Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Dedicated Instances e Dedicated Hosts.
- RAM disk ID (ID do disco de RAM): (válido somente para AMIs paravirtuais, PV) selecione um disco de RAM para a instância. Se você tiver selecionado um kernel, pode precisar selecionar um disco de RAM específico com os drivers para oferecer suporte a ele.
- Kernel ID (ID do kernel): (válido somente para AMIs paravirtuais, PV) selecione um kernel para a instância.
- Nitro Enclave: permite criar ambientes isolados de execução, chamados de enclaves, com base em instâncias do Amazon EC2. Selecione Enable (Habilitar) para habilitar a instância para o AWS Nitro Enclaves. Para obter mais informações, consulte O que é o AWS Nitro Enclaves? no Guia do usuário do AWS Nitro Enclaves.
- Configurações de licenças: é possível executar instâncias com relação à configuração de licença especificada para rastrear o uso da licença. Para obter mais informações, consulte Crie uma configuração de licença no Guia do usuário do AWS License Manager.
- Metadata accessible (Metadados acessíveis): é possível habilitar ou desabilitar o acesso aos metadados da instância. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Endpoint IPv6 de metadados: você pode habilitar a instância para usar o endereço IPv6 do IMDS `[fd00:ec2::254]` para recuperar os metadados da instância. Essa opção só estará disponível se você for iniciar instâncias baseadas no AWS Nitro System em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas). Para obter mais informações sobre a recuperação de metadados de instâncias, consulte Recuperar metadados da instância.

- Metadata version (Versão de metadados): se você habilitar o acesso aos metadados da instância, poderá optar por exigir o uso de Serviço de metadados da instância versão 2 ao solicitar metadados da instância. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Limite de salto de resposta de metadados: se você habilitar metadados de instância, será possível definir o número permitido de saltos de rede para o token de metadados. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Permitir tags em metadados: se você selecionar Enable (Habilitar), a instância permitirá o acesso a todas as tags dos metadados. Se nenhum valor for especificado, por padrão, o acesso às etiquetas dos metadados da instância não será permitido. Para ter mais informações, consulte Permitir acesso a tags em metadados de instância.
- User data (Dados do usuário): é possível especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para obter mais informações sobre os dados do usuário para as instâncias do Linux, consulte Execução de comandos na instância do Amazon EC2 na inicialização. Para obter mais informações sobre os dados do usuário para as instâncias do Windows, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

Resumo

Use o painel Summary (Resumo) para especificar o número de instâncias a serem iniciadas, revisar a configuração da instância e iniciar as instâncias.

- Number of instances (Número de instâncias): Digite o número de instâncias para executar. Todas as instâncias serão iniciadas com a mesma configuração.

> **Tip**
>
> Para garantir uma execução mais rápida da instância, divida solicitações grandes em lotes menores. Por exemplo, crie cinco solicitações de execução separadas para 100 instâncias cada em vez de uma solicitação de execução para 500 instâncias.

- (Opcional) Se você especificar mais de uma instância, para ajudar a manter o número correto de instâncias para lidar com a demanda da aplicação, escolha Consider EC2 Auto Scaling (Considerar o EC2 Auto Scaling) para criar um modelo de execução e um grupo do Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

> **Note**
>
> Se o Amazon EC2 Auto Scaling marcar uma instância que está em um grupo do Auto Scaling como não íntegro, a instância será programada automaticamente para substituição quando for encerrada e outra for iniciada, e você perderá os dados na instância original. Uma instância será marcada como não íntegra se você parar ou reinicializar a instância, ou se outro evento marcar a instância como não íntegra. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.

- Revise os detalhes da instância e faça as alterações necessárias. É possível navegar diretamente para uma seção escolhendo seu link no painel Summary (Resumo).
- Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).

  Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

  (Opcional) É possível criar um alerta de faturamento para a instância. Na tela de confirmação, em Next Steps (Próximos passos), escolha Create billing alerts (Criar alarmes de faturamento) e siga as instruções. Também poderão ser criados alertas de faturamento após iniciar a instância. Para obter mais informações, consulte Criar um alarme de faturamento para monitorar suas cobranças estimadas da AWS no Guia do usuário do Amazon CloudWatch.

Inicie uma instância usando o assistente de inicialização de instância

Só é possível executar uma instância usando o assistente antigo de execução de instância se sua região oferecer suporte à experiência antiga de execução. O assistente de execução de instância especifica todos os parâmetros de execução necessários para executar uma instância. Quando o assistente de execução de instância fornece um valor padrão, é possível aceitá-lo ou especificar seu próprio valor. É necessário especificar uma AMI e um par de chaves para iniciar uma instância.

Para obter as instruções para usar o novo Assistente de inicialização de instância, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

> **Important**
>
> Quando você executa uma instância que não esteja dentro do Nível gratuito da AWS, será cobrado pelo tempo que a instância é executada, mesmo se ela permanecer inativa.

Etapas para executar uma instância:

- Iniciar a execução da instância
- Etapa 1: Escolher uma imagem de máquina da Amazon (AMI)
- Etapa 2: escolher um tipo de instância
- Etapa 3: configurar detalhes da instância
- Etapa 4: adicionar armazenamento
- Etapa 5: Adicionar tags
- Etapa 6: configurar o grupo de segurança
- Etapa 7: Revisar a execução da instância e selecionar o par de chaves

Iniciar a execução da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, a região atual será exibida (por exemplo, US East (Ohio)). Selecione uma região para a instância que atenda às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre regiões, enquanto outros não podem. Para ter mais informações, consulte Localizações de recursos.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).

Etapa 1: Escolher uma imagem de máquina da Amazon (AMI)

Quando você executa uma instância, deve selecionar uma configuração, conhecida como imagem de máquina da Amazon (AMI). A AMI contém as informações necessárias para criar uma nova instância. Por exemplo, uma AMI pode conter o software necessário para atuar como um servidor Web, como o Linux, o Apache e seu site.

Ao iniciar uma instância, é possível selecionar uma AMI na lista ou selecionar um parâmetro do Systems Manager que aponte para o ID de uma AMI. Para ter mais informações, consulte the section called “Encontrar uma AMI usando um parâmetro do Systems Manager”.

Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon (AMI)), use uma das duas opções para escolher uma AMI. pesquisar a lista de AMIs ou pesquisar por parâmetro do Systems Manager.

Pesquisando a lista de AMIs

1. Selecione o tipo de AMI para usar no painel esquerdo:

   Início rápido

   Uma seleção de AMIs populares para ajudá-lo a começar rapidamente. Para selecionar um AMI qualificado para o nível gratuito, escolha Free tier only (Somente nível gratuito) no painel à esquerda. Essas AMIs estão marcadas como Free tier eligible (Elegíveis para nível gratuito).

   Minhas AMIs

   As AMIs privadas que você possui, ou as AMI privadas que foram compartilhadas com você. Para visualizar as AMIs compartilhadas com você, selecione Shared with me (Compartilhadas comigo) no painel esquerdo.

   AWS Marketplace

   Uma loja online onde é possível comprar software executado na AWS, inclusive AMIs. Para obter mais informações sobre como executar uma instância pelo AWS Marketplace, consulte Executar uma instância AWS Marketplace.

   AMIs da comunidade

   Os AMIs que os membros da comunidade AWS disponibilizaram para outras pessoas usarem. Para filtrar a lista de AMI por sistema operacional, marque a caixa apropriada em Operating system (Sistema operacional). Também é possível filtrar por arquitetura e tipo de dispositivo raiz.

2. (Instâncias do Linux) Verifique o Tipo de dispositivo raiz listado para cada AMI. Observe que as AMIs são tipo de que você precisa, seja `ebs` (com Amazon EBS) ou `instance-store` (com armazenamento de instâncias). Para ter mais informações, consulte Armazenamento para o dispositivo raiz.

3. Verifique o Virtualization type (Tipo de virtualização) listado para cada AMI. Observe que as AMIs são do tipo de que você precisa, seja `hvm` ou `paravirtual`. Por exemplo, alguns tipos de instância exigem HVM. Para obter mais informações sobre os tipos de virtualização do Linux, consulte Tipos de virtualização de AMI.
4. Verifique o modo de inicialização listado para cada AMI. Observe quais AMIs usam o modo de inicialização que você precisa, `legacy-bios` ou `uefi`. Para ter mais informações, consulte Modos de inicialização do Amazon EC2.
5. Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).

Por parâmetro do Systems Manager

1. Escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager) (no canto superior direito).
2. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido ao lado de Currently resolves to (Resolve atualmente para).
3. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.
4. Selecione a AMI na lista e escolha Select (Selecionar).

Etapa 2: escolher um tipo de instância

Na página Choose an Instance Type (Escolher um tipo de instância), selecione a configuração do hardware e o tamanho da instância a ser executada. Os tipos de instâncias maiores têm mais CPU e memória. Para ter mais informações, consulte Tipos de instância do Amazon EC2.

Para permanecer qualificado para o nível gratuito, escolha o tipo de instância t2.micro (ou o tipo de instância t3.micro em regiões onde t2.micro não estiver disponível). Se um tipo de instância for qualificada para o nível gratuito, ela será rotulada Free tier eligible (Qualificada ao nível gratuito). Para obter mais informações sobre t2.micro e t3.micro, consulte Instâncias expansíveis.

Por padrão, o assistente exibe tipos de instância da geração atual e seleciona o primeiro tipo de instância disponível com base na AMI selecionada. Para ver os tipos de instância de geração anterior, escolha All generations (Todas as gerações) na lista de filtros.

> **Note**
>
> Como configurar uma instância rapidamente para fins de teste, escolha Review and Launch (Revisar e executar) para aceitar as configurações padrão e executar a instância. Caso

contrário, para configurar sua instância ainda mais, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

Etapa 3: configurar detalhes da instância

Na página Configure Instance Details (Configurar detalhes da instância), altere as configurações a seguir conforme necessário (expanda Advanced Details (Detalhes avançados) para visualizar todas as configurações) e selecione Next: Add Storage (Próximo: Adicionar armazenamento):

- Number of instances (Número de instâncias): Digite o número de instâncias para executar.

> **Tip**
>
> Para garantir uma execução mais rápida da instância, divida solicitações grandes em lotes menores. Por exemplo, crie cinco solicitações de execução separadas para 100 instâncias cada em vez de uma solicitação de execução para 500 instâncias.

- (Opcional) Para ajudar a assegurar que você mantenha o número de instâncias para lidar com a demanda do aplicativo, escolha Launch into Auto Scaling Group (Executar no grupo de Auto Scaling) para criar uma configuração de execução e um grupo de Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

> **Note**
>
> Se o Amazon EC2 Auto Scaling marcar uma instância que está em um grupo do Auto Scaling como não íntegro, a instância será programada automaticamente para substituição quando for encerrada e outra for iniciada, e você perderá os dados na instância original. Uma instância será marcada como não íntegra se você parar ou reinicializar a instância, ou se outro evento marcar a instância como não íntegra. Para obter mais informações, consulte Verificações de integridade de instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

- Purchasing option (Opção de compra): escolha Request Spot instances (Solicitar instâncias spot) para executar uma instância Spot. Isso adiciona e remove opções desta página. Opcionalmente, você pode definir seu preço máximo (não recomendado) e alterar o tipo de solicitação, o

comportamento de interrupção e a validade da solicitação. Para ter mais informações, consulte Criar uma solicitação de instância spot.

- Network (Rede): selecione a VPC ou, para criar uma nova VPC, selecione Create new VPC (Criar nova VPC) para acessar o console da Amazon VPC. Quando tiver concluído, retorne ao assistente de inicialização da instância e escolha Refresh (Atualizar) para carregar sua VPC na lista.
- Subnet (Sub-rede): é possível executar uma instância em uma sub-rede associada a uma zona de disponibilidade, a uma zona local, a uma zona de Wavelength ou a um Outpost.

  Para executar a instância em uma zona de disponibilidade, selecione a sub-rede na qual a instância será executada. É possível selecionar No preference (Sem preferência) para deixar a AWS escolher uma sub-rede padrão em alguma zona de disponibilidade. Para criar uma nova sub-rede, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Quando tiver concluído, retorne ao assistente e escolha Refresh (Atualizar) para carregar sua sub-rede na lista.

  Para iniciar a instância em uma zona local, selecione uma sub-rede que você criou na zona local.

  Para executar uma instância em um Outpost, selecione uma sub-rede em uma VPC associada a um Outpost.
- Auto-assign Public IP (Autoatribuir IP público): especifique se sua instância recebe um endereço IPv4 público. Por padrão, as instâncias em uma sub-rede padrão recebem um endereço IPv4 público, e as instâncias em uma sub-rede não padrão, não. Selecione Enable (Habilitar) ou Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Para ter mais informações, consulte Endereços IPv4 públicos.
- Auto-assign IPv6 IP (Autoatribuir IP do IPv6): especifique se sua instância recebe um endereço IPv6 do intervalo da sub-rede. Selecione Enable (Habilitar) ou Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Essa opção só estará disponível se você tiver associado um bloco CIDR IPv6 com sua VPC e sub-rede. Para obter mais informações, consulte Adicionar um bloco CIDR IPv6 à sua VPC no Guia do usuário da Amazon VPC.
- Hostname type (Tipo de nome do host): selecione se o nome do host do sistema operacional convidado da instância incluirá o nome do recurso ou o nome do IP. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.
- Hostname DNS (Nome de host DNS): determina se as consultas de DNS para o nome do recurso ou nome do IP (de acordo com o que você selecionou em Hostname type [Tipo de nome do host]) serão respondidas com o endereço IPv4 (registro A), o endereço IPv6 (registro AAAA) ou ambos. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.

- Diretório de ingresso em domínio: selecione o diretório do AWS Directory Service (domínio) ao qual sua instância será associada após a inicialização. Se selecionar um domínio, é necessário selecionar a função do IAM com as permissões necessárias. Para obter mais informações sobre o ingresso em domínio de instâncias do Linux, consulte Seamlessly join a Linux EC2 instance to your AWS Managed Microsoft AD directory. Para obter mais informações sobre o ingresso em domínio de instâncias do Windows, consulte Seamlessly join a Windows EC2 instance.
- Placement group (Grupo de posicionamento): um grupo de posicionamento determina a estratégia de posicionamento das instâncias. Selecione um grupo de posicionamento existente ou crie um novo. Essa opção só estará disponível se você tiver selecionado um tipo de instância que ofereça suporte aos grupos de posicionamento. Para ter mais informações, consulte Grupos de posicionamento.
- Reserva de capacidade: especifique se deseja executar a instância em capacidade compartilhada, qualquer Reserva de capacidade `open`, uma Reserva de capacidade específica ou um grupo de Reserva de capacidade. Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.
- IAM role (Função do IAM): selecione a função do AWS Identity and Access Management (IAM) para associar à instância. Para ter mais informações, consulte Funções do IAM para Amazon EC2.
- CPU options (Opções de CPU): escolha Specify CPU options (Especificar opções de CPU) para especificar um número personalizado de vCPUs durante a execução. Defina o número de núcleos de CPU e de threads por núcleo. Para ter mais informações, consulte Otimizar as opções de CPU.
- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.
- Stop - Hibernate behavior (Interromper - comportamento de hibernação): para habilitar a hibernação, marque essa caixa de seleção. Essa opção só estará disponível se a instância atender aos pré-requisitos de hibernação. Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.
- Enable termination protection (Permitir proteção de encerramento): para evitar o encerramento acidental, marque esta caixa de seleção. Para ter mais informações, consulte Habilitar a proteção contra encerramento.
- Enable termination protection (Habilitar a proteção contra interrupção): para evitar a interrupção acidental, selecione esta caixa. Para ter mais informações, consulte Habilitar a proteção contra interrupção.

- Monitoring (Monitoramento): marque esta caixa de seleção para ativar o monitoramento detalhado da instância usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para ter mais informações, consulte Monitorar instâncias usando o CloudWatch.
- EBS-Optimized instance (Instância otimizada para EBS): uma instância otimizada para Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade dedicada adicional para E/S do Amazon EBS. Se o tipo de instância é compatível com esse recurso, marque esta caixa de seleção pra habilitá-lo. Aplicam-se cobranças adicionais. Para ter mais informações, consulte Instâncias otimizadas para Amazon EBS.
- Tenancy (Alocação): se você estiver executando a instância em uma VPC, poderá optar por executar a instância em hardware isolado e dedicado (Dedicated - Dedicado) ou em um host dedicado (Dedicated host - Host dedicado). Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Dedicated Instances e Dedicated Hosts.
- T2/T3 Unlimited (T2/T3 ilimitado): marque essa caixa de seleção para permitir que as aplicações tenham expansão acima da linha de base pelo tempo que for necessário. Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Instâncias expansíveis.
- Sistemas de arquivos: Para criar um novo sistema de arquivos para montar na instância, escolha Create new file system (Criar novo sistema de arquivos), insira um nome para o novo sistema de arquivos e escolha Create (Criar). O sistema de arquivos é criado usando Quick Create (Criação rápida) de Amazon EFS, que aplica as configurações recomendadas pelo serviço. Os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos são criados e anexados automaticamente à instância e aos destinos de montagem do sistema de arquivos. Também é possível optar por criar e anexar manualmente os grupos de segurança necessários. Para montar um ou mais sistemas de arquivos de Amazon EFS existentes na instância, escolha Add file system (Adicionar sistema de arquivos) e, em seguida, escolha os sistemas de arquivos a serem montados e os pontos de montagem a serem usados. Para ter mais informações, consulte Uso do Amazon EFS com instâncias do Linux.
- Network interfaces (Interfaces de rede): se você tiver selecionado uma sub-rede específica, pode especificar até duas interfaces de rede para sua instância:
  - Para Network Interface (Interface de rede), selecione New network interface (Nova interface de rede) para deixar a AWS criar uma interface nova ou selecione uma interface de rede existente e disponível.
  - Para Primary IP (IP primário), insira um endereço IPv4 privado do intervalo da sua sub-rede ou deixe Auto-assign (Atribuir automaticamente) para deixar a AWS escolher um endereço IPv4 privado para você.

- Para Secondary IP addresses (Endereços IP secundários), escolha Add IP (Adicionar IP) para atribuir mais de um endereço IPv4 privado à interface de rede selecionada.
- (Somente IPv6) Em IPv6 IPs (IPs IPv6), escolha Add IP (Adicionar IP) e insira um endereço IPv6 do intervalo da sub-rede ou deixe como Auto-assign (Atribuir automaticamente) para permitir que a AWS escolha um para você.
- Network Card Index (Índice da placa de rede): O índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância suportam várias placas de rede.
- Selecione Add Device (Adicionar dispositivo) para adicionar uma interface de rede secundária. Uma interface de rede secundária pode residir em uma sub-rede diferente da VPC, pois está na mesma zona de disponibilidade que sua instância.

Para ter mais informações, consulte Interfaces de rede elástica. Se você especificar mais de uma interface de rede, sua instância não poderá receber um endereço IPv4 público. Além disso, se você especificar uma interface de rede existente para eth0, não poderá substituir a configuração de IPv4 pública da sub-rede usando Auto-assign Public IP (Atribuir IP público automaticamente). Para ter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância.

- Kernel ID (ID do kernel): (válido somente para AMIs paravirtuais (PV)) selecione Use default (Usar padrão), a menos que deseje usar um kernel específico.
- RAM disk ID (ID do disco de RAM): (válido somente para AMIs paravirtuais (PV)) selecione Use default (Usar padrão), a menos que deseje usar um disco RAM específico. Se você tiver selecionado um kernel, pode precisar selecionar um disco de RAM específico com os drivers para oferecer suporte a ele.
- Enclave: selecione Enable (Ativar) para ativar a instância para o AWS Nitro Enclaves. Para obter mais informações, consulte O que é o AWS Nitro Enclaves? no Guia do usuário do AWS Nitro Enclaves.
- Metadados acessíveis: é possível habilitar ou desabilitar o acesso ao Serviço de metadados de instância (IMDS). Para ter mais informações, consulte Usar IMDSv2.
- Endpoint IPv6 de metadados: você pode habilitar a instância para usar o endereço IPv6 do IMDS `[fd00:ec2::254]` para recuperar os metadados da instância. Essa opção só estará disponível se você for iniciar instâncias baseadas no AWS Nitro System em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas). Para obter mais informações sobre a recuperação de metadados de instâncias, consulte Recuperar metadados da instância.

- Versão de metadados: se você habilitar o acesso ao IMDS, poderá optar por exigir o uso do Serviço de metadados de instância versão 2 ao solicitar metadados da instância. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Limite de salto de resposta do token de metadados: se você habilitar o IMDS, poderá definir o número permitido de saltos de rede para o token de metadados. Para ter mais informações, consulte Usar IMDSv2.
- User data (Dados do usuário): é possível especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para associar um arquivo, selecione a opção As file (Como arquivo) e procure o arquivo a ser associado.

Etapa 4: adicionar armazenamento

A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Add Storage (Adicionar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Configure cada volume conforme a seguir e escolha Next: Add Tags (Próximo: Adicionar tags).

- Type (Tipo): selecione os volumes de armazenamento de instâncias ou do Amazon EBS para associar à instância. Os tipos de volume disponíveis na lista dependem do tipo de instância escolhido. Para obter mais informações, consulte Armazenamento de instâncias do Amazon EC2 e Volumes do Amazon EBS.
- Device (Dispositivo): selecione a lista de nomes de dispositivo disponíveis para o volume.
- Snapshots: digite o nome ou o ID do snapshot do qual deseja restaurar um volume. Também é possível pesquisar snapshots públicos e compartilhados que estão disponíveis digitando o texto no campo Snapshot. As descrições do snapshot diferenciam maiúsculas de minúsculas.
- Size (Tamanho): para volumes do EBS, especifique um tamanho de armazenamento. Mesmo se você tiver selecionado uma AMI e uma instância que estejam qualificadas para o nível gratuito, para permanecer no nível gratuito, seu armazenamento total deverá ficar abaixo de 30 GiB.
- Volume Type (Tipo de volume): para volumes do EBS, selecione um tipo de volume. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.
- IOPS: se tiver selecionado um tipo de volume Provisioned IOPS SSD, será possível inserir o número de operações de E/S por segundo (IOPS) ao qual o volume pode oferecer suporte.

- Delete on Termination (Excluir ao finalizar): para volumes do Amazon EBS, marque esta caixa para excluir o volume quando a instância for encerrada. Para ter mais informações, consulte Preservação de dados quando uma instância for encerrada.
- Encrypted (Criptografado): se o tipo de instância oferecer suporte à criptografia do EBS, será possível especificar o estado de criptografia do volume. Se tiver habilitado a criptografia por padrão nessa região, a chave gerenciada pelo cliente padrão será selecionada para você. Será possível selecionar uma chave diferente ou desabilitar a criptografia. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

Etapa 5: Adicionar tags

Na página Add Tags (Adicionar tags), especifique as tags fornecendo combinações de chave e valor. É possível marcar a instância, os volumes ou ambos com uma tag. Para instâncias spot, é possível marcar apenas a solicitação de instância spot. Escolha Add another tag (Adicionar outra tag) para adicionar mais de uma tag aos seus recursos. Escolha Next: Configure Security Group ao concluir.

Etapa 6: configurar o grupo de segurança

Na página Configurar grupo de segurança, use um grupo de segurança para definir regras do firewall para sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. (Para mais informações sobre grupos de segurança, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.) Selecione ou crie um grupo de segurança da forma a seguir e escolha Review and Launch (Revisar e executar).

- Para selecionar um grupo de segurança existente, escolha Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança. (Opcional) Não é possível editar as regras de um grupo de segurança existente, mas é possível copiá-las a um novo grupo escolhendo Copy to new (Copiar para novo). Em seguida, adicione as regras conforme descrito na próxima etapa.
- Para criar um novo grupo de segurança, escolha Create a new security group (Criar um novo grupo de segurança). O assistente define automaticamente o grupo de segurança launch-wizard-x e cria uma regra de entrada para permitir que você se conecte à sua instância. As instâncias do Linux usam uma regra de entrada para SSH (porta 22), e as instâncias do Windows usam uma regra de entrada para RDP (porta 3389).
- É possível adicionar regras de acordo com suas necessidades. Por exemplo, se a instância for um servidor Web, abra as portas 80 (HTTP) e 443 (HTTPS) para permitir o tráfego de Internet.

Para adicionar uma regra, escolha Add Rule (Adicionar regra), selecione o protocolo para abrir o tráfego de rede e especifique a origem. Escolha My IP (Meu IP) na lista Source (Origem) para deixar o assistente adicionar o endereço IP público do seu computador. No entanto, se você estiver se conectando por meio de um ISP ou por trás de um firewall sem um endereço IP estático, precisará encontrar o intervalo de endereços IP usado pelos computadores clientes.

> **Warning**
>
> Regras que permitem que todos os endereços IP (`0.0.0.0/0`) acessem a instância via SSH ou RDP são aceitáveis neste exercício rápido, mas não são seguras para ambientes de produção. É necessário autorizar apenas um endereço IP específico ou um intervalo de endereços a acessar a instância.

Etapa 7: Revisar a execução da instância e selecionar o par de chaves

Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da sua instância e faça qualquer alteração necessária selecionando o link Edit (Editar) apropriado.

Quando estiver pronto, escolha Launch (Executar).

Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), será possível escolher um par de chaves existente ou poderá criar um novo. Por exemplo, selecione Choose an existing key pair (Escolha um par de chaves existente) e selecione o par de chaves que você criou para obter configuração. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

> **Important**
>
> Se você escolher a opção Proceed without key pair (Continuar sem par de chaves), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir aos usuários uma maneira efetuar login.

Para executar uma instância, selecione a caixa de confirmação e escolha Launch Instances (Executar instâncias).

(Opcional) É possível criar um alarme de verificação de status para a instância (taxas adicionais podem ser aplicadas). Na tela de confirmação, escolha Create status check alarms (Criar alarmes

de verificação de status) e siga as instruções. Também poderão ser criados alarmes de verificação de status após iniciar a instância. Para ter mais informações, consulte Criar e editar alarmes de verificação de status.

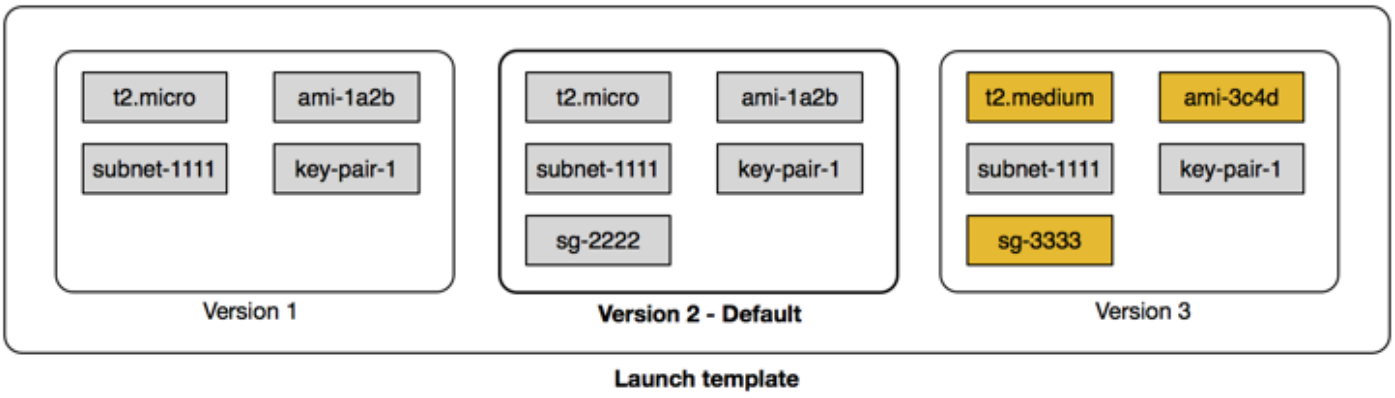
Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Executar uma instância a partir de um modelo de execução

É possível usar um modelo de execução para armazenar parâmetros de inicialização de instâncias para que não seja necessário especificá-los sempre que iniciar uma instância. Por exemplo, você pode criar um modelo de execução com o ID da AMI, o tipo de instância e as configurações de rede que normalmente usa para iniciar instâncias. Ao iniciar uma instância usando o console do Amazon EC2, um AWS SDK ou uma ferramenta de linha de comando, é possível especificar o modelo de execução em vez de inserir os parâmetros novamente.

Para cada modelo de execução, é possível criar uma ou mais versões de modelo de execução numeradas. Cada versão pode ter diferentes parâmetros de execução. Ao executar uma instância a partir de um modelo de execução, será possível usar qualquer versão do modelo de execução. Se você não especificar uma versão, a versão padrão será usada. É possível definir qualquer versão do modelo de execução como a versão padrão — por padrão, ela é a primeira versão do modelo de execução.

O diagrama a seguir mostra um modelo de execução com três versões. A primeira versão especifica o tipo de instância, o ID da AMI, a sub-rede e o par de chaves a ser usado para executar a instância. A segunda versão baseia-se na primeira versão e também especifica um grupo de segurança para a instância. A terceira versão usa valores diferentes para alguns parâmetros. A versão 2 é definida como a versão padrão. Se você tiver executado uma instância a partir desse modelo de execução, os parâmetros de execução da versão 2 serão usados caso nenhuma outra versão tenha sido especificada.



Conteúdo

- Restrições do modelo de execução
- Controlar o acesso a modelos de execução com permissões do IAM
- Use modelos de inicialização para controlar a inicialização das instâncias
- Criar um modelo de inicialização
- Modificar um modelo de inicialização (gerenciar versões do modelo de inicialização)
- Excluir um modelo de execução
- Iniciar uma instância a partir de um modelo de inicialização

Restrições do modelo de execução

As seguintes regras se aplicam aos modelos de execução e às respectivas versões:

- Cotas: para visualizar as cotas para os modelos de execução e as versões de modelos de execução, abra o console do Service Quotas ou use o comando da AWS CLI list-service-quotas. Cada conta da AWS pode ter até 5 mil modelos de execução por região e até 10 mil versões por modelo de execução. Suas contas podem ter cotas diferentes com base na idade e no histórico de uso.
- Os parâmetros são opcionais: os parâmetros do modelo de inicialização são opcionais. No entanto, você precisa garantir que sua solicitação de execução de uma instância inclua todos os parâmetros necessários. Por exemplo, se o modelo de execução não inclui um ID de AMI, você deverá especificar o modelo de execução e um ID de AMI ao executar uma instância.
- Parâmetros não validados: os parâmetros do modelo de inicialização não são totalmente validados quando você cria o modelo. Se você especificar valores incorretos para parâmetros, ou se não usar combinações de parâmetro compatíveis, nenhuma instância poderá ser iniciada usando esse modelo de execução. Verifique se você especificou os valores corretos para os parâmetros e usou combinações de parâmetro compatíveis. Por exemplo, para executar uma instância em um grupo de posicionamento, especifique um tipo de instância compatível.
- Tags: você pode marcar um modelo de inicialização, mas não pode marcar uma versão de modelo de inicialização.
- Imutável: os modelos de execução são imutáveis. Para modificar um modelo de inicialização, é necessário criar uma nova versão do modelo de inicialização.
- Números de versão: as versões de modelo de inicialização são numeradas na ordem em que são criadas. Ao criar uma versão de modelo de execução, você não pode especificar o número de versão por conta própria.

Controlar o acesso a modelos de execução com permissões do IAM

É possível usar permissões do IAM para controlar quais ações do modelo de execução os usuários podem realizar, como visualizar, criar ou excluir modelos de execução.

Ao conceder permissão aos usuários para criar modelos de execução e versões de modelos de execução, não é possível usar as permissões em nível de recursos para restringir os recursos que eles podem especificar em um modelo de execução. Portanto, certifique-se de conceder permissões para a criação de modelos de execução e versões de modelos de execução somente aos administradores apropriados.

Você deve conceder as permissões necessárias para a criação e para o acesso aos recursos especificados no modelo de execução a qualquer pessoa que usará um modelo de execução. Por exemplo:

- Para iniciar uma instância usando uma imagem de máquina da Amazon (AMI) privada compartilhada, o usuário deve ter permissão para iniciar a AMI.
- Para criar volumes do EBS com etiquetas usando snapshots existentes, o usuário deve ter acesso de leitura aos snapshots e permissões para criar e fazer a marcação dos volumes.

Conteúdo

- ec2:CreateLaunchTemplate
- ec2:DescribeLaunchTemplates
- ec2:DescribeLaunchTemplateVersions
- ec2:DeleteLaunchTemplate
- Controlar permissões de controle de versão
- Controlar o acesso a tags em modelos de execução

ec2:CreateLaunchTemplate

Para criar um modelo de execução no console ou usando as APIs, a entidade principal deve ter a permissão `ec2:CreateLaunchTemplate` em uma política do IAM. Sempre que possível, use tags para ajudar você a controlar o acesso aos modelos de execução na conta.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para criar modelos de execução somente se o modelo usa a tag especificada (*`purpose`* = *`testing`*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

As entidades principais que criam modelos de execução podem precisar de algumas permissões relacionadas, como:

- ec2:CreateTags: para adicionar tags ao modelo de execução durante a operação `CreateLaunchTemplate`, o chamador de `CreateLaunchTemplate` deve ter a permissão `ec2:CreateTags` em uma política do IAM.
- ec2:RunInstances: para iniciar instâncias do EC2 a partir do modelo de execução que criou, a entidade principal também deve ter a permissão `ec2:RunInstances` em uma política do IAM.

Para ações de criação de recursos que aplicam tags, os usuários devem ter a permissão `ec2:CreateTags`. A declaração de política do IAM a seguir usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `CreateLaunchTemplate`. Os usuários não podem marcar modelos de execução existentes nem nenhum outro recurso. Para ter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
}
```

O usuário do IAM que cria um modelo de execução não recebe automaticamente permissão para usar o modelo de execução que criou. Como qualquer outra entidade principal, o criador do modelo de execução precisa obter permissão por meio de uma política do IAM. Se um usuário do IAM quiser iniciar uma instância do EC2 a partir de um modelo de execução, ele deverá ter a permissão `ec2:RunInstances`. Ao conceder essas permissões, é possível especificar que os usuários só poderão usar modelos de execução com tags ou IDs específicos. Você também pode controlar a AMI e outros recursos aos quais qualquer pessoa que use modelos de execução possa fazer referência e usar ao iniciar instâncias especificando permissões em nível de recurso para a chamada `RunInstances`. Para obter exemplos de políticas, consulte Modelos de execução.

ec2:DescribeLaunchTemplates

Para listar modelos de execução na conta, a entidade principal deve ter a permissão `ec2:DescribeLaunchTemplates` em uma política do IAM. Porque as ações `Describe` não oferecem suporte a permissões em nível de recurso, é necessário especificá-las sem condições, e o valor do elemento de recurso na política deve ser `"*"`.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para listar todos os modelos de execução na conta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2:DescribeLaunchTemplateVersions

As entidades principais que visualizam modelos de execução também devem ter a permissão `ec2:DescribeLaunchTemplateVersions` para recuperar todo o conjunto de atributos que compõem os modelos de execução.

Para listar versões de modelos de execução na conta, a entidade principal deve ter a permissão `ec2:DescribeLaunchTemplateVersions` em uma política do IAM. Porque as ações `Describe` não oferecem suporte a permissões em nível de recurso, é necessário especificá-las sem condições, e o valor do elemento de recurso na política deve ser `"*"`.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para listar todas as versões de modelos de execução na conta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2:DeleteLaunchTemplate

> **Important**
>
> Tenha cuidado ao conceder permissão às entidades principais para excluir um recurso. A exclusão de um modelo de execução pode causar uma falha em um recurso da AWS que depende desse modelo.

Para excluir um modelo de execução, a entidade principal deve ter a permissão `ec2:DeleteLaunchTemplate` em uma política do IAM. Sempre que possível, use chaves de condição baseadas em tag para limitar as permissões.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para excluir modelos de execução somente se o modelo usa a tag especificada (*purpose* = *testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Como alternativa, é possível usar ARNs para identificar o modelo de execução ao qual a política do IAM se aplica.

Um modelo de execução tem o ARN a seguir.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

É possível especificar vários ARNs colocando-os em uma lista ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal exclua qualquer modelo de execução na conta.

Controlar permissões de controle de versão

Para administradores confiáveis, é possível conceder acesso para criar e excluir versões de um modelo de execução e para alterar a versão padrão de um modelo de execução usando políticas do IAM semelhantes aos exemplos a seguir.

Important

Tenha cuidado ao conceder permissão às entidades principais para criar versões de modelos de execução ou modificar esses modelos.

- Ao criar uma versão do modelo de execução, você afetará todos os recursos da AWS que permitem que o Amazon EC2 inicie instâncias em seu nome com a versão `Latest`.
- Ao modificar um modelo de execução, você pode alterar qual versão é a `Default` e, consequentemente, afetar quaisquer recursos da AWS permitem que o Amazon EC2 inicie instâncias em seu nome com essa versão modificada.

Além disso, é necessário ter cuidado ao lidar com os recursos da AWS que interagem com a versão do modelo de execução `Latest` ou `Default`, como o EC2 Fleet e o Frota Spot. Quando uma versão diferente do modelo de execução é usada para `Latest` ou `Default`, o Amazon EC2 não verifica novamente as permissões para que as ações sejam concluídas ao iniciar novas instâncias para atender à capacidade desejada da frota porque não há interação do usuário com o recurso da AWS. Ao conceder permissão ao usuário para chamar as APIs `CreateLaunchTemplateVersion` e `ModifyLaunchTemplate`, o usuário receberá efetivamente a permissão `iam:PassRole` se apontar a frota para uma versão do modelo de execução diferente que contenha um perfil de instância (um contêiner para um perfil do IAM). Isso significa que um usuário pode atualizar um modelo de execução para transferir um perfil do IAM para uma instância, mesmo que não tenha a permissão `iam:PassRole`. É possível gerenciar esse risco tomando cuidado ao conceder permissões para quem pode criar e gerenciar versões de modelos de execução.

ec2:CreateLaunchTemplateVersion

Para criar uma nova versão de um modelo de execução, a entidade principal deve ter a permissão `ec2:CreateLaunchTemplateVersion` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para criar versões de modelos de execução somente se a versão usa a tag especificada (*`environment`* = *`production`*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal crie versões de qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:DeleteLaunchTemplateVersion

> **Important**
>
> Como sempre, tenha cuidado ao conceder permissão às entidades principais para excluir um recurso. A exclusão de uma versão de modelo de execução pode causar uma falha em um recurso da AWS que depende dessa versão.

Para excluir uma versão de modelo de execução, a entidade principal deve ter a permissão `ec2:DeleteLaunchTemplateVersion` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para excluir versões de modelos de execução somente se a versão usa a tag especificada (*`environment`* = *`production`*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal exclua versões de qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:ModifyLaunchTemplate

Para alterar a versão `Default` associada a um modelo de execução, a entidade principal deve ter a permissão `ec2:ModifyLaunchTemplate` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para modificar modelos de execução somente se o modelo de execução usa a tag especificada (*environment* = *production*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal modifique qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Controlar o acesso a tags em modelos de execução

É possível usar chaves de condição para limitar permissões de tag quando o recurso é um modelo de execução. Por exemplo, a política do IAM a seguir permite remover somente a tag com a chave *temporary* dos modelos de lançamento na conta e região especificadas.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Para obter mais informações sobre as chaves de condições que você pode usar para controlar as chaves e valores de tag que podem ser aplicados aos recursos do Amazon EC2, consulte Controlar o acesso a tags específicas.

Use modelos de inicialização para controlar a inicialização das instâncias

Por exemplo, você pode especificar que os usuários só poderão iniciar instâncias usando um modelo de inicialização e que só poderão usar um modelo de inicialização específico. Você também pode controlar quem pode criar, modificar, descrever e excluir modelos de inicialização e versões do modelo de inicialização.

Uso de modelos de execução para controlar parâmetros de execução

Um modelo de execução pode conter todos ou alguns parâmetros para executar uma instância. Quando executa uma instância usando um modelo de execução, é possível substituir os parâmetros especificados no modelo de execução. Ou pode especificar parâmetros adicionais que não estão no modelo de execução.

> **Note**
>
> Não é possível remover os parâmetros do modelo de execução durante a execução (por exemplo, não é possível especificar um valor nulo para o parâmetro). Para remover um parâmetro, crie uma nova versão do modelo de execução sem o parâmetro e use essa versão para executar a instância.

Para iniciar instâncias, os usuários devem ter permissões para usar a ação `ec2:RunInstances`. Os usuários também devem ter permissões para criar ou usar os recursos que são criados

ou estão associados à instância. É possível usar permissões em nível de recurso para a ação `ec2:RunInstances` para controlar os parâmetros de execução que podem ser especificados pelos usuários. Como alternativa, é possível conceder permissões aos usuários para executar uma instância usando um modelo de execução. Isso permite que você gerencie parâmetros de execução em um modelo de execução, em vez de uma política do IAM, e use um modelo de execução como um veículo de autorização para executar instâncias. Por exemplo, você pode especificar que os usuários só poderão iniciar instâncias usando um modelo de execução e que só poderão usar um modelo de execução específico. Também é possível controlar os parâmetros de execução que os usuários podem substituir no modelo de execução. Para obter exemplos de políticas, consulte Modelos de execução.

Controlar o uso dos modelos de execução

Por padrão, os usuários não têm permissões para trabalhar com modelos de execução. É possível criar uma política que concede aos usuários permissões para criar, modificar, descrever e excluir modelos de execução e versões do modelo de execução. Também é possível aplicar permissões no nível do recurso a algumas ações do modelo de execução para controlar a capacidade de um usuário de usar recursos específicos nessas ações. Para obter mais informações, consulte as seguintes políticas de exemplo: Exemplo: trabalhar com modelos de execução.

Tenha cuidado ao conceder aos usuários permissões para usar as ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Não é possível usar permissões em nível de recurso para controlar quais recursos os usuários podem especificar no modelo de execução. Para restringir os recursos usados para executar uma instância, conceda permissões para criar modelos de execução e versões de modelo de execução somente a administradores apropriados.

Aspectos importantes de segurança ao usar modelos de execução com o EC2 Fleet ou o frota spot

Ao usar modelos de execução, você também deve conceder aos usuários permissões para criar, modificar, descrever e excluir modelos de execução e versões de modelo de execução. Você pode controlar quem pode criar modelos de lançamento e iniciar versões de modelos controlando o acesso às ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. . Também é possível controlar quem pode modificar os modelos de execução controlando o acesso à ação `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Se uma frota spot ou EC2 Fleet estiver configurada para usar a versão mais recente ou padrão do modelo de execução, a frota não saberá se a mais recente ou a padrão foram alteradas posteriormente para apontar para uma versão diferente do modelo de execução. Quando uma versão diferente do modelo de execução é usada para Mais recente ou Padrão, o Amazon EC2 não verifica novamente as permissões para que as ações sejam concluídas ao iniciar novas instâncias para atender à capacidade desejada da frota. Essa é uma consideração importante ao conceder permissões a quem pode criar e gerenciar versões do modelo de execução, especialmente a ação `ec2:ModifyLaunchTemplate`, que permite ao usuário alterar a versão Padrão do modelo de execução.

Ao conceder permissão ao usuário para usar as ações do EC2 para as APIs do modelo de execução, o usuário também recebe efetivamente a permissão `iam:PassRole` se criar ou atualizar uma frota spot ou EC2 Fleet para apontar para uma versão diferente do modelo de execução que contenha um perfil de instância (um contêiner para um perfil do IAM). Isso significa que um usuário pode atualizar um modelo de execução para transferir um perfil do IAM para uma instância, mesmo que não tenha a permissão `iam:PassRole`. Para obter mais informações e um exemplo de política do IAM, consulte Uso de um perfil do IAM para conceder permissões a aplicações em execução em instâncias do Amazon EC2 no Guia do usuário do IAM.

Para ter mais informações, consulte Controlar o uso dos modelos de execução e Exemplo: trabalhar com modelos de execução.

Criar um modelo de inicialização

Crie um modelo de execução usando os parâmetros definidos por você ou use um modelo de execução ou uma instância existente como base para a criação de um novo modelo de execução.

Tarefas

- Criar um modelo de execução usando parâmetros
- Criar um modelo de execução a partir de um modelo de execução existente
- Criar um modelo de execução a partir de uma instância
- Use um parâmetro de Systems Manager em vez de um ID de AMI

Criar um modelo de execução usando parâmetros

Para criar um modelo de execução, especifique o nome do modelo de execução e, pelo menos, um parâmetro de configuração de instância.

Instruções para o console

Como criar um modelo de execução usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Os parâmetros do modelo de execução são agrupados. Para obter detalhes sobre cada grupo, consulte as seções apresentadas abaixo.
4. Use o painel Resumo para analisar a configuração do modelo de execução. É possível navegar para qualquer seção ao escolher um link e, em seguida, realizar as alterações necessárias.
5. Quando você estiver pronto para criar seu modelo de execução, escolha Create launch template (Criar modelo de execução).

Nome, descrição e etiquetas do modelo de execução

1. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
2. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
3. Para marcar o modelo de execução na criação, expanda Template tags (Etiquetas do modelo), escolha Add Tag (Adicionar etiqueta) e insira um par de chave e valor de etiqueta. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

> **Note**
>
> Para marcar os recursos que são criados quando uma instância é executada, você deve especificar as etiquetas em Resource tags (Etiquetas de recursos). Para ter mais informações, consulte Tags de recursos.

Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon)

Uma imagem de máquina da Amazon (AMI) contém as informações necessárias para criar uma instância. Por exemplo, uma AMI pode conter o software que é necessário para atuar como um servidor Web, como o Linux, o Apache e seu site.

É possível encontrar uma AMI adequada da seguinte forma: Com cada opção para encontrar uma AMI, escolha Cancel (Cancelar) (no canto superior direito) para retornar ao modelo de execução sem escolher uma AMI.

Barra de pesquisa

Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa de AMI e pressione Enter. Escolha Select para selecionar uma AMI.

Recents (Recentes)

As AMIs que você usou recentemente.

Escolha Recently launched (Iniciadas recentemente) ou Currently in use (Atualmente em uso) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Minhas AMIs

As AMIs privadas que você possui, ou as AMI privadas que foram compartilhadas com você.

Escolha Owned by me (De minha propriedade) ou Shared with me (Compartilhado comigo) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Início rápido

As AMIs são agrupadas por sistema operacional (SO) para ajudá-lo a começar rapidamente.

Em primeiro lugar, selecione o sistema operacional de que precisa e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI. Para selecionar uma AMI qualificada para o nível gratuito, confira se a AMI está marcada como Free tier eligible (Qualificada para o nível gratuito).

Browse more AMIs (Procurar mais AMIs)

Selecione Browse more AMIs (Procurar mais AMIs) para navegar pelo catálogo completo de AMIs.

- Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa e pressione Enter.
- Para encontrar uma AMI usando um parâmetro do Systems Manager, escolha o botão de seta à direita da barra de pesquisa e escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager). Para ter mais informações, consulte Encontrar uma AMI usando um parâmetro do Systems Manager.
- Para especificar um parâmetro do Systems Manager que será resolvido para uma AMI no momento em que uma instância for iniciada usando o modelo de inicialização, escolha o botão de seta à direita da barra de pesquisa e escolha Especificar valor personalizado/parâmetro do Systems Manager. Para ter mais informações, consulte Use um parâmetro de Systems Manager em vez de um ID de AMI.
- Para pesquisar por categoria, escolha Quickstart AMIs (AMIS de início rápido), My AMIs (Minhas AMIs), AWS Marketplace AMIs ou Community AMIs (AMIs da comunidade).

  O AWS Marketplace é uma loja online onde é possível comprar software executado na AWS, inclusive AMIs. Para obter mais informações sobre como executar uma instância pelo AWS Marketplace, consulte Executar uma instância AWS Marketplace. Em Community AMIs (AMIs da comunidade), é possível encontrar AMIs que membros da comunidade AWS disponibilizaram para outras pessoas usarem. AMIs da Amazon ou de um parceiro verificado estão marcadas como Provedor verificado.
- Para filtrar a lista de AMIs, marque uma ou mais caixas de seleção em Refine results (Refinar resultados) do lado esquerdo da tela. As opções de filtro são diferentes dependendo da categoria de pesquisa selecionada.
- Verifique Root device type (Tipo de dispositivo raiz) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: ebs (baseadas no Amazon EBS) ou instance-store (baseadas no armazenamento de instâncias). Para ter mais informações, consulte Armazenamento para o dispositivo raiz.
- Verifique o Virtualization type (Tipo de virtualização) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: hvm ou paravirtual. Por exemplo, alguns tipos de instância exigem HVM. Para ter mais informações, consulte Tipos de virtualização de AMI.
- Verifique o modo de inicialização listado para cada AMI. Observe quais AMIs usam o modo de inicialização de que você precisa: legacy-bios, uefi ou uefi-preferred. Para ter mais informações, consulte Modos de inicialização do Amazon EC2.
- Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).

Tipo de instância

O tipo de instância define a configuração do hardware e o tamanho da instância. Os tipos de instâncias maiores têm mais CPU e memória. Para obter mais informações, consulte Tipos de instância do Amazon EC2.

Para Instance type (Tipo de instância), é possível selecionar um tipo de instância ou especificar atributos de instância e deixar o Amazon EC2 identificar os tipos de instância com esses atributos.

> **Note**
>
> Há suporte à especificação de atributos de instância somente com o uso de grupos do Auto Scaling, frota do EC2 e frota spot para iniciar instâncias. Para obter mais informações, consulte Criar um grupo do Auto Scaling usando a seleção de tipo de instância baseada em atributo, Seleção de tipo de instância baseada em atributos para frota do EC2 e Seleção de tipo de instância baseada em atributos para frota spot.
> Se você planeja usar o modelo de execução no assistente de execução de instância ou com a API RunInstances, deve selecionar um tipo de instância.

- Instance type (Tipo de instância): verifique se o tipo de instância é compatível com a AMI especificada. Para ter mais informações, consulte Tipos de instância do Amazon EC2.
- Compare instance types (Comparar tipos de instâncias): é possível comparar diferentes tipos de instâncias pelos seguintes atributos: número de vCPUs, arquitetura, quantidade de memória (GiB), quantidade de armazenamento (GB), tipo de armazenamento e performance de rede.
- Obter conselho: você pode obter orientações e sugestões de tipos de instância no seletor de tipo de instância do EC2 Amazon Q. Para ter mais informações, consulte Obter recomendações de tipo de instância para uma nova workload.
- Advanced (Avançado): para especificar atributos de instância e deixar o Amazon EC2 identificar os tipos de instância com esses atributos, selecione Advanced (Avançado) e, depois, escolha Specify instance type attributes (Especificar atributos de tipo de instância).
  - Number of vCPUs (Número de vCPUs): insira o número mínimo e máximo de vCPUs para seus requisitos de computação. Para indicar que não há limites, insira um mínimo de **0** e deixe o máximo em branco.
  - Amount of memory (MiB) (Quantidade de memória: Insira a quantidade mínima e máxima de memória, em MiB, para seus requisitos de computação. Para indicar que não há limites, insira um mínimo de **0** e deixe o máximo em branco.

- Expanda Optional instance type attributes (Atributos opcionais de tipo de instância) e selecione Add attribute (Adicionar atributo) para expressar seus requisitos de computação com mais detalhes. Para obter informações sobre cada atributo, consulte InstanceRequirementsRequest na Referência de API do Amazon EC2.
- Resulting instance types (Tipos de instância resultantes): é possível previsualizar os tipos de instância que correspondam aos atributos especificados. Para excluir tipos de instância, escolha Add attribute (Adicionar atributo) e, na lista Attribute (Atributo), escolha Excluded instance types (Tipos de instância excluídos). Na lista Attribute value (Valor do atributo), selecione os tipos de instância a serem excluídos.

Par de chaves (login)

O par de chaves para a instância.

Em Key pair name (Nome do par de chaves), escolha um par de chaves existente ou escolha Create new key pair (Criar um novo par de chaves) para criar um novo. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

Configurações de rede

Defina as configurações de rede, conforme necessário.

- Subnet (Sub-rede): é possível executar uma instância em uma sub-rede associada a uma zona de disponibilidade, a uma zona local, a uma zona Wavelength ou a um Outpost.

  Para iniciar a instância em uma zona de disponibilidade, selecione a sub-rede na qual a instância será iniciada. Para criar uma nova sub-rede, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Quando tiver concluído, retorne ao assistente e escolha o ícone Refresh (Atualizar) para carregar sua sub-rede na lista.

  Para iniciar a instância em uma zona local, selecione uma sub-rede que você criou na zona local.

  Para iniciar uma instância em um Outpost, selecione uma sub-rede em uma VPC associada ao Outpost.
- Firewall (security groups) (Firewall, grupos de segurança): use um ou mais grupos de segurança para definir as regras de firewall da sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. Para obter mais informações sobre grupos de segurança, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.

Se você adicionar uma interface de rede, deverá especificar os mesmos grupos de segurança na interface de rede.

Selecione ou crie um grupo de segurança da seguinte forma:

- Para selecionar um grupo de segurança existente, escolha Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança em Common security groups (Grupos de segurança comuns).
- Para criar um novo grupo de segurança, escolha Create a new security group (Criar um novo grupo de segurança).

  É possível adicionar regras de acordo com suas necessidades. Por exemplo, se a instância for um servidor Web, abra as portas 80 (HTTP) e 443 (HTTPS) para permitir tráfego da Internet.

  Para adicionar uma regra, escolha Add security group rule (Adicionar regra do grupo de segurança). Em Type (Tipo), selecione o tipo de tráfego da rede. O campo Protocol (Protocolo) é preenchido automaticamente com o protocolo para abrir para o tráfego de rede. Em Source type (Tipo de origem), escolha o tipo da origem. Para deixar o modelo de execução adicionar o endereço IP público do seu computador, escolha My IP (Meu IP). No entanto, se você estiver se conectando por meio de um ISP ou por trás de um firewall sem um endereço IP estático, precisará encontrar o intervalo de endereços IP usado pelos computadores clientes.

  > ⚠ Warning
  >
  > Regras que habilitam todos os endereços IP (`0.0.0.0/0`) a acessar a instância por SSH ou RDP são aceitáveis se você for iniciar, por pouco tempo, uma instância de teste e interrompê-la ou terminá-la em breve, mas não são segurar para ambientes de produção. É necessário autorizar apenas um endereço IP específico ou um intervalo de endereços a acessar a instância.

- Configuração de rede avançada

  Interface de rede

  - Device index (Índice do dispositivo): o número do dispositivo da interface de rede, por exemplo, `eth0` para a interface de rede principal. Se você deixar o campo em branco, a AWS criará a interface de rede principal.

- Network Interface (Interface de rede): selecione New interface (Nova interface), para deixar o Amazon EC2 criar uma interface nova, ou selecione uma interface de rede existente que esteja disponível.
- Description (Descrição): (opcional) uma descrição da nova interface de rede.
- Subnet (Sub-rede): a sub-rede na qual criar a nova interface de rede. Para a interface de rede principal (`eth0`), essa é a sub-rede na qual a instância será executada. Se você tiver inserido uma interface de rede existente para `eth0`, a instância será executada na sub-rede na qual a interface de rede está localizada.
- Grupos de segurança: um ou mais grupos de segurança na VPC aos quais associar a interface de rede.
- Auto-assign Public IP (Autoatribuir IP público): especifique se sua instância recebe um endereço IPv4 público. Por padrão, as instâncias em uma sub-rede padrão recebem um endereço IPv4 público e as instâncias em uma sub-rede não padrão, não. Selecione Enable (Habilitar) ou Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Para ter mais informações, consulte Endereços IPv4 públicos.
- Primary IP (IP principal): um endereço IPv4 privado no intervalo de sua sub-rede. Deixe em branco para que o Amazon EC2 escolha um endereço IPv4 privado para você.
- IP secundário: um ou mais endereços IPv4 privados adicionais do intervalo de endereços da sua sub-rede. Escolha Manually assign (Atribuir manualmente) e insira um endereço IP. Escolha Add IP (Adicionar IP) para adicionar outro endereço IP. Ou escolha Automatically assign (Atribuir automaticamente), para deixar que o Amazon EC2 escolha um para você, e insira um valor para indicar o número de endereços IP a serem adicionados.
- (Somente para IPv6) IPv6 IPs (IPs IPv6): um endereço IPv6 no intervalo da sub-rede. Escolha Manually assign (Atribuir manualmente) e insira um endereço IP. Escolha Add IP (Adicionar IP) para adicionar outro endereço IP. Ou escolha Automatically assign (Atribuir automaticamente), para deixar que o Amazon EC2 escolha um para você, e insira um valor para indicar o número de endereços IP a serem adicionados.
- IPv4 Prefixes (Prefixos IPv4): os prefixos IPv4 para a interface de rede.
- IPv6 Prefixes (Prefixos IPv6): os prefixos IPv6 para a interface de rede.
- (Opcional) Atribuir IP IPv6 primário: se você estiver iniciando uma instância em uma sub-rede de pilha dupla ou somente IPv6, terá a opção de Atribuir IP IPv6 primário. A atribuição de um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Escolha Habilitar se essa instância depender do seu endereço IPv6 permanecer inalterado. Quando a instância é executada, a AWS atribuirá automaticamente um endereço IPv6 associado

à ENI anexada à sua instância como o endereço IPv6 principal. Após habilitar um endereço GUA IPv6 para ser um IPv6 primário, não será possível desabilitá-lo. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se tornará o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada. Se você tiver vários endereços IPv6 associados a uma ENI anexada à sua instância e habilitar um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à ENI se tornará o endereço IPv6 primário.

- Delete on termination (Excluir no encerramento): se a interface de rede deve ser excluída quando a instância for excluída.
- Elastic Fabric Adapter: indica se a interface de rede é um Elastic Fabric Adapter. Para ter mais informações, consulte the section called “Elastic Fabric Adapter”.
- Índice da placa de rede: O índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância suportam várias placas de rede.
- ENA Express: o ENA Express tem a tecnologia Scalable Reliable Datagram (SRD) da AWS. A tecnologia SRD usa um mecanismo de pulverização de pacotes para distribuir carga e evitar congestionamento de rede. A ativação do ENA Express permite que as instâncias compatíveis se comuniquem usando SRD além do tráfego TCP normal, quando possível. O modelo de inicialização de instância não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar.
- UDP do ENA Express: se habilitou o ENA Express, tem a opção de usá-lo para tráfego UDP. O modelo de inicialização de instância não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar.

Escolha Add network interface (Adicionar interface de rede) para adicionar mais interfaces de rede. O número de interfaces de rede que é possível adicionar depende do número que é aceito pelo tipo de instância selecionado. Outras interfaces de rede podem residir em uma sub-rede diferente da mesma VPC ou em uma sub-rede em outra VPC que você possua (desde que a sub-rede esteja na mesma zona de disponibilidade da sua instância). Se você selecionar uma sub-rede em outra VPC, o rótulo Multi-VPC aparecerá ao lado da interface de rede que você adicionou. Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança. Observe que, se anexar uma ENI adicional de outra VPC, você deverá escolher um grupo de segurança para a ENI dessa VPC.

Para ter mais informações, consulte Interfaces de rede elástica. Se você especificar mais de uma interface de rede, sua instância não poderá receber um endereço IPv4 público. Além disso, se você especificar uma interface de rede existente para eth0, não poderá substituir a configuração

de IPv4 pública da sub-rede usando Auto-assign Public IP (Atribuir IP público automaticamente). Para ter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância.

Configurar armazenamento

Se você especificar uma AMI para o modelo de execução, a AMI incluirá um ou mais volumes de armazenamento, incluindo o volume raiz (Volume 1 [Raiz da AMI]). É possível especificar volumes adicionais a serem anexados à instância.

É possível usar a exibição Simple (Simples) ou Advanced (Avançada). Com a exibição Simple (Simples), você especifica o tamanho e o tipo de volume. Para especificar todos os parâmetros de volume, use a exibição Advanced (Avançada), no canto superior direito do cartão.

Para adicionar um novo volume, escolha Add new volume (Adicionar novo volume).

Usando a exibição Advanced (Avançada), é possível configurar cada volume da seguinte forma:

- Storage type (Tipo de armazenamento): o tipo de volume (EBS ou temporário) a ser associado à instância. O tipo de volume de armazenamento de instância (temporário) só estará disponível se você selecionar um tipo de instância compatível com ele. Para obter mais informações, consulte Armazenamento de instâncias do Amazon EC2 e Volumes do Amazon EBS.
- Device Name (Nome do dispositivo): selecione na lista de nomes de dispositivo disponíveis para o volume.
- Snapshot: selecione o snapshot do qual o volume será criado. Também é possível pesquisar snapshots públicos e compartilhados que estão disponíveis, inserindo texto no campo Snapshot.
- Size (GiB) (Tamanho): para volumes do EBS, especifique um tamanho de armazenamento. Se você tiver selecionado uma AMI e uma instância que estejam qualificadas para o nível gratuito, tenha em mente que para permanecer no nível gratuito, seu armazenamento total deverá ficar abaixo de 30 GiB.
- Volume Type (Tipo de volume): para volumes do EBS, selecione um tipo de volume. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.
- IOPS: se você tiver selecionado um SSD de IOPS provisionadas (`io1` e `io2`) ou um tipo de volume de SSD de uso geral (`gp3`), poderá inserir o número de operações de E/S por segundo (IOPS) com o qual o volume seja compatível. Isso é necessário para volumes io1, io2 e gp3. Isso não é compatível com volumes gp2, st1, sc1 ou volumes padrão. Se omitir esse parâmetro para

o modelo de execução, você deverá especificar um valor para ele ao executar uma instância com base no modelo de execução.

- Delete on termination (Excluir ao término): em volumes do Amazon EBS, escolha Yes (Sim), para excluir o volume quando a instância associada for terminada, ou escolha No (Não) para manter o volume. Para ter mais informações, consulte Preservação de dados quando uma instância for encerrada.
- Encrypted: (Criptografado): se o tipo de instância oferecer suporte à criptografia do EBS, será possível escolher Yes (Sim) para habilitar criptografia para o volume. Se você tiver habilitado a criptografia por padrão nessa região, a criptografia estará habilitada para você. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.
- KMS Key (Chave do KMS): se você selecionou Yes (Sim) para Encrypted (Criptografado), deve selecionar uma chave gerenciada pelo cliente a ser usada para criptografar o volume. Se tiver habilitado a criptografia por padrão nessa região, a chave gerenciada pelo cliente padrão será selecionada para você. É possível selecionar uma chave diferente ou especificar o ARN de qualquer chave gerenciada pelo cliente que você tenha criado.

Tags de recursos

Para marcar os recursos que são criados quando uma instância é executada, em Resource tags (Etiquetas de recursos), escolha Add tag (Adicionar etiqueta) e, em seguida, insira um par de chave e valor de etiqueta. Em Resource types (Tipos de recursos), especifique os recursos para marcar na criação. É possível especificar a mesma etiqueta para todos os recursos ou especificar etiquetas diferentes para recursos diferentes. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

É possível especificar etiquetas tags para os seguintes recursos que são criados quando um modelo de inicialização é usado:

- Instâncias
- Volumes
- Solicitações de instância Spot
- Interfaces de rede

> **Note**
>
> Para marcar o modelo de execução em si, é necessário especificar as tags em Template tags (Etiquetas de modelo). Para ter mais informações, consulte Nome, descrição e etiquetas do modelo de execução.

Detalhes avançados

Em Advanced details (Detalhes avançados), expanda a seção para visualizar os campos e especifique quaisquer parâmetros adicionais para a instância.

- Purchasing option (Opção de compra): escolha Request Spot Instances (Solicitar instâncias spot) para solicitar instâncias spot pelo preço spot, limitado ao preço sob demanda, e escolha Customize(Personalizar) para alterar as configurações padrão da instância spot. É possível definir o preço máximo (não recomendado) e alterar o tipo de solicitação, a duração da solicitação e o comportamento de interrupção. Se você não solicitar uma instância spot, o EC2 executará uma instância sob demanda por padrão. Para ter mais informações, consulte Instâncias spot.
- IAM instance profile (Perfil da instância do IAM): um perfil de instância do AWS Identity and Access Management (IAM) a ser associado à instância. Para ter mais informações, consulte Funções do IAM para Amazon EC2.
- Hostname type (Tipo de nome do host): selecione se o nome do host do sistema operacional convidado da instância incluirá o nome do recurso ou o nome do IP. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.
- Hostname DNS (Nome de host DNS): determina se as consultas de DNS para o nome do recurso ou nome do IP (de acordo com o que você selecionou em Hostname type [Tipo de nome do host]) serão respondidas com o endereço IPv4 (registro A), o endereço IPv6 (registro AAAA) ou ambos. Para ter mais informações, consulte Tipos de nome de host de instância do Amazon EC2.
- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.
- Stop - Hibernate behavior (Comportamento Parar - Hibernar): para habilitar a hibernação, escolha Enable (Habilitar). Esse campo só é válido para instâncias que atendem aos pré-requisitos de hibernação. Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.
- Termination protection (Proteção contra término): para evitar o término acidental, escolha Enable (Habilitar). Para ter mais informações, consulte Habilitar a proteção contra encerramento.

- Stop protection (Proteção contra interrupção): para prevenir interrupções acidentais, escolha Enable (Habilitar). Para ter mais informações, consulte Habilitar a proteção contra interrupção.
- Detailed CloudWatch monitoring: (Monitoramento detalhado do CloudWatch): escolha Enable (Habilitar) para habilitar o monitoramento detalhado da instância usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para ter mais informações, consulte Monitorar instâncias usando o CloudWatch.
- Elastic GPU: o Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.
- Elastic inference (Inferência elástica): uma aceleradora de inferência elástica a ser anexada à instância de CPU do EC2. Para obter mais informações, consulte Trabalhando com o Amazon Elastic Inference no Guia do desenvolvedor do Amazon Elastic Inference.

  > **Note**
  >
  > A partir de 15 de abril de 2023, a AWS não integrará novos clientes ao Amazon Elastic Inference (EI) e ajudará os clientes atuais a migrar suas workloads para opções que ofereçam melhores preço e desempenho. Depois de 15 de abril de 2023, os novos clientes não poderão executar instâncias com aceleradores Amazon EI no Amazon SageMaker, Amazon ECS ou Amazon EC2. No entanto, os clientes que tenham usado o Amazon EI pelo menos uma vez durante os últimos 30 dias serão considerados clientes atuais e poderão continuar usando o serviço.

- Credit specification (Especificação de crédito): escolha Unlimited (Ilimitado) para permitir que as aplicações ultrapassem linha de base pelo tempo que for necessário. Esse campo só é válido para instâncias T. Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Instâncias expansíveis.
- Placement group name (Nome do grupo de posicionamento): especifique um grupo de posicionamento no qual a instância será executada. É possível selecionar um grupo de posicionamento existente ou crie um novo. Nem todos os tipos de instância podem ser executados em um grupo de posicionamento. Para ter mais informações, consulte Grupos de posicionamento.
- EBS-optimized instance (Instância otimizada para EBS): selecione Enable (Habilitar) para fornecer capacidade dedicada adicional para E/S do Amazon EBS. Nem todos os tipos de instância são compatíveis com esse recurso. Aplicam-se cobranças adicionais. Para ter mais informações, consulte the section called “Otimização de EBS”.

- Capacity Reservation (Reserva de capacidade): especifique se deseja iniciar a instância em qualquer reserva de capacidade aberta (Open, Aberta), uma reserva de capacidade específica (Target by ID, Alvo por ID) ou um grupo de reservas de capacidade (Target by group, Alvo por grupo). Para especificar que nenhuma reserva de capacidade deva ser usada, escolha None (Nenhuma). Para ter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.
- Tenancy (Locação): escolha se a instância deve ser executada em hardware compartilhado (Shared (Compartilhado)), isolado, hardware dedicado (Dedicated (Dedicado)) ou em um Host dedicado (Dedicated host (Host dedicado)). Se você optar por executar a instância em um Host dedicado, poderá especificar se deseja executar a instância em um grupo de recursos de host ou poderá segmentar um Host dedicado específico. Podem se aplicar cobranças adicionais. Para ter mais informações, consulte Dedicated Instances e Dedicated Hosts.
- RAM disk ID (ID do disco de RAM): (válido somente para AMIs paravirtuais, PV) selecione um disco de RAM para a instância. Se você tiver selecionado um kernel, pode precisar selecionar um disco de RAM específico com os drivers para oferecer suporte a ele.
- Kernel ID (ID do kernel): (válido somente para AMIs paravirtuais, PV) selecione um kernel para a instância.
- Nitro Enclave: permite criar ambientes isolados de execução, chamados de enclaves, com base em instâncias do Amazon EC2. Selecione Enable (Habilitar) para habilitar a instância para o AWS Nitro Enclaves. Para obter mais informações, consulte O que é o AWS Nitro Enclaves? no Guia do usuário do AWS Nitro Enclaves.
- Configurações de licenças: é possível executar instâncias com relação à configuração de licença especificada para rastrear o uso da licença. Para obter mais informações, consulte Crie uma configuração de licença no Guia do usuário do AWS License Manager.
- Specify CPU options (Especificar opções de CPU): escolha Specify CPU options (Especificar opções de CPU) para especificar um número personalizado de vCPUs durante a execução. Defina o número de núcleos de CPU e de threads por núcleo. Para ter mais informações, consulte Otimizar as opções de CPU.
- Endpoint IPv6 de metadados: você pode habilitar a instância para usar o endereço IPv6 do IMDS `[fd00:ec2::254]` para recuperar os metadados da instância. Essa opção só estará disponível se você for iniciar instâncias baseadas no AWS Nitro System em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas). Para ter mais informações, consulte Recuperar metadados da instância.
- Metadados acessíveis: é possível habilitar ou desabilitar o acesso ao IMDS. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.

- Versão de metadados: se você habilitar o acesso ao IMDS, poderá optar por exigir o uso do Serviço de metadados de instância versão 2 ao solicitar metadados da instância. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Limite de salto de resposta de metadados: se você habilitar o IMDS, poderá definir o número permitido de saltos de rede para o token de metadados. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Allow tags in metadata (Permitir tags em metadados): se você selecionar Enable (Habilitar), a instância permitirá o acesso a todas as tags da instância dos metadados. Se você não incluir essa configuração no modelo, por padrão, o acesso às etiquetas nos metadados da instância não será permitido. Para ter mais informações, consulte Permitir acesso a tags em metadados de instância.
- User data (Dados do usuário): é possível especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para ter mais informações, consulte Execução de comandos na instância do Amazon EC2 na inicialização.

Exemplo de AWS CLI

O exemplo apresentado a seguir usa o comando create-launch-template para criar um modelo de execução com o nome e a configuração da instância especificados.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo em JSON que especifica os dados do modelo de execução para a configuração da instância. Salve o formato JSON em um arquivo e inclua-o no parâmetro `--launch-template-data`, conforme mostrado no comando de exemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
```

```
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

O seguinte é um exemplo de saída.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

Exemplo de AWS Tools for Windows PowerShell

O exemplo apresentado a seguir usa o cmdlet New-EC2LaunchTemplate para criar um modelo de execução com o nome e a configuração da instância especificados.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-8c1be5f6'
    InstanceType = 'r4.4xlarge'
    NetworkInterfaces = @(
        [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-7b16de0c'
        }
```

```
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
 'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
 $tagSpecificationData
```

O seguinte é um exemplo de saída.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Criar um modelo de execução a partir de um modelo de execução existente

É possível clonar um modelo de inicialização existente e ajustar os parâmetros para criar um novo modelo de inicialização. No entanto, você só pode fazer isso ao usar o console do Amazon EC2; oAWS CLI não suporta a clonagem de um modelo.

Console

Para criar um modelo de inicialização a partir de um modelo de inicialização existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
5. Para marcar o modelo de execução na criação, expanda Template tags (Tags modelo), escolha Add Tag (Adicionar tag) e insira um par de chave e valor de tag.
6. Expanda o Modelo de origem e, em Nome do modelo de execução, escolha um modelo de execução no qual o novo modelo de execução se baseará.
7. Em Source template version (Versão do modelo de origem), escolha a versão do modelo de execução no qual o novo modelo de execução se baseará.
8. Ajuste todos os parâmetros de execução quando necessário e escolha Create launch template (Criar modelo de execução).

Criar um modelo de execução a partir de uma instância

Console

Para criar um modelo de inicialização a partir de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Create template from instance (Criar modelo a partir da instância).
4. Forneça um nome, uma descrição e tags e ajuste os parâmetros de execução conforme necessário.

> **Note**
>
> Quando você cria um modelo de execução de uma instância, os IDs da interface de rede da instância e os endereços IP não são incluídos no modelo.

5. Escolha Create launch template (Criar modelo de execução).

AWS CLI

É possível usar a AWS CLI para criar um modelo de execução de uma instância existente ao obter os dados do modelo de execução primeiro e depois criar um modelo de execução usando os dados dele.

Para obter dados de modelo de inicialização de uma instância

- Use o comando get-launch-template-data e especifique o ID da instância. É possível usar o resultado como base para criar um novo modelo de execução ou uma versão de modelo de execução. Por padrão, o resultado inclui um objeto `LaunchTemplateData` de nível superior, que não pode ser especificado nos dados do modelo de execução. Use a opção `--query` para excluir este objeto.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

A seguir está um exemplo de saída.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
```

```
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```

É possível gravar o resultado diretamente em um arquivo, por exemplo:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Para criar um modelo de execução usando dados do modelo de execução

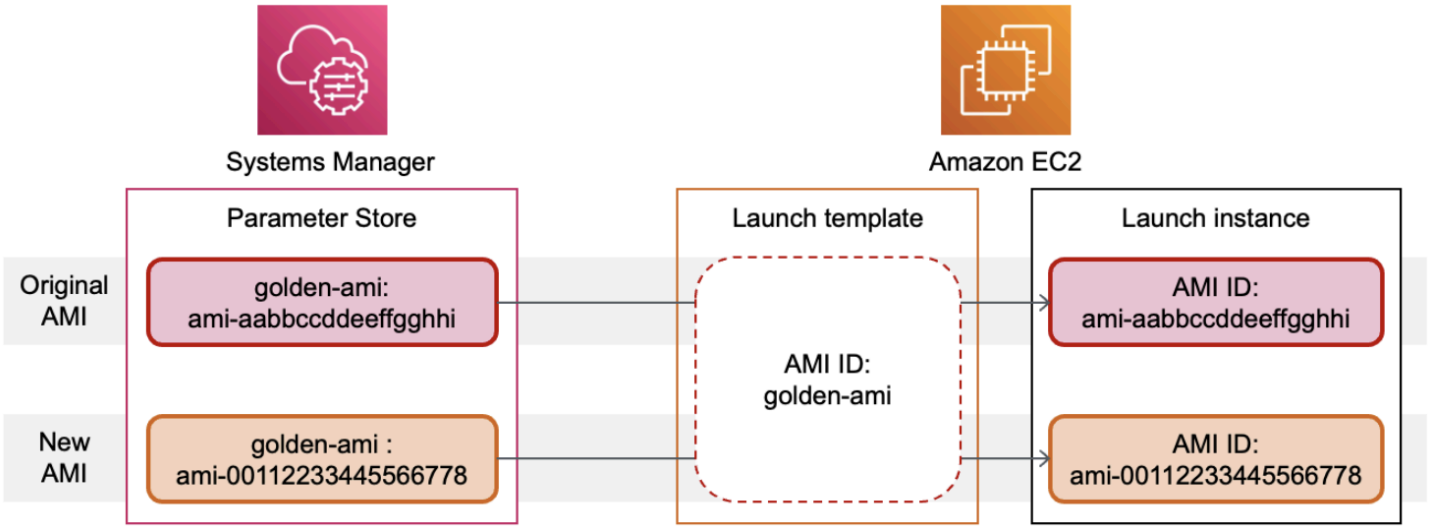
- Use o comando create-launch-template para criar um modelo de execução usando a saída do procedimento anterior. Para obter mais informações sobre como criar um modelo de execução usando a AWS CLI, consulte Criar um modelo de execução usando parâmetros.

Use um parâmetro de Systems Manager em vez de um ID de AMI

Em vez de especificar um ID de AMI em seus modelos de inicialização, você pode especificar um parâmetro AWS Systems Manager. Se o ID da AMI for alterado, você poderá atualizar o ID da AMI em um único lugar atualizando o parâmetro Systems Manager no Systems Manager Parameter Store. Os parâmetros também podem ser compartilhados com outras Contas da AWS. É possível armazenar e gerenciar os parâmetros da AMI de forma centralizada em uma conta e compartilhá-los com todas as outras contas que precisam referenciá-los. Usando um parâmetro do Systems Manager, todos os seus modelos de inicialização podem ser atualizados em uma única ação.

Um parâmetro do Systems Manager é um par chave-valor definido pelo usuário que pode ser criado no Systems Manager Parameter Store. O Parameter Store fornece um lugar central para armazenar os valores de configuração da aplicação. Para obter mais informações, consulte o Armazenamento de parâmetros do AWS Systems Manager, no Guia do usuário do AWS Systems Manager.

No diagrama a seguir, o parâmetro `golden-ami` é mapeado primeiro para a AMI original `ami-aabbccddeeffgghhi` no Parameter Store. No modelo de inicialização, o valor do ID da AMI é `golden-ami`. Quando uma instância é iniciada usando esse modelo de inicialização, o ID da AMI é resolvido para `ami-aabbccddeeffgghhi`. Posteriormente, a AMI é atualizada, resultando em um novo ID de AMI. No Parameter Store, o parâmetro `golden-ami` é mapeado para o novo `ami-00112233445566778`. O modelo de inicialização permanece inalterado. Quando uma instância é iniciada usando esse modelo de inicialização, o ID de AMI é resolvido para `ami-00112233445566778`.



Formato de parâmetros do Systems Manager para IDs de AMI

Os modelos de inicialização exigem que os parâmetros do Systems Manager definidos pelo usuário sigam o seguinte formato quando usados no lugar de um ID de AMI:

- Tipo de parâmetro: `String`
- Tipo de dados do parâmetro: `aws:ec2:image`; garante que o Parameter Store valide que o valor inserido está no formato adequado para um ID de AMI.

Para obter mais informações sobre como criar um parâmetro válido para um ID de AMI, consulte Crie um parâmetro do Systems Manager no Guia do usuário do AWS Systems Manager.

Formato de parâmetros do Systems Manager em modelos de inicialização

Para usar um parâmetro do Systems Manager no lugar de um ID de AMI em um modelo de inicialização, você deve usar um dos seguintes formatos ao especificar o parâmetro no modelo de inicialização:

Para fazer referência a um parâmetro público:

- `resolve:ssm:`*`public-parameter`*

Para fazer referência a um parâmetro armazenado na mesma conta:

- `resolve:ssm:`*`parameter-name`*
- `resolve:ssm:`*`parameter-name`*`:`*`version-number`*: o número da versão em si é um rótulo padrão
- `resolve:ssm:`*`parameter-name`*`:`*`label`*

Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

- `resolve:ssm:`*`parameter-ARN`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`version-number`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`label`*

Versões de parâmetros

Os parâmetros do Systems Manager são recursos versionados. Ao atualizar um parâmetro, você cria novas versões sucessivas do parâmetro. O Systems Manager é compatível com rótulos de parâmetros que você pode mapear para versões específicas de um parâmetro.

Por exemplo, o parâmetro `golden-ami` pode ter três versões: `1`, `2` e `3`. Você pode criar um rótulo de parâmetro `beta` que é mapeado para a versão `2` e um rótulo de parâmetro `prod` que é mapeado para a versão `3`.

Em um modelo de inicialização, você pode especificar a versão 3 do parâmetro `golden-ami` usando um dos seguintes formatos:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Especificar a versão ou o rótulo é opcional. Por padrão, a versão mais recente do parâmetro é usada quando nenhuma versão é especificada.

Especificar um parâmetro do Systems Manager em um modelo de inicialização

Você pode especificar um parâmetro do Systems Manager em um modelo de inicialização em vez de um ID de AMI ao criar um modelo de inicialização ou uma nova versão de um modelo de inicialização.

Console

Para especificar um parâmetro do Systems Manager em um modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha Browse more AMIs (Procurar mais AMIs).
5. Escolha o botão de seta à direita da barra de pesquisa e escolha Especificar valor personalizado/parâmetro do Systems Manager.

6. Na caixa de diálogo Especificar valor personalizado ou parâmetro do Systems Manager, faça o seguinte:

   a. Em ID de AMI ou string de parâmetros do Systems Manager, insira o nome do parâmetro do Systems Manager usando um destes formatos:

      Para fazer referência a um parâmetro público:

      - **resolve:ssm:*public-parameter***

      Para fazer referência a um parâmetro armazenado na mesma conta:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Escolha Salvar.

7. Especifique quaisquer outros parâmetros do modelo de inicialização conforme necessário e escolha Criar modelo de inicialização.

Para ter mais informações, consulte Criar um modelo de execução usando parâmetros.

AWS CLI

Para especificar um parâmetro do Systems Manager em um modelo de inicialização

- Use o comando create-launch-template para criar o modelo de inicialização. Para especificar a AMI a ser usada, insira o nome do parâmetro do Systems Manager usando um dos seguintes formatos:

  Para fazer referência a um parâmetro público:

  - **resolve:ssm:*public-parameter***

Para fazer referência a um parâmetro armazenado na mesma conta:

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name*:*version-number***
- **resolve:ssm:*parameter-name*:*label***

Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN*:*version-number***
- **resolve:ssm:*parameter-ARN*:*label***

O exemplo a seguir cria um modelo de execução que especifica o seguinte:

- Um nome para o modelo de inicialização (*TemplateForWebServer*)
- Uma etiqueta para o modelo de execução (*purpose*=*production*)
- Os dados para a configuração da instância, especificados em um arquivo JSON:
  - A AMI a ser usada (`resolve:ssm:`*golden-ami*)
  - O tipo de instância a ser executada iniciada (*m5.4xlarge*)
  - Uma etiqueta para a instância (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo de arquivo JSON que contém os dados do modelo de execução para a configuração da instância. O valor de `ImageId` é o nome do parâmetro do Systems Manager, inserido no formato exigido `resolve:ssm:`*golden-ami*.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
```

```
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verifique se um modelo de execução obtém o ID da AMI correto

Como resolver o parâmetro do Systems Manager para o ID da AMI real

Use o comando describe-launch-template-versions e inclua o parâmetro `--resolve-alias`.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

A resposta inclui o ID da AMI para `ImageId`. Neste exemplo, quando uma instância é iniciada usando esse modelo de execução, o ID da AMI é resolvido como `ami-0ac394d6a3example`.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Recursos relacionados

Para obter mais informações sobre como trabalhar com os parâmetros do Systems Manager, consulte os materiais de referência apresentados a seguir na documentação do Systems Manager.

- Para obter informações sobre como pesquisar os parâmetros públicos da AMI com suporte para o Amazon EC2, consulte Calling AMI public parameters.
- Para obter informações sobre como compartilhar os parâmetros com outras contas da AWS ou por meio do AWS Organizations, consulte Working with shared parameters.
- Para obter informações sobre como monitorar se os parâmetros foram criados com êxito, consulte Native parameter support for Amazon Machine Image IDs.

Limitações

- Atualmente, as frotas do EC2 e as frotas spot não oferecem suporte ao uso de um modelo de execução que tenha um parâmetro do Systems Manager especificado no lugar de um ID de AMI. Para frotas do EC2 e frotas spot, se você especificar uma AMI no modelo de execução, deverá especificar o ID de AMI.
- O Amazon EC2 Auto Scaling fornece outras restrições. Para obter mais informações, consulte Use AWS Systems Manager parameters instead of AMI IDs in launch templates no Guia do usuário do Amazon EC2 Auto Scaling.

Modificar um modelo de inicialização (gerenciar versões do modelo de inicialização)

Os modelos de inicialização são imutáveis. Após criar um modelo de inicialização, você não poderá modificá-lo. Em vez disso, é possível criar uma nova versão do modelo de inicialização que inclua as alterações necessárias.

É possível criar diferentes versões de um modelo de execução, definir a versão padrão, descrever uma versão de modelo de execução e excluir versões que não são mais necessárias.

Tarefas

- Criar uma versão de modelo de execução
- Definir a versão do modelo de execução padrão
- Descrever uma versão de modelo de execução
- Excluir uma versão de modelo de execução

Criar uma versão de modelo de execução

Ao criar uma versão de modelo de execução, é possível especificar novos parâmetros de execução ou usar uma versão existente como base para a nova versão. Para obter mais informações sobre os parâmetros de execução, consulte Criar um modelo de inicialização.

Console

Para criar uma versão de modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione um modelo de execução e escolha Actions (Ações), Modify template (Create new version) (Modificar modelo (Criar versão)).
4. Em Template version description (Descrição da versão do modelo), insira uma descrição para a versão do modelo de execução.
5. (Opcional) Expanda o Source template (Modelo de origem) e selecione uma versão do modelo de execução a ser usado como base para a nova versão do modelo de execução. A nova versão de modelo de execução herdará os parâmetros de execução desta versão do modelo de execução.
6. Modifique os parâmetros de execução conforme necessário e escolha Create launch template (Criar modelo de execução).

AWS CLI

Para criar uma versão de modelo de inicialização

- Use o comando create-launch-template-version. É possível especificar uma versão de origem na qual a nova versão será baseada. A nova versão herdará os parâmetros de execução desta versão, e será possível substituí-los usando `--launch-template-data`. O exemplo a seguir cria uma nova versão com base na versão 1 do modelo de execução e especifica um ID de AMI diferente.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

Definir a versão do modelo de execução padrão

É possível definir a versão padrão do modelo de execução. Quando você executa uma instância a partir de um modelo de execução e não especifica uma versão, a instância é executada por meio dos parâmetros da versão padrão.

Console

Para definir a versão do modelo de inicialização padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Set default version (Definir versão padrão).
4. Em Template version (Versão do modelo), selecione o número da versão a ser definida como versão padrão e escolha Set as default version (Definir como versão padrão).

AWS CLI

Para definir a versão do modelo de inicialização padrão

- Use o comando modify-launch-template e especifique a versão que deseja definir como padrão.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

Descrever uma versão de modelo de execução

Usando o console, é possível visualizar todas as versões do modelo de execução selecionado ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico. Usando o AWS CLI, é possível descrever todas as versões, versões individuais ou um intervalo de versões de um modelo de execução especificado. Também é possível descrever todas as versões mais recentes ou todas as versões padrão de todos os modelos de execução da sua conta.

Console

Para descrever uma versão de modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. É possível visualizar uma versão de um modelo de lançamento específico ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico.
   - Para visualizar uma versão de um modelo de execução: selecione o modelo de execução. Na guia Versões em Versão, selecione uma versão para visualizar seus detalhes.
   - Para obter uma lista de todos os modelos de execução cuja versão mais recente corresponde a um número de versão específico: na barra de pesquisa, escolha Versão mais recente e selecione um número de versão.
   - Para obter uma lista de todos os modelos de execução cuja versão padrão corresponde a um número de versão específico: na barra de pesquisa, escolha Versão padrão e selecione um número de versão.

AWS CLI

Para descrever uma versão de modelo de inicialização

- Use o comando delete-launch-template-versions e especifique os números de versão. No exemplo a seguir, as versões *1* e *3* são especificadas.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Para descrever todas as versões mais recentes e padrão do modelo de inicialização da sua conta

- Use o comando describe-launch-template-versions e especifique `$Latest`, `$Default`, ou ambos. É necessário omitir o ID e o nome do modelo de execução na chamada. Não é possível especificar números de versão.

```
aws ec2 describe-launch-template-versions \
```

```
    --versions "$Latest,$Default"
```

Excluir uma versão de modelo de execução

Caso não precise mais de uma versão de modelo de execução, exclua-a.

Considerações

- Não é possível substituir o número de versão após excluí-lo.
- Não é possível excluir a versão padrão do modelo de execução; antes é necessário atribuir outra versão como a padrão. Se a versão padrão for a única versão para o modelo de execução, exclua todo o modelo de execução.
- No console, é possível excluir uma versão do modelo de execução por vez. Usando a AWS CLI, é possível excluir até 200 versões do modelo de execução em uma única solicitação. Para excluir mais de 200 versões em uma única solicitação, exclua o modelo de execução, o que também exclui todas as suas versões.

Console

Para excluir uma versão de modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template version (Excluir versão de modelo).
4. Selecione a versão a ser excluída e escolha Delete (Excluir).

AWS CLI

Para excluir uma versão de modelo de inicialização

- Use o comando delete-launch-template-versions e especifique os números de versão a serem excluídos. É possível especificar até 200 versões do modelo de execução para excluir em uma única solicitação.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
```

```
    --versions 1
```

Excluir um modelo de execução

Caso não precise mais de um modelo de execução, exclua-o. A exclusão de um modelo de execução excluirá todas as suas versões. Para excluir uma versão específica de um modelo de inicialização, consulte Excluir uma versão de modelo de execução.

Quando você exclui um modelo de execução, isso não afeta nenhuma instância que você iniciou a partir dele.

Console

Para excluir um modelo de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template (Excluir modelo).
4. Digite **`Delete`** para confirmar a exclusão e escolha Delete (Excluir).

AWS CLI

Para excluir um modelo de execução

Use o comando delete-launch-template (AWS CLI) e especifique o modelo de execução.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Para excluir um modelo de execução

Use o comando Remove-EC2LaunchTemplate (AWS Tools for PowerShell) e especifique o modelo de execução. Se `-Force` for omitido, o PowerShell solicitará uma confirmação.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Iniciar uma instância a partir de um modelo de inicialização

Iniciar modelos de execução é compatível com vários serviços de execução de instâncias. Este tópico descreve como usar um modelo de inicialização ao iniciar uma instância usando o assistente de inicialização de instâncias do EC2, o Amazon EC2 Auto Scaling, a Frota do EC2 e a frota spot.

Tópicos

- Executar uma instância a partir de um modelo de execução
- Usar modelos de execução com o Amazon EC2 Auto Scaling
- Usar modelos de execução com o Frota do EC2
- Usar modelos de execução com a frota spot

Executar uma instância a partir de um modelo de execução

É possível usar os parâmetros contidos em um modelo de execução para executar uma instância. É possível substituir ou adicionar parâmetros de execução antes de executar a instância.

As instâncias executadas por meio de um modelo de execução recebem automaticamente duas tags com as chaves `aws:ec2launchtemplate:id` e `aws:ec2launchtemplate:version`. Não é possível remover ou editar essas tags.

Console

Para executar uma instância a partir de um modelo de execução usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Launch instance from template (Executar instância do modelo).
4. Em Source template version (Versão do modelo de origem), selecione a versão do modelo de execução a ser usado.
5. Em Number of instances (Número de instâncias), especifique o número de instâncias a serem executadas.
6. (Opcional) É possível substituir ou adicionar parâmetros de modelo de execução alterando e adicionando parâmetros na seção Instance details (Detalhes da instância).
7. Escolha Launch instance from template (Executar instância do modelo).

AWS CLI

Como executar uma instância a partir de um modelo de execução usando a AWS CLI

- Use o comando run-instances e especifique o parâmetro `--launch-template`. Se desejar, especifique a versão de modelo de execução a ser usada. Se você não especificar a versão, a versão padrão será usada.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Para substituir um parâmetro de modelo de execução, especifique o parâmetro no comando run-instances. O exemplo a seguir substitui o tipo de instância especificado no modelo de execução (se houver algum).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Se você especificar um parâmetro aninhado que faça parte de uma estrutura complexa, a instância será executada por meio da estrutura complexa conforme especificado no modelo de execução, além de quaisquer parâmetros aninhados adicionais que você especificar.

  No exemplo a seguir, a instância é executada com a tag *Owner*=*TeamA*, bem como com quaisquer outras tags especificadas no modelo de execução. Se o modelo de execução tiver uma tag com uma chave *Owner*, o valor será substituído por *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  No exemplo a seguir, a instância é executada com um volume com o nome de dispositivo */dev/xvdb*, bem como com quaisquer outros mapeamentos de dispositivos de blocos especificados no modelo de execução. Se o modelo de execução tiver um volume existente definido para */dev/xvdb*, seus valores serão substituídos pelos valores especificados.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

PowerShell

Como executar uma instância a partir de um modelo de execução usando a AWS Tools for PowerShell

- Use o comando New-EC2Instance e especifique o parâmetro `-LaunchTemplate`. Se desejar, especifique a versão de modelo de execução a ser usada. Se você não especificar a versão, a versão padrão será usada.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Para substituir um parâmetro de modelo de execução, especifique o parâmetro no comando New-EC2Instance. O exemplo a seguir substitui o tipo de instância especificado no modelo de execução (se houver algum).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Se você especificar um parâmetro aninhado que faça parte de uma estrutura complexa, a instância será executada por meio da estrutura complexa conforme especificado no modelo de execução, além de quaisquer parâmetros aninhados adicionais que você especificar.

No exemplo a seguir, a instância é executada com a tag *Owner*=*TeamA*, bem como com quaisquer outras tags especificadas no modelo de execução. Se o modelo de execução tiver uma tag com uma chave *Owner*, o valor será substituído por *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

No exemplo a seguir, a instância é executada com um volume com o nome de dispositivo */dev/xvdb*, bem como com quaisquer outros mapeamentos de dispositivos de blocos especificados no modelo de execução. Se o modelo de execução tiver um volume existente definido para */dev/xvdb*, seus valores serão substituídos pelos valores especificados.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
```

```
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Usar modelos de execução com o Amazon EC2 Auto Scaling

É possível criar um grupo do Auto Scaling e especificar um modelo de execução a ser usado no grupo. Quando o Amazon EC2 Auto Scaling executar instâncias no grupo do Auto Scaling, ele usará os parâmetros de execução definidos no modelo de execução associado. Para obter mais informações, consulte Criar um modelo de execução para um grupo do Auto Scaling e Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.

Antes de criar um grupo do Auto Scaling usando um modelo de execução, você deverá criar um modelo de execução que inclua os parâmetros necessários para executar uma instância em um grupo do Auto Scaling, como o ID da AMI. O console fornece orientações para ajudar você a criar um modelo que pode ser usado com o Amazon EC2 Auto Scaling.

Como criar um modelo de execução para uso com o Auto Scaling usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.

5. Em Auto Scaling guidance (Orientação do Auto Scaling), marque a caixa de seleção para que o Amazon EC2 forneça orientações para ajudar você a criar um modelo para usar com o Auto Scaling.
6. Modifique os parâmetros de execução conforme necessário. Como você selecionou a orientação do Auto Scaling, alguns campos são obrigatórios e alguns ficam indisponíveis. Para obter informações sobre como configurar os parâmetros de execução para o Amazon EC2 Auto Scaling, consulte Criar um modelo de execução para um grupo do Auto Scaling e Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.
7. Escolha Criar modelo de execução.
8. (Opcional) Para criar um grupo do Auto Scaling usando esse modelo de inicialização, na página Next steps (Próximas etapas), escolha Create Auto Scaling group (Criar grupo do Auto Scaling).

Para obter exemplos que demonstram como usar a AWS CLI para criar modelos de execução com diversas combinações de parâmetros, consulte Examples for creating and managing launch templates with the AWS Command Line Interface (AWS CLI) no Guia do usuário do Amazon EC2 Auto Scaling.

Criar ou atualizar um grupo do Auto Scaling com um modelo de execução usando a AWS CLI

- Use o comando create-auto-scaling-group ou update-auto-scaling-group e especifique o parâmetro `--launch-template`.

Para obter mais informações sobre como criar ou atualizar um grupo do Auto Scaling usando um modelo de execução, consulte os tópicos apresentados a seguir no Guia do usuário do Amazon EC2 Auto Scaling.

- Create Auto Scaling groups using launch templates
- Update an Auto Scaling group

Usar modelos de execução com o Frota do EC2

É possível criar uma solicitação de um Frota do EC2 e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação do Frota do EC2, ele usará os parâmetros de execução definidos no modelo de execução associado. É possível substituir alguns parâmetros especificados no modelo de execução.

Para ter mais informações, consulte Criar uma Frota do EC2..

Para criar uma EC2 Fleet com um modelo de execução usando a AWS CLI

- Use o comando create-fleet. Use o parâmetro `--launch-template-configs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Usar modelos de execução com a frota spot

É possível criar uma solicitação de uma frota spot e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação da frota spot, ele usará os parâmetros de execução definidos no modelo de execução associado. É possível substituir alguns parâmetros especificados no modelo de execução.

Para ter mais informações, consulte Criar uma solicitação de frota spot.

Para criar uma solicitação de frota spot com um modelo de inicialização usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione Request Spot Instances (Solicitar instâncias spot).
4. Em Launch parameters (Parâmetros de inicialização), escolha Use a launch template (Usar um modelo de inicialização).
5. Em Launch template (Modelo de inicialização), escolha um modelo de inicialização e, no campo à direita, escolha a versão do modelo de inicialização.
6. Configure a frota Spot selecionando diferentes opções nessa tela. Para obter mais informações sobre essas opções, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console).
7. Quando você estiver pronto para criar uma frota spot, escolha Launch (Iniciar).

Para criar uma solicitação de frota spot com um modelo de inicialização usando a AWS CLI

- Use o comando request-spot-fleet. Use o parâmetro `LaunchTemplateConfigs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Executar uma instância usando parâmetros de uma instância existente

O console do Amazon EC2 fornece uma opção Launch more like this (Iniciar mais como esta) que permite usar uma instância atual como base para iniciar outras instâncias. Essa opção preenche automaticamente o assistente de execução de instâncias do Amazon EC2 com determinados detalhes de configuração da instância selecionada.

Considerações

- Não clonamos suas instâncias; replicamos apenas alguns detalhes da configuração. Para criar uma cópia da sua instância, primeiro crie uma AMI a partir dela e então execute mais instâncias a partir da AMI. Crie um modelo de execução para garantir que você execute as instâncias usando os mesmos detalhes de execução.
- A instância atual deve estar no estado `running`.

Detalhes copiados

Os detalhes de configuração a seguir são copiados da instância selecionada para o assistente de execução de instâncias:

- ID de AMI
- Tipo de instância
- Zona de disponibilidade, ou a VPC e a sub-rede nas quais a instância selecionada fica localizada
- Endereço IPv4 público. Se a instância selecionada atualmente tiver um endereço IPv4 público, a nova instância receberá um endereço IPv4 público – independentemente da configuração do endereço IPv4 pública padrão da instância selecionada. Para mais informações sobre endereços IPv4 públicos, consulte Endereços IPv4 públicos.
- Grupo de posicionamento, se aplicável
- A função do IAM associada à instância, se aplicável
- Configuração de comportamento de desativação (interromper ou encerrar)
- Configuração de proteção de encerramento (verdadeiro ou falso)
- Monitoramento do CloudWatch (habilitado ou desabilitado)
- Configuração de otimização do Amazon EBS (verdadeiro ou falso)
- Configuração de locação, se executando dentro de uma VPC (compartilhada ou dedicada)
- ID do kernel e ID do disco RAM, se aplicável

- Dados do usuário, se especificado
- Tags associadas à instância, se aplicável
- Grupos de segurança associados à instância
- [Instâncias do Windows] Informações de associações. Se a instância selecionada estiver associada a um arquivo de configuração, o mesmo arquivo será automaticamente associado à nova instância. Se o arquivo de configuração incluir uma configuração de domínio ingressado, a nova instância será ingressada no mesmo domínio. Para obter mais informações sobre como ingressar em um domínio, consulte Seamlessly Join a Windows EC2 Instance (Associe perfeitamente uma instância do EC2 do Windows) no Guia de administração do AWS Directory Service.

Detalhes não copiados

Os seguintes detalhes da configuração não são copiados da instância selecionada. Em vez disso, o assistente aplica as configurações ou o comportamento padrão:

- Número de interfaces de rede: o padrão é uma interface de rede, que é a interface de rede primária (eth0).
- Armazenamento: a configuração de armazenamento padrão é determinada pela AMI e pelo tipo de instância.

Para executar mais instâncias como uma instância existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Ações, Imagens e modelos e Executar mais como esta.
4. O assistente de execução de instância é aberto. É possível fazer as alterações necessárias na configuração da instância selecionando diferentes opções nesta tela.

   Quando estiver pronto para iniciar sua instância, escolha Launch instance (Iniciar instância).
5. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Executar uma instância AWS Marketplace

É possível assinar um produto da AWS Marketplace e iniciar uma instância na AMI do produto usando o assistente de inicialização do Amazon EC2. Para obter mais informações sobre AMIs pagas, consulte AMIs pagas. Para cancelar sua assinatura depois do lançamento, primeiro encerre todas as instâncias sendo executadas a partir delas. Para ter mais informações, consulte Gerenciar suas assinaturas do AWS Marketplace.

New console

Para executar uma instância no AWS Marketplace usando o assistente de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
3. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha Browse more AMIs (Explorar mais AMIs) e escolha a guia AWS Marketplace AMIs. Encontre uma AMI adequada navegando pelas categorias ou utilizando a funcionalidade de pesquisa. Para escolher seu produto, escolha Select (Selecionar).
5. O sistema apresentará uma janela com uma visão geral do produto selecionado. É possível visualizar as informações de preços, bem como quaisquer outras informações que o fornecedor fornecer. Quando estiver pronto, escolha um dos seguintes botões:
   - Assinar na execução da instância: sua assinatura começará quando você escolher a opção Executar instância (na etapa 10).
   - Assinar agora: sua assinatura começará imediatamente. Enquanto a assinatura estiver a caminho, você poderá configurar a instância seguindo as etapas deste procedimento. Se houver algum problema com os detalhes do cartão de crédito, você será convidado a atualizar os detalhes da conta.

> **Note**
>
> Não será cobrado o uso do produto até você executar uma instância com a AMI. Ao selecionar um tipo de instância, anote o preço de cada tipo de instância compatível. Também poderão ser aplicados impostos adicionais ao produto.

6. Em Instance type (Tipo de instância), escolha um tipo de instância para a instância. O tipo de instância define a configuração do hardware e o tamanho da instância a ser iniciada.
7. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
8. Em Network settings (Configurações de rede), Firewall (security groups) (Firewall [grupos de segurança]), anote o novo grupo de segurança criado conforme as especificações do fornecedor do produto. O grupo de segurança poderá conter regras que permitam a todos os endereços IPv4 (`0.0.0.0/0`) acesso a SSH (porta 22) no Linux ou RDP (porta 3389) no Windows. Recomendamos que você ajuste essas regras para permitir somente que um endereço específico ou um intervalo de endereços acessem sua instância nessas portas.
9. É possível usar outros campos na tela para configurar sua instância e adicionar armazenamento e etiquetas. Para obter informações sobre as diferentes opções que é possível configurar, consulte Iniciar uma instância usando parâmetros definidos.
10. No painel Summary (Resumo), em Software Image (AMI) (Imagem de software [AMI]), verifique os detalhes da AMI em que a instância será iniciada. Verifique também os outros detalhes de configuração que você especificou. Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).
11. Dependendo do produto no qual você se inscreveu, a instância poderá levar alguns minutos ou mais para ser executada. Se você escolher Assinar na execução da instância na etapa 5, primeiro será inscrito no produto antes da execução da sua instância. Se houver algum problema com os detalhes do cartão de crédito, você será convidado a atualizar os detalhes da conta. Quando a página de confirmação da execução for exibida, selecione View Instances (Visualizar instâncias) para acessar a página Instances (Instâncias).

> **Note**
>
> Você pagará o preço da assinatura, desde que sua instância esteja no estado `running`, mesmo se estiver ociosa. Se sua instância for interrompida, você ainda poderá ser cobrado pelo armazenamento.

12. Quando o status da sua instância estiver no estado `running`, será possível se conectar a ela. Para isso, selecione sua instância na lista, escolha Connect (Conectar) e escolha uma opção de conexão. Para obter mais informações sobre como se conectar à sua instância, consulte Conecte-se à sua instância do LinuxConectar-se à sua instância do Windows do .

> **Important**
>
> Verifique com atenção as instruções de uso do fornecedor, pois talvez seja necessário utilizar um nome de usuário específico para se conectar à instância. Para obter informações sobre como acessar os detalhes de assinatura, consulte Gerenciar suas assinaturas do AWS Marketplace.

13. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Old console

Para executar uma instância no AWS Marketplace usando o assistente de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do Amazon EC2, escolha Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon), escolha a categoria AWS Marketplace à esquerda. Encontre uma AMI adequada navegando pelas categorias ou utilizando a funcionalidade de pesquisa. Escolha Select (Selecionar) para escolher seu produto.
4. A caixa de diálogo exibe uma visão geral do produto selecionado. É possível visualizar as informações de preços, bem como quaisquer outras informações que o fornecedor fornecer. Quando você estiver pronto, escolha Continue (Continuar).

> **Note**
>
> Não será cobrado o uso do produto até que você execute uma instância com a AMI. Anote o preço de cada tipo de instância compatível, pois você deverá selecionar um tipo de instância na próxima página do assistente. Podem ser aplicados também impostos adicionais ao produto.

5. Na página Choose an Instance Type (Escolher um tipo de instância), selecione a configuração do hardware e o tamanho da instância a ser executada. Ao terminar, selecione Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
6. Nas próximas páginas do assistente, é possível configurar a instância, adicionar armazenamento e tags. Para obter mais informações sobre as diferentes opções que é possível configurar, consulte Inicie uma instância usando o assistente de inicialização de instância. Escolha Next (Próximo) até alcançar a página Configure Security Group (Configurar grupo de segurança).

   O assistente cria um novo grupo de segurança de acordo com as especificações do fornecedor do produto. O grupo de segurança pode incluir regras que permitem a todos os endereços IPv4 (`0.0.0.0/0`) acesso a SSH (porta 22) no Linux ou RDP (porta 3389) no Windows. Recomendamos que você ajuste essas regras para permitir somente que um endereço específico ou um intervalo de endereços acessem sua instância nessas portas.

   Quando estiver pronto, selecione Review and Launch (Revisar e executar).
7. Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da AMI a partir da qual você está prestes a executar a instância, assim como outros detalhes de configuração definidos no assistente. Quando você estiver pronto, escolha Launch (Executar) para selecionar ou criar um par de chaves e execute sua instância.
8. Dependendo do produto ao qual você se inscreveu, a instância pode levar alguns minutos ou mais para ser executada. Você primeiro é inscrito no produto antes de sua instância ser executada. Se houver algum problema com os detalhes do cartão de crédito, você será convidado a atualizar os detalhes da conta. Quando a página de confirmação da execução for exibida, selecione View Instances (Exibir instâncias) para acessar a página Instâncias.

> **Note**
>
> De você será cobrado o preço da assinatura, desde que sua instância esteja em execução, mesmo se estiver inativa. Se sua instância for interrompida, você ainda pode ser cobrado pelo armazenamento.

9. Quando o status da sua instância estiver no estado `running`, será possível se conectar a ela. Para fazer isso, selecione sua instância na lista e escolha Connect (Conectar). Siga as instruções na caixa de diálogo. Para obter mais informações sobre como se conectar à sua instância, consulte Conecte-se à sua instância do LinuxConectar-se à sua instância do Windows do .

   > **Important**
   >
   > Verifique as instruções de uso do fornecedor com cuidado, pois é possível precisar usar um nome de usuário específico para efetuar login na instância. Para obter mais informações sobre como acessar os detalhes de assinatura, consulte Gerenciar suas assinaturas do AWS Marketplace.

10. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Executar uma instância de AMI de AWS Marketplace usando a API e a CLI

Para executar instâncias de produtos do AWS Marketplace usando a API ou as ferramentas da linha de comando, primeiro garanta que você esteja inscrito no produto. É possível então executar uma instância com o ID da AMI do produto usando os seguintes métodos:

Método	Documentação
AWS CLI	Use o comando run-instances ou consulte o tópico a seguir para obter mais informações: Execução de uma instância.
AWS Tools for Windows PowerShell	Use o comando New-EC2Instance ou consulte o tópico a seguir para obter mais informações: Executar uma instância do Amazon EC2 usando o Windows PowerShell

Método	Documentação
API de consulta	Use a solicitação RunInstances.

Início e interrupção de instâncias do Amazon EC2

É possível interromper e iniciar a instância se ela tiver um volume do Amazon EBS como seu dispositivo raiz. Quando você interrompe uma instância, ela é desligada. Quando você inicia uma instância, ela é normalmente migrada para um novo computador host subjacente e recebe um novo endereço IPv4 público.

Quando você interrompe uma instância, ela não é excluída. Se você decidir que não necessita mais de uma instância, pode encerrá-la. Para ter mais informações, consulte Encerramento de instâncias do Amazon EC2. Se você quiser hibernar uma instância para salvar o conteúdo da memória da instância (RAM), consulte Hibernar sua instância do Amazon EC2. Para obter distinções entre as ações do ciclo de vida da instância, consulte. Diferenças entre reinicialização, interrupção, hibernação e encerramento

Conteúdo

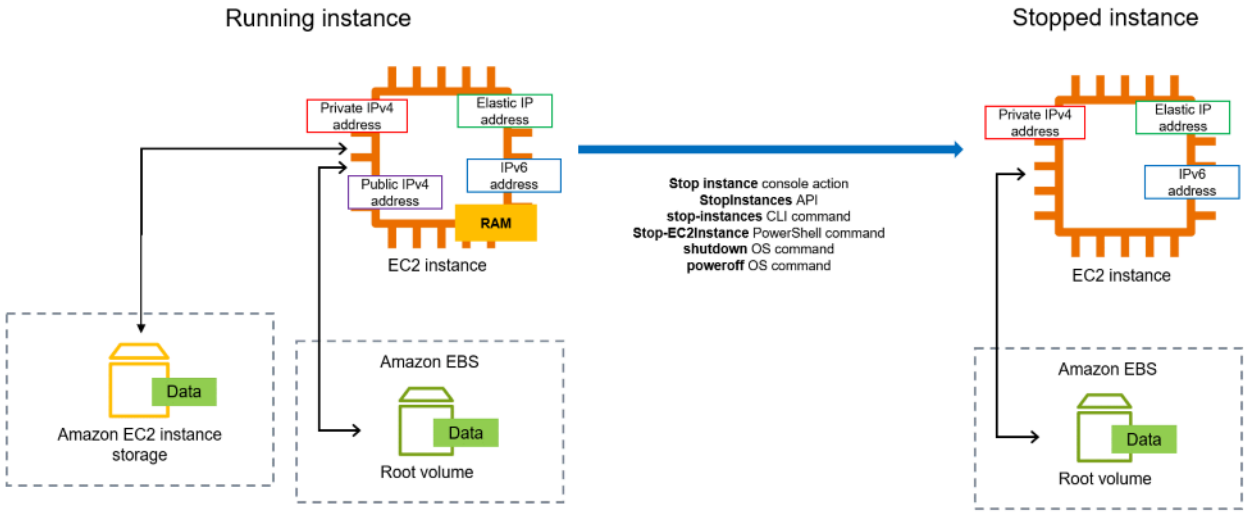
- Como funciona o início e a interrupção de uma instância
- Início e interrupção manuais das instâncias
- Parar e iniciar instâncias automaticamente
- Localizar todas as instâncias em execução e interrompidas
- Habilitação da proteção contra interrupção para sua instância

Como funciona o início e a interrupção de uma instância

Quando você interrompe uma instância, as alterações são registradas no nível do sistema operacional da instância, alguns recursos são perdidos e outros persistem. Quando você inicia uma instância, as alterações são registradas no nível da instância.

O diagrama a seguir mostra o que é perdido e o que persiste quando uma instância do Amazon EC2 é interrompida. Quando uma instância é interrompida, ela perde todos os volumes de armazenamento de instância anexados e os dados armazenados nesses volumes, os dados armazenados na RAM da instância e o endereço IPv4 público atribuído (se um endereço IP elástico

não estiver associado à instância). Uma instância retém endereços IPv4 privados atribuídos, endereços IP elásticos associados à instância, quaisquer endereços IPv6 e quaisquer volumes do Amazon EBS anexados e os dados desses volumes.



O que acontece quando você interrompe uma instância

Alterações registradas no nível do sistema operacional

- A solicitação da API envia um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema são interrompidos como resultado do evento de pressionamento de botão. O desligamento normal é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.
- O desligamento de ACPI é iniciado.
- A instância será desligada quando o processo de desligamento normal terminar. Não existe um tempo de desligamento configurável para o SO.
- Se o sistema operacional da instância não for desligado de forma limpa em alguns minutos, um desligamento forçado será executado.
- A execução da instância é interrompida.
- O status da instância muda para `stopping` e depois para `stopped`.
- [Auto Scaling] Se a instância estiver em um grupo do Auto Scaling, quando ela estiver em qualquer estado do Amazon EC2 diferente de `running` ou se o status para as verificações de status mudar para `impaired`, o Amazon EC2 Auto Scaling considerará a instância como não íntegra e a substituirá. Para obter mais informações, consulte Verificações de integridade de instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

- [Instâncias do Windows] Quando você interrompe e inicia uma instância do Windows, o agente de inicialização executa tarefas na instância, como alterar as letras das unidades de quaisquer volumes do Amazon EBS anexados. Para obter mais informações sobre esses padrões e como é possível alterá-los, consulte the section called “EC2Launch v2”.

Recursos perdidos

- Dados armazenados na RAM.
- Dados armazenados nos volumes de armazenamento de instância.
- O endereço IPv4 público que o Amazon EC2 atribuiu automaticamente à instância quando ela foi iniciada. Para manter um endereço IPv4 público que nunca muda, é possível associar um endereço IP elástico à instância.

Recursos que persistem

- Quaisquer volumes do Amazon EBS anexados.
- Dados armazenados nos volumes do Amazon EBS anexados.
- Endereços IPv4 privados.
- Endereços IPv6.
- O endereço IP elástico a ser associado à instância. Observe que, quando a instância for interrompida, você será cobrado pelos endereços IP elásticos associados.

Para obter informações sobre o que acontece quando você interrompe uma instância do Mac, consulte the section called “Interromper e encerrar a instância do Mac”.

O que acontece quando você inicia uma instância

Alterações registradas no nível do sistema operacional

- Na maioria dos casos, a instância é migrada para um novo computador host subjacente (embora em alguns casos, como quando uma instância está alocada a um host em uma configuração de Host dedicado, ela permaneça no host atual).
- O Amazon EC2 atribuirá um novo endereço IPv4 público à instância se ela estiver configurada para receber um endereço IPv4 público. Para manter um endereço IPv4 público que nunca muda, é possível associar um endereço IP elástico à instância.

Teste a resposta da aplicação para interromper e iniciar

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é interrompida e iniciada. Para obter mais informações, consulte o Guia do usuário do AWS Fault Injection Service.

Custos relacionados ao início e à interrupção de uma instância

Os custos a seguir estão associados à interrupção e inicialização de uma instância.

Interrupção: assim que o estado de uma instância muda para `shutting-down` ou `terminated`, as cobranças pela instância deixam de ser feitas. Você não é cobrado pelas taxas de uso ou transferência de dados para instâncias interrompidas. No entanto, cobranças são aplicáveis para armazenar volumes de armazenamento do Amazon EBS.

Inicialização: toda vez que você inicia uma instância interrompida, cobramos o mínimo de um minuto pelo uso. Após um minuto, você será cobrado apenas pelos segundos que usar. Por exemplo, se você executar uma instância por 20 segundos e, em seguida, interrompê-la, será cobrado por um minuto completo. Se você executar uma instância por 3 minutos e 40 segundos, você será cobrado exatamente por 3 minutos e 40 segundos de uso.

Início e interrupção manuais das instâncias

É possível iniciar e interromper instâncias baseadas no Amazon EBS (instâncias com dispositivos raiz do EBS). Não é possível iniciar e interromper instâncias com o dispositivo raiz de armazenamento de instância.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instância para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

Console

Para parar e iniciar uma instância baseada no Amazon EBS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação à esquerda, escolha Instâncias e, em seguida, selecione a instância.
3. Na guia Armazenamento, verifique se o Tipo de dispositivo raiz é EBS. Caso contrário, não será possível interromper a instância.
4. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.
5. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
6. Para iniciar a instância interrompida, selecione a instância e escolha Estado da instância e Iniciar instância.
7. Pode demorar alguns minutos para que a instância entre no estado `running`.
8. Se você interrompeu uma instância baseada no Amazon EBS e ela aparentar estar "presa" no estado `stopping`, será possível interrompê-la à força. Para ter mais informações, consulte Solução de problemas na interrupção da instância.

Command line

Pré-requisitos

Verifique se o dispositivo raiz da instância é um volume do EBS. Por exemplo, execute o comando describe-instances da AWS CLI e verifique se `RootDeviceType` é `ebs`, e não `instance-store`.

Para parar e iniciar uma instância baseada no Amazon EBS

Use um dos seguintes comandos:

- AWS CLI: stop-instances e start-instances.
- AWS Tools for PowerShell: Stop-EC2Instance e Start-EC2Instance.
- Comandos do sistema operacional: você pode iniciar um desligamento usando os comandos shutdown ou poweroff. Quando você usa um comando do sistema operacional, a instância é interrompida por padrão. É possível alterar esse comportamento para que, em vez disso, seja encerrada. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.

[Instâncias do Linux] Usar o comando halt do sistema operacional de uma instância não inicia um desligamento. Se você usar o comando halt, a instância não será encerrada; em vez disso, ela colocará a CPU em HLT, o que suspende a operação da CPU. A instância permanece em execução.

Parar e iniciar instâncias automaticamente

É possível automatizar a interrupção e o início de instâncias com os seguintes serviços:

Instance Scheduler na AWS

É possível usar o Instance Scheduler na AWS para automatizar o início e a interrupção de instâncias do EC2. Para obter mais informações, consulte How do I use Instance Scheduler with CloudFormation to schedule EC2 instances? (Como uso o Instance Scheduler com o CloudFormation para agendar instâncias do EC2?) Observe que se aplicam outras cobranças.

AWS Lambda e uma regra do Amazon EventBridge

É possível usar o Lambda e uma regra do EventBridge para interromper e iniciar suas instâncias em um agendamento. Para obter mais informações, consulte Como usar o Lambda para interromper e iniciar instâncias do Amazon EC2 em intervalos regulares?

Amazon EC2 Auto Scaling

Para garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga de uma aplicação, crie grupos do Auto Scaling. O Amazon EC2 Auto Scaling garante que sua aplicação sempre tenha a capacidade certa para lidar com a demanda de tráfego e economiza custos ao iniciar instâncias somente quando elas são necessárias. Observe que o Amazon EC2 Auto Scaling encerra, em vez de interromper, instâncias desnecessárias. Para configurar grupos do Auto Scaling, consulte Começar a usar o Amazon EC2 Auto Scaling.

Localizar todas as instâncias em execução e interrompidas

Você pode localizar todas as instâncias em execução e interrompidas em todas as Regiões da AWS em uma única página na Visualização Global do Amazon EC2. Isso é útil especialmente para inventariar e localizar instâncias esquecidas. Para obter informações sobre como usar o Visualização Global , consulte Amazon EC2 Global View.

Habilitação da proteção contra interrupção para sua instância

Para impedir que uma instância seja interrompida acidentalmente, habilite a proteção contra interrupção da instância. A proteção contra interrupção também protege a instância contra término acidental.

O atributo `DisableApiStop` da API `ModifyInstanceAttribute` do Amazon EC2 controla se a instância pode ser interrompida usando o console do Amazon EC2, a AWS CLI ou a API do Amazon EC2. Você pode definir o valor desse atributo ao executar a instância, enquanto a instância estiver em execução ou quando a instância for interrompida.

Considerações

- Habilitar a proteção contra interrupção não impede que você interrompa acidentalmente uma instância iniciando um desligamento da instância com um comando do sistema operacional, como shutdown ou poweroff.
- Habilitar a proteção contra interrupção não impede que a AWS interrompa a instância quando houver um evento programado para interromper a instância.
- Habilitar a proteção contra interrupção não impede que Amazon EC2 Auto Scaling termine uma instância quando ela não estiver íntegra ou durante eventos de redução da escala horizontal. É possível controlar se um grupo do Auto Scaling pode encerrar uma instância específica ao reduzir a escala horizontalmente usando a proteção contra redução da escala da instância na horizontal.
- A proteção contra interrupção não só impede que a instância seja interrompida acidentalmente, mas também previne o término acidental durante o uso do console, da AWS CLI ou da API. No entanto, isso não define automaticamente o atributo `DisableApiTermination`. Observe que, quando o atributo `DisableApiStop` é definido como `false`, o atributo `DisableApiTermination` é usado para determinar se a instância pode ser encerrada usando o console, a AWS CLI ou a API. Para ter mais informações, consulte Encerramento de instâncias do Amazon EC2.
- Não é possível habilitar a proteção contra interrupção para instâncias baseadas no armazenamento de instância.
- Não é possível habilitar a proteção contra interrupção para instâncias spot.
- A API do Amazon EC2 segue um modelo de consistência eventual quando você habilita ou desabilita a proteção contra interrupção. Isso significa que o resultado da execução de comandos para definir o atributo da proteção contra interrupção poderá não ser imediatamente visível para todos os comandos subsequentes que forem executados. Para obter mais informações, consulte Eventual consistency no Guia do desenvolvedor do Amazon EC2.

Tarefas de proteção contra interrupção

- Habilitar a proteção contra interrupção de uma instância na inicialização
- Habilitar a proteção contra interrupção de uma instância em execução ou interrompida
- Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Habilitar a proteção contra interrupção de uma instância na inicialização

Habilite a proteção contra interrupções de uma instância ao executar a instância usando um dos métodos a seguir.

Console

Como habilitar a proteção contra término de uma instância na inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Configure sua instância no novo assistente de inicialização de instância.
4. Para habilitar a proteção contra interrupções, em Advanced details (Detalhes avançados), em Stop protection (Proteção contra interrupções), escolha Enable (Habilitar).

AWS CLI

Como habilitar a proteção contra término de uma instância na inicialização

Use o comando run-instances da AWS CLI para iniciar a instância e especifique o parâmetro `disable-api-stop`.

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

Habilitar a proteção contra interrupção de uma instância em execução ou interrompida

Habilite a proteção contra interrupções de uma instância enquanto a instância é executada ou interrompida usando um dos métodos a seguir.

Console

Para habilitar a proteção contra encerramento de uma instância em execução ou interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância e escolha Ações > Configurações da instância > Alterar proteção contra interrupção.
4. Marque a caixa de seleção Enable (Habilitar) e escolha Save (Salvar).

AWS CLI

Para habilitar a proteção contra encerramento de uma instância em execução ou interrompida

Use o comando modify-instance-attribute da AWS CLI e especifique o parâmetro `disable-api-stop`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Desabilite a proteção contra interrupções de uma instância em execução ou interrompida usando um dos métodos a seguir.

Console

Para desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance Settings (Configurações da instância) e Change Termination Protection (Alterar proteção contra interrupção).
4. Desmarque a caixa de seleção Enable (Habilitar) e escolha Save (Salvar).

AWS CLI

Para desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Use o comando modify-instance-attribute da AWS CLI e especifique o parâmetro `no-disable-api-stop`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

Hibernar sua instância do Amazon EC2

Ao hibernar uma instância, o Amazon EC2 indica a realização da hibernação (suspend-to-disk) ao sistema operacional. A hibernação salva os conteúdos da memória da instância (RAM) para o volume raiz do Amazon Elastic Block Store (Amazon EBS). O Amazon EC2 persiste o volume raiz do EBS e todos os volumes de dados do EBS anexados. Quando a instância é iniciada:

- O volume raiz do EBS é restaurado para seu estado anterior
- Os conteúdos da RAM são recarregados
- Os processos que estavam em execução anteriormente na instância são retomados
- Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

É possível hibernar uma instância apenas se ela estiver habilitada para hibernação e atender aos pré-requisitos de hibernação.

Se uma instância ou aplicação levar muito tempo para o bootstrap e criar um espaço de memória para se tornar totalmente produtivo, será possível usar a hibernação para preaquecer a instância. Para pré-aquecer a instância:

1. Execute-a com a hibernação habilitada.
2. Coloque-a em um estado desejado.
3. Deixe-a em hibernação para que ela fique pronta para ser retomada no estado desejado sempre que necessário.

Você não terá cobranças pelo uso de uma instância em hibernação quando ela estiver no estado `stopped` ou pela transferência de dados quando o conteúdo da RAM for transferido para o volume raiz do EBS. Você terá cobranças pelo armazenamento de quaisquer volumes do EBS, incluindo o armazenamento de conteúdo da RAM.

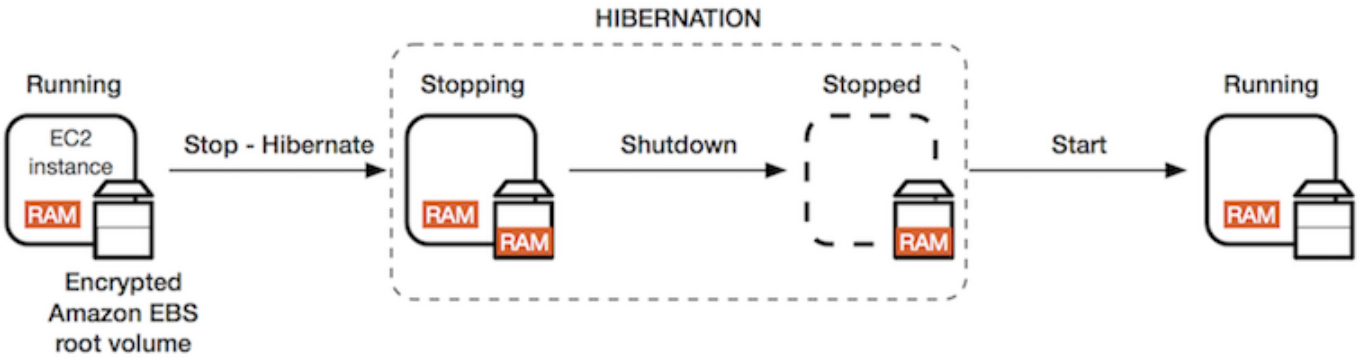
Se não precisar mais de uma instância, é possível encerrá-la a qualquer momento, incluindo quando ela está em um estado `stopped` (em hibernação). Para ter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Conteúdo

- Como a hibernação de instâncias do Amazon EC2 funciona
- Pré-requisitos para a hibernação de instâncias do Amazon EC2
- Configurar uma AMI para oferecer suporte à hibernação
- Habilitar a hibernação para uma instância do Amazon EC2
- Desabilitar o KASLR em uma instância (apenas Ubuntu)
- Hibernar uma instância do Amazon EC2
- Iniciar um instância do Amazon EC2 em hibernação
- Solucionar problemas de hibernação de instâncias do Amazon EC2

Como a hibernação de instâncias do Amazon EC2 funciona

O diagrama a seguir mostra uma visão geral básica do processo de hibernação para instâncias do EC2.



O que acontece quando uma instância é colocada em hibernação

Quando uma instância é colocada em hibernação, o seguinte acontece:

- O instância entrará no estado `stopping`. O Amazon EC2 sinaliza o sistema operacional para realizar a hibernação (suspend-to-disk). A hibernação congela todos os processos, salva o conteúdo da RAM no volume raiz do EBS e, depois, executa um desligamento normal.
- Quando o desligamento é concluído, a instância muda para o estado `stopped`.
- Todos os volumes do EBS permanecem anexados à instância, e seus dados são mantidos, incluindo o conteúdo salvo da RAM.
- Todos os volumes de armazenamento de instâncias do Amazon EC2 permanecem associados à instância, mas os dados nos volumes de armazenamento de instância são perdidos.
- Quando a instância está no estado `stopped`, você pode modificar alguns de seus atributos, inclusive o tipo de instância.
- Na maioria dos casos, a instância é migrada para um novo computador host subjacente quando ele é iniciado. Isso também acontece ao interromper e iniciar uma instância.
- Quando a instância é iniciada, ela é carregada e o sistema operacional lê o conteúdo da RAM no volume raiz do EBS antes de descongelar os processos para retomar ao seu estado.
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6. Quando a instância é iniciada, ela continua a reter os endereços IPv4 privados e todos os endereços IPv6.
- O Amazon EC2 libera o endereço IPv4 público. Quando a instância é iniciada, o Amazon EC2 atribui a ela um novo endereço IPv4 público.
- A instância retém os endereços IP elásticos associados. Você é cobrado por todos os endereços IP elásticos associados a uma instância em hibernação.

Para obter informações sobre como a hibernação difere da reinicialização, da interrupção e do encerramento, consulte Diferenças entre reinicialização, interrupção, hibernação e encerramento.

Limitações

- Quando você hiberna uma instância, os dados em todos os volumes de armazenamento de instâncias são perdidos.
- (Instâncias do Linux) Não é possível hibernar uma instância do Linux com mais de 150 GB de RAM.
- (Instâncias do Windows) Não é possível hibernar uma instância do Windows com mais de 16 GB de RAM.
- Se você criar um snapshot ou uma AMI a partir de uma instância que está hibernada ou que tenha hibernação habilitada, talvez não consiga se conectar a uma nova instância iniciada a partir da AMI ou de uma AMI criada pelo snapshot.

- (Apenas instâncias spot) Se o Amazon EC2 colocar sua instância spot em hibernação, somente o Amazon EC2 poderá reiniciá-la. Se você mesmo colocar a instância spot em hibernação (hibernação iniciada pelo usuário), poderá reiniciá-la. Uma instância spot colocada em hibernação só poderá ser reiniciada se houver capacidade disponível e se o preço spot for menor ou igual ao preço máximo especificado.
- Não é possível hibernar uma instância que está em um grupo do Auto Scaling ou é usada pelo Amazon ECS. Se sua instância estiver em um grupo do Auto Scaling, e você tentar hiberná-la, o serviço Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.
- Não é possível efetuar a hibernação de uma instância configurada para inicializar no modo UEFI com o UEFI Secure Boot habilitado.
- Se você hibernar uma instância que foi executada em um Reserva de capacidade, o Reserva de capacidade não garante que a instância hibernada possa retornar depois de tentar iniciá-la.
- Você não pode hibernar uma instância que usa um kernel abaixo de 5.10 se o modo Federal Information Processing Standard (FIPS) estiver ativado.
- Não oferecemos suporte à manutenção de uma instância em hibernação por mais de 60 dias. Para manter a instância por mais que 60 dias, inicie, interrompa e inicialize a instância em hibernação.
- Atualizamos constantemente nossa plataforma com atualizações e patches de segurança, o que entra em conflito com instâncias em hibernação. Notificamos você sobre as atualizações críticas que exijam uma inicialização das instâncias em hibernação para que você possa executar um desligamento ou uma reinicialização para aplicar as atualizações e os patches de segurança necessários.

Considerações sobre colocar uma instância spot em hibernação

- Se você colocar em hibernação a instância spot, poderá reiniciá-la, desde que haja capacidade disponível e o preço spot seja menor ou igual ao preço máximo especificado.
- Se o Amazon EC2 colocar a instância spot em hibernação:
  - Somente o Amazon EC2 poderá reiniciar a instância.
  - O Amazon EC2 reinicia a instância spot que foi colocada em hibernação quando a capacidade fica disponível por um preço spot igual ou inferior ao preço máximo especificado por você.
  - Dois minutos antes que o Amazon EC2 coloque a instância spot em hibernação, você receberá um aviso de interrupção.

Para ter mais informações, consulte Interrupções de instâncias spot.

- Existem várias maneiras de habilitar a hibernação de uma instância spot. Para ter mais informações, consulte Especificar o comportamento de interrupção.

Pré-requisitos para a hibernação de instâncias do Amazon EC2

É possível habilitar o suporte à hibernação para uma instância sob demanda ou uma instância spot ao iniciá-la. Não é possível habilitar a hibernação em uma instância existente, esteja ela em execução ou parada. Para ter mais informações, consulte Habilitar hibernação da instância.

Requisitos para hibernar uma instância

- Regiões da AWS
- AMIs
- Famílias de instâncias
- Tamanho da instância RAM
- Tipo do volume de raiz
- Tamanho do volume raiz
- Criptografia do volume raiz
- Tipo de volume do EBS
- Solicitações de instância Spot

Regiões da AWS

É possível usar a hibernação com instâncias em todas as Regiões da AWS.

AMIs

É necessário usar uma AMI do HVM que ofereça suporte à hibernação. As seguintes AMIs oferecem suporte para hibernação:

AMIs Linux

- AMI do AL2023 lançada em 20/9/2023 ou posteriormente.
- AMI do Amazon Linux 2 lançada em 29/08/2019 ou posterior
- AMI do Amazon Linux 2018.03 lançada em 16/11/2018 ou posterior

- CentOS versão 8 AMI [1] (configuração adicional necessária)
- Fedora versão 34 ou AMI [1] posterior (configuração adicional necessária)
- Red Hat Enterprise Linux (RHEL) 9 AMI [1] (configuração adicional necessária)
- Red Hat Enterprise Linux (RHEL) 8 AMI [1] (configuração adicional necessária)
- AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish) lançada com o número de série 20230303 ou posterior [2]
- AMI do Ubuntu 20.04 LTS (Focal Fossa) lançada com o número de série 20210820 ou posterior [2]
- AMI do Ubuntu 18.04 LTS (Bionic Beaver) lançada com o número de série 20190722.1 ou posterior [2] [4]
- AMI do Ubuntu 16.04 LTS (Xenial Xerus) [2] [3] [4] (uma configuração adicional é necessária)

[1] Para CentOS, Fedora e Red Hat Enterprise Linux, a hibernação é possível apenas em instâncias baseadas em Nitro.

[2] Recomendamos desabilitar o KASLR em instâncias com o Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus). Para ter mais informações, consulte Desabilitar o KASLR em uma instância (apenas Ubuntu).

[3] Para a AMI do Ubuntu 16.04 LTS (Xenial Xerus), a hibernação não é compatível com os tipos de instância `t3.nano`. Nenhum patch será disponibilizado porque o Ubuntu (Xenial Xerus) encerrou o suporte em abril de 2021. Se quiser usar os tipos de instância `t3.nano`, recomendamos que você atualize para a AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish), a AMI do Ubuntu 20.04 LTS (Focal Fossa) ou a AMI do Ubuntu 18.04 LTS (Bionic Beaver).

[4] O suporte para Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus) chegou ao fim da vida útil.

Para configurar sua AMI para oferecer suporte à hibernação, consulte Configurar uma AMI para oferecer suporte à hibernação.

O suporte para outras versões do Ubuntu e outros sistemas operacionais será disponibilizado em breve.

AMIs do Windows

- AMI do Windows Server 2022 lançada em 13/09/2023 ou posterior.

- AMI do Windows Server 2019 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2016 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2012 R2 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2012 lançada em 11/09/2019 ou posterior.

Famílias de instâncias

É necessário usar uma família de instâncias que ofereça suporte à hibernação.

- Uso geral: M3, M4, M5, M5a, M5ad, M5d, M6i, M6id, M7i, M7i-flex, T2, T3 e T3a
- Otimizada para computação: C3, C4, C5, C5d, C6i, C6id, C7a, C7i e C7i-flex
- Otimizada para memória: R3, R4, R5, R5a, R5ad, R5d, R7a, R7i e R7iz
- Otimizada para armazenamento: I3 e I3en

Instâncias do Nitro: não há suporte a instâncias bare metal.

Para ver os tipos de instância disponíveis que suportam hibernação em uma região específica

Os tipos de instância disponíveis variam de acordo com a região. Para ver os tipos de instâncias disponíveis que suportam hibernação em uma região, use o comando describe-instance-types com o parâmetro `--region`. Inclua o parâmetro `--filters` para definir o escopo dos resultados para os tipos de instância com suporte a hibernação e o parâmetro `--query` para definir o escopo da saída para o valor de `InstanceType`.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Exemplo de saída

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
c4.8xlarge
```

```
...
```

Tamanho da instância RAM

Instâncias do Linux: devem ter menos de 150 GB.

Instâncias do Windows: podem ter até 16 GB. Para colocar uma instância T3 ou T3a em hibernação, recomendamos pelo menos 1 GB de RAM.

Tipo do volume de raiz

O volume raiz deve ser um volume do EBS, e não um volume de armazenamento de instâncias.

Tamanho do volume raiz

O volume raiz deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado, por exemplo, sistema operacional ou aplicações. Quando você habilita a hibernação, é alocado espaço no volume raiz no lançamento para armazenar a RAM.

Criptografia do volume raiz

O volume raiz deve ser criptografado para garantir a proteção do conteúdo confidencial existente na memória no momento da hibernação. Quando os dados da RAM são movidos para o volume raiz do EBS, eles sempre são criptografados. A criptografia do volume raiz é imposta na execução da instância.

Use uma das três opções a seguir para garantir que o volume raiz seja um volume criptografado do EBS:

- Criptografia do EBS por padrão: é possível habilitar a criptografia do EBS por padrão para garantir que todos os novos volumes do EBS criados na sua conta da AWS sejam criptografados. Dessa forma, você habilita a hibernação para suas instâncias sem especificar a intenção da criptografia na execução da instância. Para obter mais informações, consulte Habilitar criptografia por padrão.
- Criptografia EBS de uma “única etapa”: é possível iniciar instâncias do EC2 criptografadas com suporte de EBS a partir de uma AMI não criptografada e, ao mesmo tempo, habilitar a hibernação. Para ter mais informações, consulte Usar criptografia com AMIs com EBS.
- AMI criptografada: é possível habilitar a criptografia do EBS usando uma AMI criptografada para iniciar sua instância. Se a sua AMI não tiver um snapshot raiz criptografado, será possível copiá-lo para uma nova AMI e solicitar a criptografia. Para ter mais informações, consulte Criptografar uma imagem não criptografada durante a cópia e Copiar um AMI.

Tipo de volume do EBS

Os volumes do EBS devem usar um dos seguintes tipos de volume do EBS:

- SSD para uso geral (`gp2` e `gp3`)
- IOPS provisionado SSD (`io1` e `io2`)

Se você escolher um tipo de volume SSD de IOPS Provisionado SSD, você deverá provisionar o volume do EBS com as IOPS apropriadas para alcançar a performance ideal para hibernação. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.

Solicitações de instância Spot

Os seguintes requisitos se aplicam a instâncias spot:

- O tipo de solicitação da instância spot deve ser `persistent`.
- Não é possível especificar um grupo de execução na solicitação de instância spot.

Configurar uma AMI para oferecer suporte à hibernação

As seguintes AMIs do Linux oferecem suporte à hibernação, mas, para hibernar uma instância que foi iniciada com uma dessas AMIs, uma configuração adicional é necessária para que você possa colocar a instância em hibernação.

Configurações adicionais são necessárias para:

- AMI do Amazon Linux 2 mínima lançada em 29/08/2019 ou posterior
- Amazon Linux 2 lançado antes de 29/08/2019
- Amazon Linux lançado antes de 16/11/2018
- CentOS versão 8 ou posterior
- Fedora versão 34 ou posterior
- Red Hat Enterprise Linux versão 8 ou 9
- Ubuntu 20.04 LTS (Focal Fossa) liberado antes do número de série 20210820
- Ubuntu 18.04 (Bionic Beaver) lançado antes do número de série 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Para obter mais informações, consulte Update instance software on your Amazon Linux 2 instance.

Nenhuma configuração adicional é necessária para as AMIs a seguir, porque elas já estão configuradas para suportar hibernação:

- AMI do AL2023 lançada em 20/9/2023 ou posteriormente.
- AMI do Amazon Linux 2 completa lançada em 29/08/2019 ou posterior
- AMI do Amazon Linux 2018.03 lançada em 16/11/2018 ou posterior
- AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish) lançada com o número de série 20230303 ou posterior
- AMI do Ubuntu 20.04 LTS (Focal Fossa) lançada com o número de série 20210820 ou posterior
- AMI do Ubuntu 18.04 LTS (Bionic Beaver) lançada com o número de série 20190722.1 ou posterior

AMI do Amazon Linux 2 mínima lançada em 29/08/2019 ou posterior

Para configurar uma AMI do Amazon Linux 2 mínima lançada antes de 29/08/2019 para permitir hibernação

1. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Reinicie o serviço .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 lançado antes de 29/08/2019

Como configurar uma AMI do Amazon Linux 2 lançada antes de 29/08/2019 para suportar hibernação

1. Atualize o kernel para `4.14.138-114.102` ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para `4.14.138-114.102` ou posterior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Amazon Linux lançado antes de 16/11/2018

Para configurar uma AMI do Amazon Linux lançada antes de 16/11/2018 para oferecer suporte à hibernação

1. Atualize o kernel para `4.14.77-70.59` ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para `4.14.77-70.59` ou maior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

CentOS versão 8 ou posterior

Para configurar uma AMI do CentOS versão 8 ou posterior para suportar hibernação

1. Atualize o kernel para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

6. Confirme se a versão do kernel está atualizada para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Fedora versão 34 ou posterior

Para configurar uma AMI do Fedora versão 34 ou posterior para suportar hibernação

1. Atualize o kernel para `5.12.10-300.fc34.x86_64` ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

5. Confirme se a versão do kernel está atualizada para `5.12.10-300.fc34.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux versão 8 ou 9

Para configurar uma AMI do Red Hat Enterprise Linux 8 ou 9 para suportar hibernação

1. Atualize o kernel para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

   Versão 8 da RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   Versão 9 da RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

6. Confirme se a versão do kernel está atualizada para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) liberado antes do número de série 20210820

Para configurar uma AMI do Ubuntu 20.04 LTS (Focal Fossa) lançada antes do número de série 20210820 para ser compatível com hibernação

1. Atualize o linux-aws-kernel para `5.8.0-1038.40` ou posterior, e grub2 para `2.04-1ubuntu26.13` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

3. Confirme se a versão do kernel está atualizada para `5.8.0-1038.40` ou posterior.

```
[ec2-user ~]$ uname -a
```

4. Confirme se a versão do grub2 está atualizada para `2.04-1ubuntu26.13` ou posterior.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) lançado antes do número de série 20190722.1

Para configurar uma AMI do Ubuntu 18.04 LTS lançada antes do número de série 20190722.1 para suportar hibernação

1. Atualize o kernel para `4.15.0-1044` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para `4.15.0-1044` ou posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Para configurar o Ubuntu 16.04 LTS para ser compatível com a hibernação, é necessário instalar o pacote do kernel linux-aws-hwe versão 4.15.0-1058-aws ou posterior e o agente ec2-hibint.

> **Important**
>
> O pacote do kernel `linux-aws-hwe` é totalmente compatível com o Canonical. O suporte padrão para o Ubuntu 16.04 LTS terminou em abril de 2021, e o pacote não recebe mais atualizações regulares. No entanto, ele receberá atualizações de segurança adicionais até que o suporte de Manutenção de segurança estendida termine em 2024. Para obter mais informações, consulte Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available no blog do Canonical Ubuntu.
> Recomendamos que você atualize para a AMI do Ubuntu 20.04 LTS (Focal Fossa) ou a AMI do Ubuntu 18.04 LTS (Bionic Beaver).

Como configurar uma AMI do Ubuntu 16.04 LTS para que seja compatível com a hibernação

1. Atualize o kernel para `4.15.0-1058-aws` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para `4.15.0-1058-aws` ou posterior.

```
[ec2-user ~]$ uname -a
```

Habilitar a hibernação para uma instância do Amazon EC2

Para colocar uma instância em hibernação, é necessário habilitá-la para hibernação ao iniciar a instância.

> **Important**
>
> Não é possível habilitar ou desabilitar a hibernação para uma instância depois de executá-la.

Tópicos

- Habilitar a hibernação de uma instância sob demanda
- Para habilitar a hibernação de instâncias spot
- Visualizar se uma instância está habilitada para hibernação

Habilitar a hibernação de uma instância sob demanda

Use um dos métodos a seguir para habilitar a hibernação de instâncias sob demanda.

New console

Para habilitar a hibernação de uma instância sob demanda

1. Siga o procedimento para iniciar uma instância, mas não inicie a instância até concluir as etapas a seguir para habilitar a hibernação.
2. Para habilitar a hibernação, configure os seguintes campos no assistente de inicialização da instância:

   a. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI com suporte à hibernação. Para ter mais informações, consulte AMIs.

   b. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para ter mais informações, consulte Famílias de instâncias.

   c. Em Configure storage (Configurar armazenamento), escolha Advanced (Avançado) (à direita) e especifique estas informações para o volume raiz:

      - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
      - Em Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível: SSD de uso geral (`gp2` e `gp3`) ou SSD de IOPS provisionadas (`io1` e `io2`).
      - Em Encrypted (Criptografado), escolha Yes (Sim). Se você tiver habilitado a criptografia por padrão nessa região da AWS, a opção Yes (Sim) estará selecionada.
      - Para KMS key (Chave do KMS), selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

      Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.

   d. Expanda Advanced details (Detalhes avançados) e, em Stop - Hibernate behavior (Interromper: comportamento de hibernação), escolha Enable (Habilitar).
3. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Old console

Para habilitar a hibernação de uma instância sob demanda

1. Siga o procedimento do Inicie uma instância usando o assistente de inicialização de instância.
2. Na página Choose an Amazon Machine Image (AMI) (Escolher uma Imagem de máquina da Amazon (AMI)), selecione uma AMI compatível com a hibernação. Para obter mais informações sobre as AMIs compatíveis, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.
3. Na página Escolher um tipo de instância, selecione um tipo de instância compatível e escolha Próximo: configurar os detalhes da instância. Para obter mais informações sobre os tipos de instância compatíveis, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.
4. Na página Configure Instance Details (Configurar detalhes da instância), em Stop - Hibernate Behavior (Interromper - comportamento de hibernação), marque a caixa de seleção Enable hibernation as an additional stop behavior (Habilitar a hibernação como um comportamento de interrupção adicional).
5. Na página Adicionar armazenamento, para o volume raiz, especifique as seguintes informações:

   - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
   - Para Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível (SSD de uso geral (`gp2` e `gp3`) ou SSD de IOPS provisionadas (`io1` e `io2`)).
   - Para Criptografia, selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

   Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.
6. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para ter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância.

AWS CLI

Para habilitar a hibernação de uma instância sob demanda

Use o comando run-instances para executar uma instância. Especifique os parâmetros do volume raiz do EBS usando o parâmetro `--block-device-mappings file://mapping.json` e habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Especifique o seguinte em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Se você habilitou a criptografia por padrão nesta região da AWS, é possível omitir `"Encrypted": true`.

PowerShell

Para habilitar a hibernação de uma instância sob demanda usando o AWS Tools for Windows PowerShell

Use o comando New-EC2Instance para executar uma instância. Especifique o volume raiz do EBS definindo primeiro o mapeamento do dispositivo de bloco e adicionando-o ao comando usando o parâmetro `-BlockDeviceMappings`. Habilite a hibernação usando o parâmetro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
              -ImageId ami-0abcdef1234567890 `
              -InstanceType m5.large `
              -BlockDeviceMappings $ebs_encrypt `
              -HibernationOptions_Configured $true `
              -MinCount 1 `
              -MaxCount 1 `
              -KeyName MyKeyPair
```

> **Note**
>
> O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando Get-EC2Image.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Se você habilitou a criptografia por padrão nesta região da AWS, poderá omitir o `Encrypted = $true` do mapeamento do dispositivo de bloco.

Para habilitar a hibernação de instâncias spot

Use um dos métodos a seguir para habilitar a hibernação de instâncias spot. Para obter mais informações sobre a hibernação de instâncias spot ao ocorrer uma interrupção, consulte Interrupções de instâncias spot.

Console

Você pode usar o assistente de inicialização de instância no console do Amazon EC2 para habilitar a hibernação de uma instância spot.

Para habilitar a hibernação de uma instância spot

1. Siga o procedimento para solicitar uma instância spot usando o assistente de inicialização de instâncias, mas não inicie a instância até concluir as etapas a seguir para habilitar a hibernação.
2. Para habilitar a hibernação, configure os seguintes campos no assistente de inicialização da instância:

   a. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI com suporte à hibernação. Para ter mais informações, consulte AMIs.

   b. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para ter mais informações, consulte Famílias de instâncias.

   c. Em Configure storage (Configurar armazenamento), escolha Advanced (Avançado) (à direita) e especifique estas informações para o volume raiz:

      - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
      - Em Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível: SSD de uso geral (`gp2` e `gp3`) ou SSD de IOPS provisionadas (`io1` e `io2`).
      - Em Encrypted (Criptografado), escolha Yes (Sim). Se você tiver habilitado a criptografia por padrão nessa região da AWS, a opção Yes (Sim) estará selecionada.
      - Para KMS key (Chave do KMS), selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.

d. Expanda Detalhes avançados e, além de preencher os campos para configurar uma instância spot, faça o seguinte:

   i. Em Tipo de solicitação, escolha Persistente.

   ii. Em Comportamento de interrupção, escolha Hibernar. Ou então, em Comportamento de parar - hibernar, escolha Habilitar. Ambos os campos habilitam a hibernação da instância spot. Você só precisa configurar um deles.

3. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

AWS CLI

Você pode habilitar a hibernação de uma instância spot usando o comando run-instances da AWS CLI.

Para habilitar a hibernação de uma instância spot usando o parâmetro **`hibernation-options`**

Use o comando run-instances para executar uma instância spot. Especifique os parâmetros do volume raiz do EBS usando o parâmetro `--block-device-mappings file://mapping.json` e habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`. O tipo de solicitação da instância spot (`SpotInstanceType`) deve ser `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
```

```
            "SpotInstanceType":"persistent"
        }
    }
```

Especifique os parâmetros do volume raiz do EBS no `mapping.json` como se segue.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Se você habilitou a criptografia por padrão nesta região da AWS, é possível omitir `"Encrypted": true`.

PowerShell

Para habilitar a hibernação de uma instância spot usando o AWS Tools for Windows PowerShell

Use o comando New-EC2Instance para solicitar uma instância spot. Especifique o volume raiz do EBS definindo primeiro o mapeamento do dispositivo de bloco e adicionando-o ao comando usando o parâmetro `-BlockDeviceMappings`. Habilite a hibernação usando o parâmetro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
```

```
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
              -ImageId ami-0abcdef1234567890 `
              -InstanceType m5.large `
              -BlockDeviceMappings $ebs_encrypt `
              -HibernationOptions_Configured $true `
              -MinCount 1 `
              -MaxCount 1 `
              -KeyName MyKeyPair `
              -InstanceMarketOption @(
                    MarketType = spot;
                    SpotOptions @{
                    MaxPrice = 1;
                    SpotInstanceType = persistent}
                )
```

> **Note**
>
> O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando Get-EC2Image.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Se você habilitou a criptografia por padrão nesta região da AWS, poderá omitir o `Encrypted = $true` do mapeamento do dispositivo de bloco.

Existem várias maneiras de habilitar a hibernação de uma instância spot. Para ter mais informações, consulte Especificar o comportamento de interrupção.

Visualizar se uma instância está habilitada para hibernação

Use as instruções a seguir para visualizar se uma instância está habilitada para hibernação.

Console

Para visualizar se uma instância está habilitada para hibernação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, na guia Details (Detalhes), na seção Instance details (Detalhes da instância), verifique Stop-hibernate behavior (Interromper - comportamento de hibernação). Enabled (Habilitada) indica que a instância está habilitada para hibernação.

AWS CLI

Para visualizar se uma instância está habilitada para hibernação

Use o comando describe-instances e especifique o parâmetro `--filters "Name=hibernation-options.configured,Values=true"` para filtrar as instâncias que estão habilitadas para hibernação.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

O campo da saída a seguir indica que a instância está habilitada para hibernação.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Para visualizar se uma instância está habilitada para hibernação usando a AWS Tools for Windows PowerShell

Use o comando Get-EC2Instance e especifique o parâmetro `-Filter @{ Name="hibernation-options.configured"; Value="true"}` para filtrar as instâncias que estão habilitadas para hibernação.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";
 Value="true"}).Instances
```

A saída lista as instâncias do EC2 habilitadas para hibernação.

Desabilitar o KASLR em uma instância (apenas Ubuntu)

Para executar a hibernação em uma instância recém-executada com o Ubuntu 16.04 LTS (Xenial Xerus), o Ubuntu 18.04 LTS (Bionic Beaver) lançado com o número de série 20190722.1 ou posterior ou o Ubuntu 20.04 LTS (Focal Fossa) lançado com o número de série 20210820 ou posterior, recomendamos desabilitar o KASLR (Kernel Address Space Layout Randomization). No Ubuntu 16.04 LTS, Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS, o KASLR é habilitado por padrão.

O KASLR é um recurso de segurança do kernel padrão do Linux que ajuda a mitigar as ramificações de e a exposição e às vulnerabilidades de acesso à memória ainda não descobertas por randomização do valor base do endereço do kernel. Com o KASLR habilitado, há uma possibilidade de a instância não ser retomada depois de ter estado em hibernação.

Para saber mais sobre o KASLR, consulte Recursos do Ubuntu.

Para desabilitar o KASLR em uma instância executada com o Ubuntu

1. Conecte-se à sua instância usando SSH. Para ter mais informações, consulte the section called “Conectar com SSH via macOS ou Linux”.
2. Abra o arquivo `/etc/default/grub.d/50-cloudimg-settings.cfg` com seu editor de preferência. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` para anexar a opção `nokaslr` no final, conforme mostrado no exemplo a seguir.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295 nokaslr"
   ```
3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração do grub.

   ```
   [ec2-user ~]$ sudo update-grub
   ```
5. Reinicialize a instância.

   ```
   [ec2-user ~]$ sudo reboot
   ```
6. Execute o seguinte comando para confirmar que `nokaslr` foi adicionado.

   ```
   [ec2-user ~]$ cat /proc/cmdline
   ```

   A saída do comando deve incluir a opção `nokaslr`.

Hibernar uma instância do Amazon EC2

Você poderá iniciar a hibernação em uma instância sob demanda ou de uma instância spot se a instância for baseada em EBS, estiver habilitada para hibernação e atender aos pré-requisitos para hibernação. Se uma instância não puder hibernar com sucesso, ocorrerá um desligamento normal.

Console

Para hibernar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Instance state (Estado da instância) e Hibernate instance (Hibernar instância). Se Hibernate instance (Hibernar instância) estiver desabilitado, a instância já estará em hibernação ou interrompida ou não poderá ser hibernada. Para ter mais informações, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2.
4. Quando a confirmação for solicitada, escolha Hibernate (Hibernar). Pode demorar alguns minutos para que a instância hiberne. O estado da instância primeiro muda para Interrompendo e, em seguida, muda para Interrompido quando a instância tiver hibernado.

AWS CLI

Para hibernar uma instância baseada no Amazon EBS

Use o comando stop-instances e especifique o parâmetro `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Para hibernar uma instância usando o AWS Tools for Windows PowerShell

Use o comando Stop-EC2Instance e especifique o parâmetro `-Hibernate $true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

Para visualizar se a hibernação foi iniciada em uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, na guia Detalhes, na seção Detalhes da instância), verifique o valor de Mensagem de transição de estado.

   Client.UserInitiatedHibernate: hibernação iniciada pelo usuário indica que você iniciou a hibernação da instância sob demanda ou da instância spot.

AWS CLI

Para visualizar se a hibernação foi iniciada em uma instância

Use o comando describe-instances e especifique o filtro `state-reason-code` para ver as instâncias nas quais a hibernação foi iniciada.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

O campo da saída a seguir indica que a hibernação foi iniciada na instância sob demanda ou na instância spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Para visualizar se a hibernação foi iniciada em uma instância usando a AWS Tools for Windows PowerShell

Use o comando Get-EC2Instance e especifique o filtro `state-reason-code` para ver as instâncias nas quais a hibernação foi iniciada.

```
Get-EC2Instance `
```

```
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

A saída lista as instâncias do EC2 nas quais a hibernação foi iniciada.

Iniciar um instância do Amazon EC2 em hibernação

Inicie uma instância em hibernação da mesma maneira como faria em uma instância interrompida.

> **Note**
>
> Para instâncias spot, se o Amazon EC2 colocou a instância em hibernação, só Amazon EC2 poderá reiniciá-la. Você só poderá reiniciar uma instância spot em hibernação se tiver sido você que a colocou em hibernação. Instâncias spot colocadas em hibernação só poderão ser reiniciadas se houver capacidade disponível e se o preço spot for menor ou igual ao preço máximo especificado.

Console

Para iniciar um instância em hibernação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância em hibernação e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no estado `running`. Durante esse tempo, as verificações de status da instância mostram a instância em um estado de falha até que a instância seja iniciada.

AWS CLI

Para iniciar um instância em hibernação

Use o comando start-instances.

```
aws ec2 start-instances \
    --instance-ids i-1234567890abcdef0
```

PowerShell

Como iniciar uma instância em hibernação usando o AWS Tools for Windows PowerShell

Use o comando Start-EC2Instance.

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

Solucionar problemas de hibernação de instâncias do Amazon EC2

Use estas informações para ajudar a diagnosticar e corrigir problemas que podem ser encontrados ao hibernar uma instância.

Problemas de hibernação

- Não é possível hibernar imediatamente após a execução
- A transição de stopping para stopped demora muito tempo, e o estado da memória não é restaurado depois da execução
- Instância "presa" no estado de parada
- Não é possível iniciar a instância spot imediatamente após a hibernação
- Falha ao retomar instâncias spot

Não é possível hibernar imediatamente após a execução

Você receberá uma mensagem de erro se tentar hibernar uma instância muito rapidamente depois de executá-la.

Após iniciar a execução, aguarde cerca de dois minutos para instâncias do Linux e cerca de cinco minutos para instâncias do Windows para hiberná-las.

A transição de **`stopping`** para **`stopped`** demora muito tempo, e o estado da memória não é restaurado depois da execução

Quando demora muito tempo para que a instância em hibernação faça a transição do estado `stopping` para `stopped`, e se o estado da memória não é restaurado depois da execução, isso pode indicar que a hibernação não foi configurada corretamente.

Instâncias do Linux

Verifique o log do sistema da instância e procure as mensagens relacionadas à hibernação. Para acessar o log do sistema, conecte-se à instância ou use o comando get-console-output. Localize as linhas do log no `hibinit-agent`. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que o volume raiz da instância não é grande o suficiente: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Se a última linha do log no `hibinit-agent` for `hibinit-agent: Running: swapoff /swap`, a hibernação foi configurada com êxito.

Se você não vir nenhum log desses processos, talvez sua AMI não ofereça suporte à hibernação. Para obter informações sobre as AMIs compatíveis, consulte Pré-requisitos para a hibernação de instâncias do Amazon EC2. Se você usou sua própria AMI do Linux, certifique-se de seguir as instruções para Configurar uma AMI para oferecer suporte à hibernação.

Windows Server 2016 e posterior

Verifique o log de execução do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de execução do EC2, conecte-se à instância e abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` em um editor de texto. Se você estiver usando EC2Launch v2, abra `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e os arquivos do EC2, insira o caminho no Windows Explorer ou altere as propriedades da pasta para visualizar os arquivos e as pastas ocultos.

Localize as linhas do log para hibernação. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que a hibernação falhou na configuração: `Message: Failed to enable hibernation.` Se a mensagem de erro incluir valores ASCII decimais, você poderá converter os valores ASCII em texto simples para ler a mensagem de erro completa.

Se a linha do log contiver `HibernationEnabled: true`, a hibernação terá sido configurada com êxito.

Windows Server 2012 R2 e anteriores

Verifique o log de configuração do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de configuração do EC2, conecte-se à instância e abra o arquivo `C:\Program Files \Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` em um editor de texto. Localize as linhas do log para `SetHibernateOnSleep`. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que o volume raiz da instância não é grande o suficiente: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Se a linha do log for `SetHibernateOnSleep: HibernationEnabled: true`, a hibernação terá sido configurada com êxito.

Tamanho da instância do Windows

Se você estiver usando uma instância do Windows T3 ou T3a com menos de 1 GB de RAM, tente aumentar o tamanho da instância para uma que tenha pelo menos 1 GB de RAM.

Instância "presa" no estado de parada

Se você tiver hibernado sua instância e ela aparentar estar "presa" no estado `stopping`, será possível interrompê-la à força. Para ter mais informações, consulte Solução de problemas na interrupção da instância.

Não é possível iniciar a instância spot imediatamente após a hibernação

Se você tentar iniciar uma instância spot até dois minutos após colocá-la em hibernação, poderá receber o seguinte erro:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Aguarde cerca de dois minutos para as instâncias do Linux e cerca de cinco minutos para as instâncias do Windows e tente iniciar a instância novamente.

Falha ao retomar instâncias spot

Se a instância spot foi colocada em hibernação com sucesso, mas não foi possível retomá-la e, em vez disso, ela foi reinicializada (uma nova inicialização em que o estado de hibernação não é retido), talvez os dados do usuário contivessem o seguinte script:

```
/usr/bin/enable-ec2-spot-hibernation
```

Remova esse script do campo Dados de usuário no modelo de inicialização e solicite uma nova instância spot.

Observe que, mesmo havendo falha ao retomar a instância, se o estado de hibernação não for preservado, a instância ainda poderá ser iniciada da mesma forma que aconteceria se ela estivesse no estado `stopped`.

Reinicializar a instância

Reinicializar a instância equivale a reinicializar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reinicializar sua instância.

Quando você reinicializa uma instância, ela mantém o seguinte:

- Nome DNS público (IPv4)
- Endereço IPv4 privado
- Endereço IPv4 público
- Endereço IPv6 (se aplicável)
- Todos os dados em seus volumes de armazenamento de instância

A reinicialização de uma instância não inicia um novo período (com uma cobrança mínima de um minuto) de faturamento de instância, diferentemente do que acontece ao interromper e iniciar a instância.

Nós pudemos programar sua instância para uma reinicialização para manutenção necessária, como para aplicar atualizações que exigem uma reinicialização. Nenhuma ação é necessária da sua parte; recomendamos esperar a reinicialização ocorrer na janela programada. Para ter mais informações, consulte Eventos programados para instâncias.

Recomendamos que você use o console do Amazon EC2 uma ferramenta da linha de comando ou a API do Amazon EC2 para reiniciar sua instância, em vez de executar o comando de reinicialização

do sistema operacional pela sua instância. Se você usar o console do Amazon EC2, uma ferramenta da linha de comando ou a API do Amazon EC2 para reiniciar sua instância, executaremos uma reinicialização forçada se a instância não fechar corretamente em alguns minutos. Se você usar o AWS CloudTrail e, em seguida, usar o Amazon EC2 para reinicializar sua instância também criará um registro de API de quando a instância foi reinicializada.

Instâncias do Windows

Se o Windows está instalando atualizações em sua instância, recomendamos que você não reinicie ou feche sua instância usando o console Amazon EC2 ou a linha de comando até que todas as atualizações estejam instaladas. Ao usar o console ou a linha de comando Amazon EC2 para reinicializar ou fechar sua instância, há risco que sua instância seja reinicializada forçadamente. Uma "hard reboot" enquanto as atualizações estão sendo instaladas poderia colocar suas instâncias em um estado instável.

Console

Para reinicializar uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Instance State (Estado da instância), Reboot instance (Reinicializar a instância).

   Se preferir, selecione a instância e escolha Actions (Ações), Manage instance state (Gerenciar o estado da instância). Na tela que será aberta, escolha Reboot (Reinicializar) e Change state (Alterar estado).
4. Escolha Reboot (Reinicializar) quando a confirmação for solicitada.

   A instância permanecerá no estado `running`.

Command line

Para reinicializar uma instância

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- reboot-instances (AWS CLI)

- Restart-EC2Instance (AWS Tools for Windows PowerShell)

Para executar um experimento controlado de injeção de falha

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é reinicializada. Para obter mais informações, consulte o Guia do usuário do AWS Fault Injection Service.

Encerramento de instâncias do Amazon EC2

É possível excluir sua instância quando não precisar mais dela. Isso é chamado de encerrar sua instância. Assim que o estado de uma instância mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Não é possível conectar-se a uma instância ou iniciá-la depois de interrompê-la. No entanto, é possível executar instâncias adicionais usando a mesma AMI. Se você preferir interromper ou hibernar uma instância, consulte Início e interrupção de instâncias do Amazon EC2 ou Hibernar sua instância do Amazon EC2. Para ter mais informações, consulte Diferenças entre reinicialização, interrupção, hibernação e encerramento.

Conteúdo

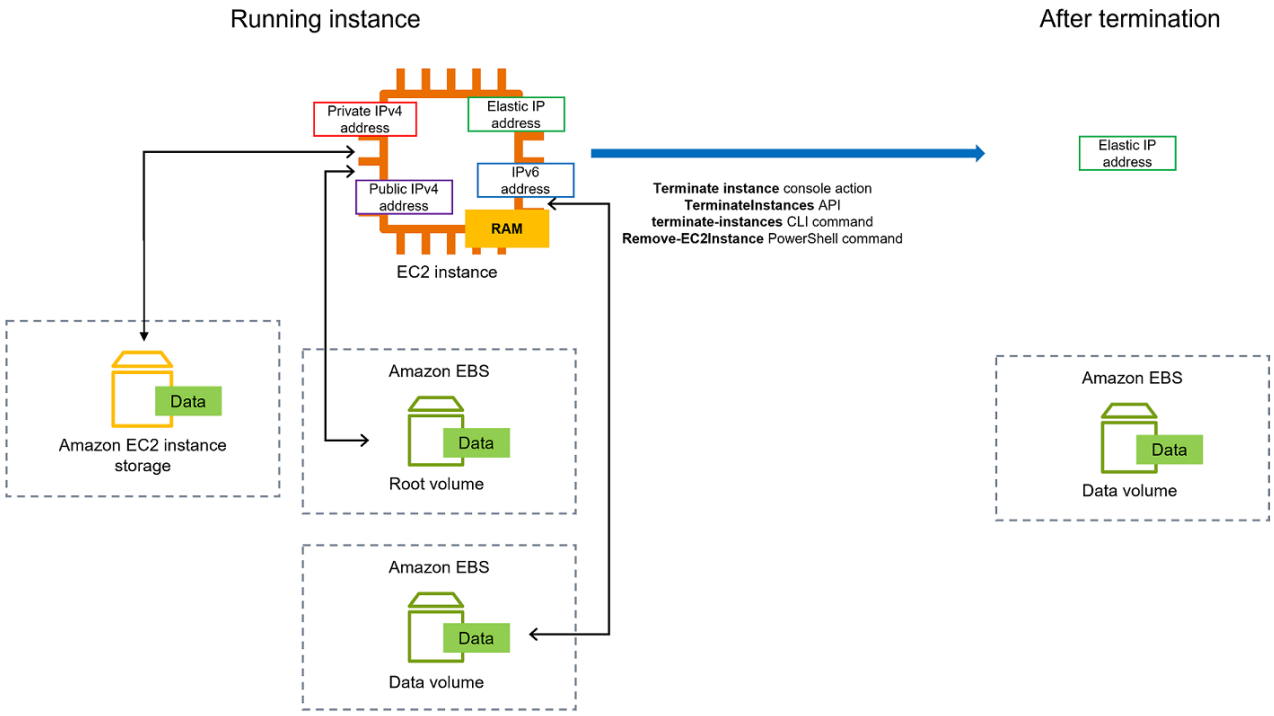
- Como funciona o encerramento de uma instância
- Como encerrar uma instância
- Solucionar problemas de encerramento da instância
- Habilitar a proteção contra encerramento
- Alterar o comportamento de desligamento iniciado da instância
- Preservação de dados quando uma instância for encerrada

Como funciona o encerramento de uma instância

Quando você encerra uma instância, as alterações são registradas no nível do sistema operacional da instância, alguns recursos são perdidos e outros persistem.

O diagrama apresentado a seguir mostra o que é perdido e o que persiste quando uma instância do Amazon EC2 é encerrada. Quando uma instância é encerrada, os dados em quaisquer volumes de armazenamento de instância e os dados armazenados na RAM da instância são apagados. Todos os endereços IP elásticos associados à instância são desanexados. Para os volumes do

Amazon EBS e os dados presentes nesses volumes, o resultado depende da configuração Excluir no encerramento definida para o volume. Por padrão, o volume raiz é excluído e os volumes de dados são preservados.



Considerações

- Quando uma instância é encerrada, os dados em quaisquer volumes de armazenamento de instâncias associados a ela são excluídos.
- Por padrão, os volumes do dispositivo raiz do Amazon EBS são excluídos automaticamente quando a instância é encerrada. Contudo, todos os volumes adicionais do EBS que você anexar na execução ou todos os volumes do EBS que você anexar a uma instância existente persistirão mesmo após o encerramento da instância. Para ter mais informações, consulte Preservação de dados quando uma instância for encerrada.

> **Note**
>
> Todos os volumes que não forem excluídos após o encerramento da instância continuarão incorrendo em cobranças.

- Para evitar que uma instância seja encerrada acidentalmente por alguém, habilite a proteção contra encerramento.

- Para controlar se uma instância é interrompida ou encerrada quando o desligamento é iniciado usando a instância, altere o comportamento de desligamento iniciado pela instância.
- Se você executar um script no encerramento da instância, ela pode ter uma interrupção anormal, pois não há como garantir que os scripts de desativação sejam executados. O Amazon EC2 tenta desativar uma instância corretamente e executar quaisquer scripts de desativação do sistema. No entanto, determinados eventos (como falha de hardware) podem impedir que esses scripts de desativação do sistema sejam executados.

O que acontece quando você encerra uma instância

Alterações registradas no nível do sistema operacional

- A solicitação da API envia um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema são interrompidos como resultado do evento de pressionamento de botão. O desligamento normal do sistema é fornecido pelo systemd (Linux) ou pelo processo do sistema (Windows). O desligamento normal é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.
- O desligamento de ACPI é iniciado.
- A instância será encerrada após o término do processo de desligamento normal. Não existe um tempo de desligamento configurável para o SO. A instância permanece visível no console por um curto período e depois a entrada é excluída automaticamente.

Recursos perdidos

- Dados armazenados no volume de um armazenamento de instância.
- Dados armazenados nos volumes raiz do dispositivo do Amazon EBS se o atributo `DeleteOnTermination` estiver definido como verdadeiro.

Recursos que persistem

- Dados armazenados em volumes adicionais do Amazon EBS anexados no momento da execução ou após a execução de uma instância.

Teste da resposta da aplicação ao encerramento da instância

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é encerrada. Para obter mais informações, consulte o Guia do usuário do AWS Fault Injection Service.

Como encerrar uma instância

É possível encerrar uma instância a qualquer momento.

Console

Para encerrar uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).
5. Após encerrar uma instância, ela permanecerá visível por um breve período, com um estado de `terminated`.

   Se o encerramento apresentar falhas ou se uma instância encerrada permanecer visível por mais do que algumas horas, consulte Instância encerrada ainda sendo exibida.

Command line

Para encerrar uma instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- terminate-instances (AWS CLI)
- Remove-EC2Instance (AWS Tools for Windows PowerShell)

Solucionar problemas de encerramento da instância

O solicitante deve ter permissão para chamar `ec2:TerminateInstances`. Para obter mais informações, consulte Exemplos de políticas para trabalhar com instâncias.

Se você encerrar a instância e outra instância for iniciada, provavelmente você configurou a escalabilidade automática por meio de um recurso como o Frota do EC2 ou o Amazon EC2 Auto Scaling. Para ter mais informações, consulte Instâncias executadas ou encerradas automaticamente.

Não será possível encerrar uma instância se a proteção contra encerramento estiver ativada. Para obter mais informações, consulte proteção contra encerramento.

Se a instância permanecer no estado `shutting-down` por mais tempo do que o normal, ela será removida (encerrada) por processos automatizados no serviço do Amazon EC2. Para ter mais informações, consulte Encerramento atrasado da instância.

Habilitar a proteção contra encerramento

Para impedir que a instância seja encerrada acidentalmente, você pode habilitar a proteção contra encerramento da instância. O atributo `DisableApiTermination` controla se a instância pode ser encerrada usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API. Por padrão, a proteção contra encerramento está desabilitada para a instância, o que significa que ela pode ser encerrada usando o AWS Management Console, a AWS CLI ou a API. É possível definir o valor desse atributo ao executar uma instância, enquanto a instância estiver em execução ou quando ela for interrompida (para instâncias baseadas no Amazon EBS).

O atributo `DisableApiTermination` não impede que você encerre uma instância iniciando o desligamento nela (usando um comando do sistema operacional para o desligamento do sistema) quando o atributo `InstanceInitiatedShutdownBehavior` é definido. Para ter mais informações, consulte Alterar o comportamento de desligamento iniciado da instância.

Considerações

- Habilitar a proteção contra encerramento não impede que a AWS encerre a instância quando há um evento programado para encerrá-la.
- Habilitar a proteção contra encerramento não impede que Amazon EC2 Auto Scaling encerre uma instância quando ela não estiver íntegra ou durante eventos de redução horizontal da escala. É possível controlar se um grupo do Auto Scaling pode encerrar uma instância específica ao escalar usando a proteção contra redução horizontal da escala da instância. É possível controlar se um grupo do Auto Scaling pode encerrar instâncias não íntegras suspendendo o processo de escala ReplaceUnhealthy.
- Você não pode habilitar a proteção contra encerramento para Instâncias spot.

Para habilitar a proteção contra encerramento de uma instância no momento da execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Launch Instance (Executar instância) e siga as instruções contidas no assistente.
3. Na página Configure Instance Details (Configurar detalhes da instância), marque a caixa de seleção Enable termination protection (Habilitar proteção contra encerramento).

Para habilitar a proteção contra encerramento de uma instância em execução ou interrompida

1. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change Termination Protection (Alterar proteção contra interrupção).
2. Escolha Yes, Enable (Sim, habilitar).

Para desabilitar a proteção contra encerramento de uma instância em execução ou interrompida

1. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change Termination Protection (Alterar proteção contra interrupção).
2. Escolha Yes, Disable (Sim, desabilitar).

Para habilitar ou desabilitar a proteção contra encerramento usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Encerramento de múltiplas instâncias com proteção contra encerramento

Se você encerrar múltiplas instâncias em diversas zonas de disponibilidade usando a mesma solicitação e uma ou mais das instâncias especificadas estiverem habilitadas para a proteção contra encerramento, a solicitação falhará e apresentará os seguintes resultados:

- As instâncias especificadas que estão na mesma zona de disponibilidade que a instância protegida não estão terminadas.

- As instâncias especificadas que estão em zonas de disponibilidade diferentes, em que nenhuma outra instância especificada está protegida, estão terminadas corretamente.

Exemplo

Suponha que você tenha as quatro instâncias apresentadas a seguir em duas zonas de disponibilidade.

Instância	Availability Zone	Encerrar proteção
Instância 1	AZ A	`Disabled`
Instância 2		`Disabled`
Instância 3	AZ B	`Enabled`
Instância 4		`Disabled`

Se você tentar terminar todas essas instâncias na mesma solicitação, a solicitação relatará falha com os seguintes resultados:

- A Instância 1 e a Instância 2 foram encerradas com êxito porque nenhuma das instâncias está habilitada para a proteção contra encerramento.
- A Instância 3 e a Instância 4 não são encerradas porque a Instância 3 está habilitada para a proteção contra encerramento.

Alterar o comportamento de desligamento iniciado da instância

Por padrão, ao iniciar um desligamento de uma instância baseada no Amazon EBS (usando comandos como shutdown ou poweroff), a instância será interrompida. É possível alterar esse comportamento usando o atributo `InstanceInitiatedShutdownBehavior` para a instância de forma que, em vez de ser desligada, ela seja encerrada. É possível atualizar esse atributo enquanto a instância estiver sendo executada ou interrompida.

O comando halt não inicia um desligamento. Se ele for usado, a instância não será encerrada. Em vez disso, ele colocará a CPU em `HLT` e a instância permanecerá em execução.

> **Note**
>
> O `InstanceInitiatedShutdownBehavior` atributo só se aplica quando você executa um desligamento a partir do sistema operacional da instância em si. Ele não se aplica quando você interrompe uma instância usando a API `StopInstances` ou o console do Amazon EC2.

É possível atualizar o atributo `InstanceInitiatedShutdownBehavior` usando o console do Amazon EC2 ou a linha de comando.

Console

Alterar o comportamento de desligamento iniciado da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Actions (Ações), Instance settings (Configurações da instância), Change shutdown behavior (Alterar comportamento de desativação).

   O comportamento de desligamento exibe o comportamento atual.
5. Para alterar o comportamento, em Comportamento de desligamento, selecione Interromper ou Encerrar.
6. Escolha Salvar.

Command line

Alterar o comportamento de desligamento iniciado da instância

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Preservação de dados quando uma instância for encerrada

Dependendo do seu caso de uso, talvez você queira preservar os dados no volume de armazenamento de instância ou no volume do Amazon EBS quando a instância do Amazon EC2 for encerrada. Os dados em um volume de armazenamento de instância não persistem quando uma instância é encerrada. Se precisar preservar os dados armazenados em um volume de armazenamento de instância além da vida útil da instância, você precisará copiar manualmente esses dados para um armazenamento mais persistente, como um volume do Amazon EBS, um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS. Para ter mais informações, consulte Opções de armazenamento para as instâncias do Amazon EC2.

Para os dados nos volumes do Amazon EBS, o Amazon EC2 usa o valor do atributo `DeleteOnTermination` para cada volume do Amazon EBS anexado a fim de determinar se o volume será preservado ou excluído.

O valor padrão do atributo `DeleteOnTermination` difere dependendo de se o volume é o volume raiz da instância ou um volume não raiz anexado à instância.

Volume raiz

Por padrão, quando você inicia uma instância, o atributo `DeleteOnTermination` para o volume raiz de uma instância é definido como `true`. Portanto, o padrão é excluir o volume raiz da instância quando a instância é encerrada.

Volume não raiz

Por padrão, quando um volume do EBS não raiz é associado a uma instância, seu atributo `DeleteOnTermination` é definido como `false`. Portanto, o padrão é preservar esses volumes.

> **Note**
>
> Depois que a instância é encerrada, é possível criar uma snapshot do volume preservado ou anexá-lo a outra instância. Exclua um volume para evitar cobranças adicionais.

O atributo `DeleteOnTermination` pode ser definido pelo criador de uma AMI, bem como pela pessoa que executa a instância. Quando o atributo é alterado pelo criador de uma AMI ou pela pessoa que executa uma instância, a nova configuração substitui a configuração padrão original da AMI. Recomendamos que você verifique a configuração padrão do atributo `DeleteOnTermination` após executar uma instância com uma AMI.

Para verificar se um volume do Amazon EBS será excluído no encerramento da instância, visualize os detalhes do volume no painel de detalhes da instância. Na guia Armazenamento, em Dispositivos de blocos, role para a direita para ver a configuração Excluir no encerramento para o volume.

- Se Sim, o volume será excluído quando a instância for encerrada.
- Se Não, o volume não será excluído quando a instância for encerrada. Todos os volumes que não forem excluídos após o encerramento da instância continuarão incorrendo em cobranças.

Alteração do volume raiz para persistir na inicialização

Usando o console, é possível alterar o atributo `DeleteOnTermination` quando executar uma instância. Para alterar esse atributo para uma instância em execução, use a linha de comando.

Use um dos métodos a seguir para alterar o volume raiz a ser mantido na execução.

Console

Para alterar o volume raiz de uma instância a ser mantido na execução usando o console

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para alterar o volume raiz a ser mantido.
2. Em Armazenamento (volumes), expanda as informações sob o volume raiz.
3. Em Excluir no encerramento, escolha Não.
4. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Command line

Para alterar o volume raiz de uma instância a ser mantido na execução usando a linha de comando

Ao executar uma instância baseada no EBS, é possível usar um dos seguintes comandos para alterar o volume do dispositivo raiz a ser mantido. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Nos mapeamentos de dispositivos de blocos para os volumes que você deseja persistir, inclua `--DeleteOnTermination` e especifique `false`.

Por exemplo, para persistir um volume, adicione a opção a seguir ao comando `run-instances`:

```
--block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `--DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Alteração do volume raiz de uma instância em execução para persistir

É possível usar um dos seguintes comandos para alterar o volume do dispositivo raiz de uma instância baseada no EBS em execução a ser mantido. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Por exemplo, use o comando a seguir:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `--DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
```

```
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Desativação da instância

A instância é programada para ser desativada quando a AWS detecta uma falha irreparável do hardware subjacente que hospeda a instância. O dispositivo raiz da instância determina o comportamento da desativação da instância:

- Se o dispositivo raiz da instância estiver em um volume do Amazon EBS, a instância será interrompida e será possível reiniciá-la a qualquer momento. Iniciar a instância interrompida migra-a para o novo hardware.
- Se o dispositivo raiz da instância for um volume de armazenamento de instâncias, a instância será encerrada e não poderá ser usada novamente.

Para obter mais informações sobre os tipos de eventos de instância, consulte Eventos programados para instâncias.

Tópicos

- Identificar instâncias programadas para desativação
- Ações a serem executadas para instâncias baseadas em EBS programadas para desativação
- Ações a serem executadas para instâncias com armazenamento de instâncias programadas para desativação

Identificar instâncias programadas para desativação

Se a sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância. Também é possível verificar se há instâncias programadas para desativação usando o console do Amazon EC2 ou a linha de comando.

> **Important**
>
> Se uma instância estiver programada para desativação, recomendamos que você aja o mais rápido possível, pois a instância poderá ficar inacessível. (A notificação por e-mail

que você recebe indica o seguinte: “Devido a essa degradação, sua instância já pode estar inacessível.”) Para obter mais informações sobre a ação recomendada que é necessário executar, consulte Check if your instance is reachable.

Formas de identificar instâncias programadas para desativação

- Notificação por e-mail
- Identificação do console

Notificação por e-mail

Se a sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância.

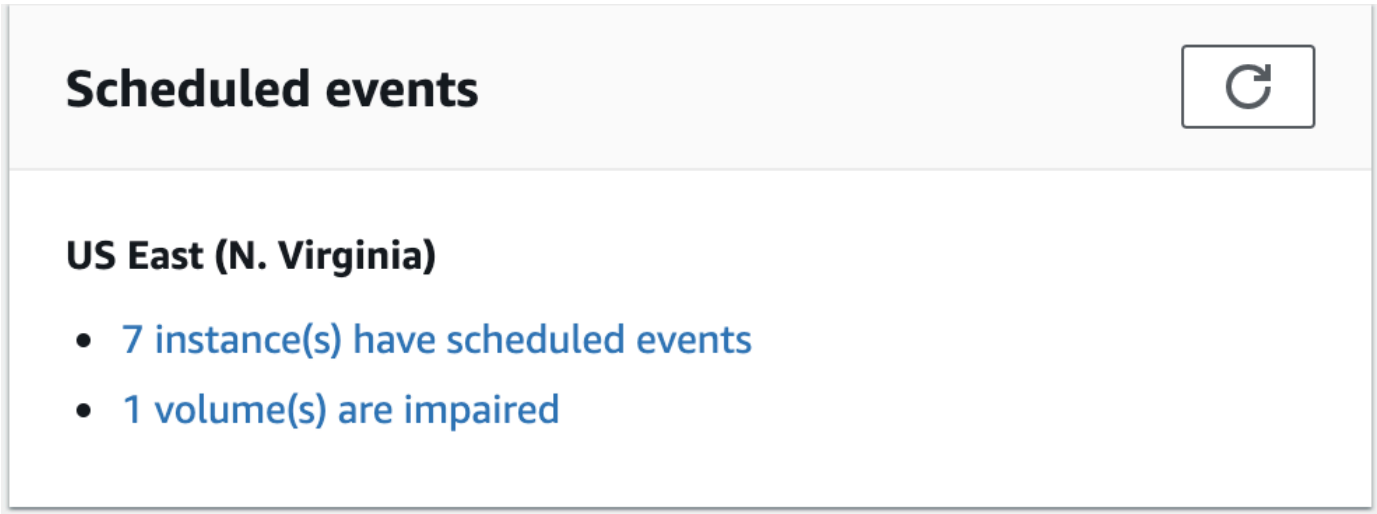
O e-mail é enviado ao titular da conta principal e ao contato de operações. Para obter mais informações, consulte Adição, alteração ou remoção de contatos alternativos no Guia do usuário do AWS Billing.

Identificação do console

Se você usa uma conta de e-mail que não verifica regularmente, por exemplo, notificações de desativação, use o console do Amazon EC2 ou a linha de comando para determinar se alguma de suas instâncias estão programadas para desativação.

Para identificar as instâncias agendadas para desativação usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2). Em Scheduled events (Eventos agendados), é possível ver os eventos associados a volumes e instâncias do Amazon EC2, organizados por região.



3. Se você tiver uma instância com um evento agendado listado, selecione o link abaixo do nome da região para acessar a página Events (Eventos).
4. A página Events (Eventos) lista todos os recursos com eventos associados a eles. Para visualizar as instâncias que estão agendadas para desativação, selecione Instance resources (Recursos da instância) na primeira lista de filtros e, em seguida, Instance stop or retirement (Interrupção ou desativação de instância) na segunda lista de filtros.
5. Se os resultados do filtro mostrarem que uma instância está agendada para desativação, selecione-a e anote a data e a hora do campo Start time (Hora de início) no painel de detalhes. Essa é a data de desativação da instância.

Para identificar as instâncias agendadas para desativação usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-instance-status (AWS CLI)
- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)

Ações a serem executadas para instâncias baseadas em EBS programadas para desativação

Para preservar os dados em sua instância sendo desativada, é possível executar uma das ações a seguir. É importante que você execute essa ação antes da data de desativação da instância, para evitar períodos de desativação e perda de dados imprevistos.

Para instâncias do Linux, se você não tiver certeza se a instância é baseada no EBS ou no armazenamento de instâncias, consulte Determinação do tipo de dispositivo raiz da instância do Linux.

Verifique se sua instância está acessível

Quando você for notificado de que sua instância está programada para desativação, recomendamos que execute a seguinte ação o mais rápido possível:

- Verifique se sua instância está acessível conectando-se ou fazendo ping na instância.
- Se sua instância estiver acessível, planeje interromper/iniciar a instância em um momento apropriado antes da data de desativação programada, quando o impacto for mínimo. Para obter mais informações sobre como interromper e iniciar sua instância e o que esperar quando a instância é interrompida, como o efeito em endereços IP elásticos, públicos e privados associados à instância, consulte Início e interrupção de instâncias do Amazon EC2. Observe que os dados em volumes de armazenamento de instâncias são perdidos quando você interrompe e inicia sua instância.
- Se sua instância estiver inacessível, você deverá agir imediatamente e executar uma interrupção/inicialização para recuperar sua instância.
- Se preferir encerrar sua instância, planeje fazê-lo o mais rápido possível, para que você pare de receber cobranças pela instância.

Crie um backup da sua instância

Crie uma AMI baseada em EBS em sua instância para que você tenha um backup. Para garantir a integridade dos dados, interrompa a instância antes de criar a AMI. Espere a data de desativação agendada para a interrupção da instância ou interrompa a instância por conta própria antes dessa data. É possível iniciar a instância novamente a qualquer momento. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Execute uma instância de substituição

Depois de criar uma AMI a partir da sua instância, é possível usar a AMI para iniciar uma instância de substituição. No console do Amazon EC2, selecione sua nova AMI e escolha Iniciar instância a partir da AMI. Configure os parâmetros da sua instância e escolha Iniciar instância. Para obter mais informações sobre cada campo, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Ações a serem executadas para instâncias com armazenamento de instâncias programadas para desativação

Para preservar os dados em sua instância sendo desativada, é possível executar uma das ações a seguir. É importante que você execute essa ação antes da data de desativação da instância, para evitar períodos de desativação e perda de dados imprevistos.

> **Warning**
>
> Se a sua instância baseada em armazenamento de instâncias passar de sua data de desativação, ela será encerrada e você não poderá recuperar a instância nem os dados que foram armazenados nela. Independentemente do dispositivo raiz de sua instância, os dados em volumes de armazenamento de instâncias são perdidos quando a instância é desativada, mesmo que os volumes estejam anexados a uma instância baseada no EBS.

Verifique se sua instância está acessível

Quando você for notificado de que sua instância está programada para desativação, recomendamos que execute a seguinte ação o mais rápido possível:

- Verifique se sua instância está acessível conectando-se ou fazendo ping na instância.
- Se sua instância estiver inacessível, é provável que haja muito pouco que possa ser feito para recuperá-la. Para obter mais informações, consulte Solucionar problemas de uma instância não acessível. A AWS encerrará a instância na data de desativação programada, portanto, para uma instância inacessível, é possível encerrar a instância por conta própria.

Execute uma instância de substituição

Crie uma AMI com armazenamento de instâncias a partir da sua instância usando as ferramentas da AMI, conforme descrito em Criar uma AMI em Linux com armazenamento de instâncias. No console do Amazon EC2, selecione sua nova AMI e escolha Iniciar instância a partir da AMI. Configure os parâmetros da sua instância e escolha Iniciar instância. Para obter mais informações sobre cada campo, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Converta sua instância em uma instância baseada em EBS

Transfira seus dados para um volume do EBS, obtenha um snapshot do volume e crie a AMI a partir do snapshot. É possível executar uma instância de substituição a partir da nova AMI. Para ter mais informações, consulte Converter de uma AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS.

Resiliência de instância

> **Important**
>
> As informações a seguir se aplicam à configuração de recursos relacionados à recuperação em instâncias íntegras. Se você está enfrentando dificuldades para acessar sua instância, consulte Solucionar problemas de instâncias do EC2.

Caso a AWS determine que uma instância não está disponível devido a um problema de hardware subjacente, há dois mecanismos que você pode configurar para cada resiliência de instância que pode restaurar a disponibilidade: recuperação automática simplificada e recuperação baseada em ações do Amazon CloudWatch. Esse processo é chamado de recuperação de instâncias.

Pelo menos um mecanismo deve ser configurado ou habilitado com antecedência com recursos compatíveis para que o processo de recuperação da instância ocorra. Por padrão, a recuperação automática simplificada é habilitada para instâncias compatíveis quando elas são iniciadas.

Tópicos

- Visão geral da recuperação de instância
- Alternativas à recuperação de instância
- Configurar a recuperação baseada em ação do CloudWatch
- Configurar a recuperação automática simplificada

Visão geral da recuperação de instância

Veja a seguir exemplos de problemas de hardware subjacentes que podem exigir a recuperação de instância:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico

- Problemas de hardware de host físico que afetam a acessibilidade de rede

Uma instância recuperada é idêntica à instância original incluindo:

- ID da instância
- seus endereços IP públicos, privados e elásticos;
- Metadados da instância
- Grupo de posicionamento
- volumes do EBS associados.
- Availability Zone (zona de disponibilidade)

Uma recuperação de instância bem-sucedida aparecerá para a instância como uma reinicialização não planejada. Em outras palavras, o conteúdo armazenado na memória volátil será perdido, os dados do armazenamento de instâncias serão apagados e o tempo de atividade do sistema operacional recomeçará do zero.

Para ajudar a se proteger contra a perda de dados, recomendamos que você crie regularmente backups de dados importantes. Para obter mais informações sobre as melhores práticas de backup e recuperação para instâncias do Amazon EC2, consulte Melhores práticas do Amazon EC2.

Alternativas à recuperação de instância

As seguintes alternativas para recuperação de instâncias podem ser consideradas quando atendem ao caso de uso de suas instâncias.

Grupos do Auto Scaling

Você pode usar grupos do Auto Scaling para permitir agrupar um conjunto de instâncias para fins de escalabilidade e disponibilidade. Caso uma instância dentro de um grupo do Auto Scaling fique indisponível, a instância será automaticamente substituída (não recuperada) pelo grupo do Auto Scaling. Para obter mais informações, consulte O que é o Amazon EC2 Auto Scaling? no Guia do usuário do Amazon EC2 Auto Scaling.

Amazon EBS Multi-Attach

Você pode configurar o Amazon EBS Multi-Attach para suas instâncias para permitir que várias instâncias sejam conectadas ao mesmo volume do EBS. Quando combinado com o software apropriado, isso permite que o clustering de alta disponibilidade seja ativado. Para ver um

exemplo de configuração com instâncias do Linux, consulte Clustered storage simplified: GFS2 on Amazon EBS Multi-Attach enabled volumes no AWS Storage Blog.

Configurar a recuperação baseada em ação do CloudWatch

Important

- As informações a seguir se aplicam à configuração de recursos relacionados à recuperação em instâncias íntegras. Se você está enfrentando dificuldades para acessar sua instância, consulte Solucionar problemas de instâncias do EC2.
- Para que sua workload funcione adequadamente após uma recuperação bem-sucedida da instância, sua instância deve inicializar e aceitar o tráfego sem exigir intervenção manual.

Você pode configurar a recuperação baseada em ações do Amazon CloudWatch para adicionar ações de recuperação aos alarmes do Amazon CloudWatch. A recuperação baseada em ações do CloudWatch funciona com a métrica `StatusCheckFailed_System`. A recuperação baseada em ações do CloudWatch fornece granularidade de tempo de resposta de recuperação a cada minuto e notificações do Amazon Simple Notification Service (Amazon SNS) sobre as ações e os resultados da recuperação. Essas opções de configuração permitem tentativas de recuperação mais rápidas com controle mais granular sobre a resposta do evento de falha na verificação de status do sistema em comparação com a recuperação automática simplificada. Para obter mais informações sobre as opções disponíveis do CloudWatch, consulte Verificações de status para as instâncias.

A recuperação baseada em ações do Amazon CloudWatch não opera durante eventos de serviço no AWS Health Dashboard. Para ter mais informações, consulte the section called “Solucionar problemas de falha de recuperação baseada em ações do CloudWatch”.

Tópicos

- Requisitos e limitações da recuperação baseada em ações do CloudWatch
- Configurar a recuperação baseada em ação do CloudWatch
- Solucionar problemas de falha de recuperação baseada em ações do CloudWatch

Requisitos e limitações da recuperação baseada em ações do CloudWatch

A recuperação baseada em ações do CloudWatch poderá tentar recuperar uma instância se:

- Estiver no estado `running`. Para ter mais informações, consulte the section called “Ciclo de vida da instância”.
- Ela usar `default` (sob demanda) ou locação de instâncias `dedicated`. Para ter mais informações, consulte the section called “Opções de compra de instância”.
- For do tipo de instância para o qual o Amazon EC2 tem capacidade disponível. Em algumas situações, como interrupções significativas, não haverá capacidade suficiente, e algumas tentativas de recuperação poderão falhar.
- Não usa locação de instâncias `dedicated`. Nos hosts dedicados do Amazon EC2, você pode usar a Recuperação automática de host dedicado para recuperar automaticamente as instâncias que não estão íntegras.
- Não usa um Elastic Fabric Adaptor.
- Não é um membro de um grupo do Auto Scaling.
- No momento, não está passando por um evento de manutenção programado.
- Usa um dos seguintes tipos de instância:
  - Uso geral: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Otimizadas para computação: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-flex
  - Otimizadas para memória: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iezn
  - Computação acelerada: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Computação de alta performance: Hpc6a | Hpc7a | Hpc7g
  - Instâncias de metal: qualquer um dos tipos acima com o tamanho da instância de metal.
- Tem volumes de armazenamento de instância e usa um dos seguintes tipos de instância: M3 | C3 | R3 | X1 | X1e | X2idn | X2iedn

> **Warning**
>
> - Os dados nos volumes de armazenamento de instância serão perdidos quando a instância for interrompida. Para obter mais informações sobre como interromper uma instância, consulte the section called “Início e interrupção da instância”.

- No caso de uma falha na verificação do status do sistema, os dados de armazenamento de instância e mapeamento de dispositivos de blocos podem ser perdidos. Para esses tipos de instância, você pode considerar usar the section called “Habilitar a proteção contra encerramento”.

Recomendamos que você crie regularmente backups de dados importantes. Para obter informações sobre as melhores práticas de backup e recuperação do Amazon EC2, consulte Melhores práticas do Amazon EC2.

Também é possível usar o AWS Management Console ou a AWS CLI para visualizar os tipos de instância compatíveis com a recuperação baseada em ação do CloudWatch.

Console

Como visualizar os tipos de instância que oferecem suporte à recuperação baseada em ação do Amazon CloudWatch

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Na barra de filtros, insira Auto Recovery support: true (Suporte para Recuperação Automática: true). Como alternativa, à medida que você insere os caracteres e o nome do filtro aparece, é possível selecioná-lo.

   A tabela de tipos de instância exibe todos os tipos de instância que oferecem suporte à recuperação baseada em ação do Amazon CloudWatch.

AWS CLI

Como visualizar os tipos de instância que oferecem suporte à recuperação baseada em ação do Amazon CloudWatch

Use o comando describe-instance-types.

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Configurar a recuperação baseada em ação do CloudWatch

A recuperação baseada em ações do CloudWatch funciona com a métrica `StatusCheckFailed_System`. A recuperação baseada em ações do CloudWatch é configurada no console do CloudWatch. Para configurar a recuperação baseada em ações do CloudWatch, consulte Adding recover actions to CloudWatch alarms no Guia do usuário do Amazon CloudWatch.

Solucionar problemas de falha de recuperação baseada em ações do CloudWatch

Os problemas a seguir podem fazer com que a recuperação da instância com uma recuperação baseada em ações do CloudWatch falhe:

- A recuperação baseada em ações do CloudWatch não opera durante eventos de serviço no AWS Health Dashboard. Talvez você não receba notificações de falha de recuperação para esses eventos. Para obter as informações mais recentes sobre a disponibilidade do serviço, consulte a página status do serviço.
- Capacidade temporária e insuficiente do hardware de substituição.
- A instância alcançou a franquia diária máxima de tentativas de recuperação. Sua instância poderá ser subsequentemente retirada se a recuperação automática falhar e se for determinado que a degradação do hardware é a causa-raiz da falha de verificação do status do sistema original.

Se a falha na verificação de status do sistema da instância persistir apesar de várias tentativas de recuperação, consulte Solução de problemas em instâncias com falha nas verificações de status para obter mais informações.

Configurar a recuperação automática simplificada

> **Important**
>
> - As informações a seguir se aplicam à configuração de recursos relacionados à recuperação em instâncias íntegras. Se você está enfrentando dificuldades para acessar sua instância, consulte Solucionar problemas de instâncias do EC2.
> - Para que sua workload funcione adequadamente após uma recuperação bem-sucedida da instância, sua instância deve inicializar e aceitar o tráfego sem exigir intervenção manual.

Por padrão, a recuperação automática simplificada monitora todas as instâncias em execução suportadas. Caso seja detectada uma falha na verificação do status do sistema, a recuperação

automática simplificada tenta corrigir a instância para um estado íntegro. A recuperação automática simplificada não opera durante eventos de serviço no AWS Health Dashboard. Para ter mais informações, consulte the section called “Solução de problemas de falhas de recuperação automática simplificada”.

Quando ocorrer um evento de recuperação automática simplificado, você receberá um evento AWS Health Dashboard. Para configurar notificações para esses eventos, consulte Conceitos básicos do Notificações de Usuários da AWS no Guia do usuário do Notificações de Usuários da AWS. Você também pode usar as regras do Amazon EventBridge para monitorar eventos de recuperação automática simplificados usando os seguintes códigos de evento:

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`: eventos com êxito
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`: eventos com falha

Para obter mais informações, consulte as regras do Amazon EventBridge.

Tópicos

- Requisitos e limitações de uma recuperação automática simplificada
- Configurar a recuperação automática simplificada
- Solução de problemas de falhas de recuperação automática simplificada

Requisitos e limitações de uma recuperação automática simplificada

A recuperação automática simplificada tentará recuperar uma instância se:

- Estiver no estado `running`. Para ter mais informações, consulte the section called “Ciclo de vida da instância”.
- Usar locação `default` (sob demanda) ou `dedicated`. Para ter mais informações, consulte the section called “Opções de compra de instância”.
- For do tipo de instância para o qual o Amazon EC2 tem capacidade disponível. Em algumas situações, como interrupções significativas, não haverá capacidade suficiente, e algumas tentativas de recuperação poderão falhar.
- Não usar locação `host`. Nos hosts dedicados do Amazon EC2, você pode usar a Recuperação automática de host dedicado para recuperar automaticamente as instâncias que não estão íntegras.
- Não usa um Elastic Fabric Adaptor.

- Não é o tamanho da instância `metal`.
- Não é um membro de um grupo do Auto Scaling.
- No momento, não está passando por um evento de manutenção programado.
- Não tem volumes de armazenamento de instância.
- Usa um dos seguintes tipos de instância:
  - Uso geral: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Otimizadas para computação: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-flex
  - Otimizadas para memória: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7in-16tb | u7in-24tb | u7in-32tb | X1 | X1e | X2iezn
  - Computação acelerada: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Computação de alta performance: Hpc6a | Hpc7a | Hpc7g

> **Warning**
>
> - Os dados nos volumes de armazenamento de instância serão perdidos quando a instância for interrompida. Para obter mais informações sobre como interromper uma instância, consulte the section called “Início e interrupção da instância”.
> - No caso de uma falha na verificação do status do sistema, os dados de armazenamento de instância e mapeamento de dispositivos de blocos podem ser perdidos. Para esses tipos de instância, você pode considerar usar the section called “Habilitar a proteção contra encerramento”.
>
> Recomendamos que você crie regularmente backups de dados importantes. Para obter informações sobre as melhores práticas de backup e recuperação do Amazon EC2, consulte Melhores práticas do Amazon EC2.

Configurar a recuperação automática simplificada

A recuperação automática simplificada é ativada por padrão quando você executa uma instância compatível. É possível definir o comportamento de recuperação automática como `disabled` durante

ou após a inicialização da instância. A configuração `default` não habilita a recuperação automática simplificada para um tipo de instância não compatível.

Console

Para desabilitar a recuperação automática simplificada na inicialização da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e Launch Instance (Iniciar instância).
3. Na seção Advanced details (Detalhes avançados), em Instance auto-recovery (Recuperação automática de instâncias), selecione Disabled (Desabilitado).
4. Defina as configurações de execução da instância restantes conforme necessário e, em seguida, inicie a instância.

Para desabilitar a recuperação automática simplificada de uma instância em execução ou interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change auto-recovery Behavior (Alterar o comportamento da recuperação automática).
4. Escolha Off (Desativar) e, em seguida, escolha Save (Salvar).

Para definir o comportamento de recuperação automática como **`default`** para uma instância em execução ou interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change auto-recovery Behavior (Alterar o comportamento da recuperação automática).
4. Escolha Padrão e depois Save (Salvar).

AWS CLI

Para desabilitar a recuperação automática simplificada na inicialização

Use o comando run-instances.

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
  [...]
```

Para desabilitar a recuperação automática simplificada de uma instância em execução ou interrompida

Use o comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

Para definir o comportamento de recuperação automática como **`default`** para uma instância em execução ou interrompida

Use o comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery default
```

Solução de problemas de falhas de recuperação automática simplificada

Os problemas a seguir podem fazer com que a recuperação automática simplificada da sua instância falhe:

- A recuperação automática simplificada não opera durante eventos de serviço no AWS Health Dashboard. Talvez você não receba notificações de falha de recuperação para esses eventos. Para obter as informações mais recentes sobre a disponibilidade do serviço, consulte a página de status do serviço.

- Capacidade temporária e insuficiente do hardware de substituição.
- A instância alcançou a franquia diária máxima de tentativas de recuperação. Sua instância poderá ser subsequentemente retirada se a recuperação automática falhar e se for determinado que a degradação do hardware é a causa-raiz da falha de verificação do status do sistema original.

Se a falha na verificação de status do sistema da instância persistir apesar de várias tentativas de recuperação, consulte Solução de problemas em instâncias com falha nas verificações de status para obter mais informações.

Trabalhar com metadados de instância

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução. Os metadados de instância são divididos em categorias, por exemplo, nome do host, eventos e grupos de segurança.

Também é possível usar os metadados da instância para acessar os dados do usuário que você especificou ao executar sua instância. Por exemplo, é possível especificar parâmetros para configurar a instância ou incluir um script simples. Além disso, é possível criar AMIs genéricas e usar dados do usuário para modificar os arquivos de configuração fornecidos no momento da inicialização. Por exemplo, se você executar servidores Web para diversas pequenas empresas, todos eles poderão usar a mesma AMI genérica e recuperar o conteúdo de um bucket do Amazon S3 especificado nos dados do usuário na inicialização. Para adicionar um novo cliente a qualquer momento, crie um bucket para o cliente, adicione seu conteúdo e inicie a AMI com o nome exclusivo do bucket fornecido ao código nos dados do usuário. Se você executar várias instâncias usando a mesma chamada `RunInstances`, os dados do usuário estarão disponíveis para todas as instâncias nessa reserva. Cada instância que integra a mesma reserva tem um número de `ami-launch-index` exclusivo, permitindo que você escreva código que controle o que as instâncias farão. Por exemplo, o primeiro host pode se eleger como o nó original em um cluster. Para obter um exemplo detalhado de inicialização da AMI, consulte Exemplo do Linux: valor do índice de execução da AMI.

As instâncias do EC2 também podem incluir dados dinâmicos, como um documento de identidade de instância que é gerado quando a instância é executada. Para ter mais informações, consulte Categorias de dados dinâmicos.

> **Important**
>
> Embora você só possa acessar os metadados de instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por autenticação ou métodos

de criptografia. Qualquer usuário que tenha acesso direto à instância e, potencialmente, qualquer software em execução na instância, pode visualizar seus metadados. Portanto, você não deve armazenar dados confidenciais, como senhas ou chaves de criptografia de longa duração, como dados de usuário.

Conteúdo

- Usar IMDSv2
- Configurar as opções de metadados da instância
- Recuperar metadados da instância
- Trabalhar com dados do usuário da instância
- Execução de comandos na instância do Amazon EC2 na inicialização
- Recuperar dados dinâmicos da sua instância
- Categorias de metadados da instância
- Exemplo do Linux: valor do índice de execução da AMI
- Documentos de identidade da instância
- Perfis de identidade da instância

Usar IMDSv2

É possível acessar metadados de instância em uma instância em execução usando um dos seguintes métodos:

- Serviço de metadados da instância versão 1 (IMDSv1) – um método de solicitação/resposta
- Serviço de metadados da instância versão 2 (IMDSv2) – um método orientado a sessões

Por padrão, você pode usar o IMDSv1 ou o IMDSv2 ou ambos.

É possível configurar o Serviço de metadados de instância (IMDS) em cada instância de modo que o código ou os usuários locais devam usar o IMDSv2. Quando você especifica que o IMDSv2 deve ser usado, o IMDSv1 não funciona mais. Para obter informações sobre como configurar sua instância para usar o IMDSv2, consulte Configurar as opções de metadados da instância.

Os cabeçalhos PUT ou GET são exclusivos do IMDSv2. Se esses cabeçalhos estiverem presentes na solicitação, a solicitação será destinada ao IMDSv2. Se nenhum cabeçalho estiver presente, presume-se que a solicitação seja destinada ao IMDSv1.

Para obter uma análise extensa do IMDSv2, consulte Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados da instância do EC2.

Para recuperar metadados da instância, consulte Recuperar metadados da instância.

Tópicos

- Como Serviço de metadados da instância versão 2 funciona
- Transição para usar o Serviço de metadados da instância versão 2
- Usar um AWS SDK compatível

Como Serviço de metadados da instância versão 2 funciona

O IMDSv2 usa solicitações orientadas a sessão. Com solicitações orientadas a sessão, você cria um token de sessão que define a duração da sessão, que pode ser, no mínimo, um segundo e, no máximo, seis horas. Durante o período especificado, é possível usar o mesmo token de sessão para solicitações subsequentes. Depois que a duração especificada expira, crie um novo token de sessão para uso em solicitações futuras.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do Serviço de metadados da instância (IMDS): `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias do EC2 pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `[fd00:ec2::254]`. O endereço IPv6 do IMDS é compatível com comandos IMDSv2. O endereço IPv6 só pode ser acessado em instâncias baseadas no AWS Nitro System e em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas).

Os exemplos apresentados a seguir usam um script de shell e um IMDSv2 para recuperar os itens de metadados da instância de nível superior. Cada exemplo:

- Cria um token de sessão que dura seis horas (21.600 segundos) usando a solicitação PUT.

- Armazena o cabeçalho do token da sessão em uma variável chamada `TOKEN` (para as instâncias do Linux) ou `token` (para as instâncias do Windows)
- Solicita os itens de metadados de nível superior usando o token

Exemplo do Linux

É possível executar dois comandos separados ou combiná-los.

Comandos separados

Primeiro, gere um token usando o comando a seguir.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
```

Em seguida, use o token para gerar itens de metadados de nível superior usando o comando a seguir.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Comandos combinados

É possível armazenar o token e combinar os comandos. O exemplo a seguir combina os dois comandos acima e armazena o cabeçalho do token de sessão em uma variável chamada TOKEN.

> **Note**
>
> Se houver um erro na criação do token, em vez de um token válido, uma mensagem de erro será armazenada na variável e o comando não funcionará.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Depois de criar um token, é possível reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$TOKEN` no exemplo anterior é reutilizado.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Exemplo do Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Depois de criar um token, é possível reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$token` no exemplo anterior é reutilizado.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Quando você usa o IMDSv2 para solicitar os metadados da instância, a solicitação deve incluir o seguinte:

1. Use uma solicitação PUT para solicitar a inicialização de uma sessão para o serviço de metadados da instância. A solicitação PUT retorna um token que deve ser incluído em solicitações GET subsequentes para o serviço de metadados da instância. O token é exigido para acessar metadados usando o IMDSv2.
2. Inclua o token em todas as solicitações GET para o IMDS. Quando o uso do token está definido como `required`, as solicitações sem um token válido ou com um token expirado recebem um código de erro HTTP `401 - Unauthorized`.
   - O token é uma chave específica da instância. O token não é válido em outras instâncias do EC2 e será rejeitado se você tentar usá-lo fora da instância na qual foi gerado.
   - A solicitação PUT deve incluir um cabeçalho que especifique a vida útil (TTL) do token, em segundos, até um máximo de seis horas (21.600 segundos). O token representa uma sessão lógica. O TTL especifica o período de validade do token e, portanto, a duração da sessão.
   - Depois que o token expira, para continuar a acessar os metadados da instância, crie uma nova sessão usando outro PUT.

- É possível optar por reutilizar um token ou criar um novo token para cada solicitação. Para um número pequeno de solicitações, pode ser mais fácil gerar e usar imediatamente um token a cada vez que você precisar acessar o IMDS. Mas, para obter eficiência, é possível especificar uma duração maior para o token e reutilizá-lo, em vez de precisar escrever uma solicitação PUT toda vez que precisar solicitar metadados da instância. Não há um limite prático para o número de tokens simultâneos, cada um representando sua própria sessão. No entanto, o IMDSv2 ainda é restringido pela conexão do IMDS e pelos limites de controle de utilização. Para ter mais informações, consulte Limitação de consulta.

Os métodos HTTP GET e HEAD são permitidos em solicitações de metadados de instâncias do IMDSv2. As solicitações PUT serão rejeitadas se contiverem um cabeçalho X-Forwarded-For.

Por padrão, a resposta a solicitações PUT tem um limite de saltos de resposta (vida útil) de 1 no nível de protocolo IP. Se você precisar de um limite maior de saltos, é possível ajustar o limite usando o comando modify-instance-metadata-options da AWS CLI. Por exemplo, um limite de saltos maior pode ser necessário para compatibilidade com versões anteriores de serviços de contêiner em execução na instância. Para ter mais informações, consulte Modificar as opções de metadados de instância para as instâncias existentes.

Transição para usar o Serviço de metadados da instância versão 2

Se você optar por migrar para o IMDSv2, recomendamos que use as ferramentas e o caminho de transição a seguir.

Tópicos

- Ferramentas para ajudar com a transição para o IMDSv2
- Caminho recomendado para exigir IMDSv2

Ferramentas para ajudar com a transição para o IMDSv2

Se seu software usar o IMDSv1, use as ferramentas a seguir para ajudar a configurar o software para usar o IMDSv2.

Software da AWS

As versões mais recentes da AWS CLI e dos AWS SDKs são compatíveis com o IMDSv2. Para usar o IMDSv2, certifique-se de que as instâncias do EC2 tenham as versões mais recentes

da CLI e dos SDKs. Para obter informações sobre como atualizar a CLI, consulte Instalação, atualização e desinstalação da AWS CLI no Guia do usuário da AWS Command Line Interface.

Todos os pacotes de software Amazon Linux 2 e Amazon Linux 2023 são compatíveis com o IMDSv2. No Amazon Linux 2023, o IMDSv1 é desabilitado por padrão.

Para obter as versões mínimas do AWS SDK compatíveis com IMDSv2, consulte Usar um AWS SDK compatível.

IMDS Packet Analyzer

O IMDS Packet Analyzer é uma ferramenta de código aberto que identifica e registra as chamadas IMDSv1 da fase de inicialização da sua instância. Isso pode ajudar a identificar o software que faz chamadas IMDSv1 em instâncias do EC2, permitindo que você identifique exatamente o que precisa atualizar para preparar suas instâncias para usar somente o IMDSv2. Você pode executar o IMDS Packet Analyzer em uma linha de comando ou instalá-lo como um serviço. Para obter mais informações, consulte IMDS Packet Analyzer no GitHub.

CloudWatch

O IMDSv2 usa sessões baseadas em token, enquanto o IMDSv1 não o faz. A métrica `MetadataNoToken` do CloudWatch rastreia o número de chamadas para o Serviço de metadados da instância (IMDS) que estão usando o IMDSv1. Rastreando essa métrica até zero, é possível determinar se e quando todo o software foi atualizado para usar o IMDSv2.

Após desabilitar o IMDSv1, é possível usar a métrica `MetadataNoTokenRejected` do CloudWatch para rastrear o número de vezes que uma chamada do IMDSv1 foi tentada e rejeitada. Ao rastrear essa métrica, você pode verificar se o software precisa ser atualizado para usar o IMDSv2.

Para ter mais informações, consulte Métricas de instância.

Atualizações para APIs e CLIs do EC2

Para novas instâncias, é possível usar a API RunInstances para executar novas instâncias que exijam o uso do IMDSv2. Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.

Para instâncias existentes, é possível usar a API ModifyInstanceMetadataOptions para exigir o uso do IMDSv2. Para ter mais informações, consulte Modificar as opções de metadados de instância para as instâncias existentes.

Para exigir o uso do IMDSv2 em todas as novas instâncias executadas por grupos de Auto Scaling, seus grupos de Auto Scaling podem usar um modelo de execução ou uma configuração de execução. Quando você cria um modelo de execução ou cria uma configuração de execução, é necessário configurar os parâmetros de `MetadataOptions` para exigir o uso do IMDSv2. O grupo do Auto Scaling inicia novas instâncias usando o novo modelo de execução ou configuração de execução, mas as instâncias existentes não serão afetadas. Para instâncias existentes em um grupo do Auto Scaling, é possível usar a API ModifyInstanceMetadataOptions para exigir o uso do IMDSv2 em instâncias existentes, ou encerrar as instâncias e o grupo do Auto Scaling executará novas instâncias de substituição com as configurações das opções de metadados de instância definidas no modelo ou na configuração de execução.

Usar uma AMI que configura o IMDSv2 por padrão

Ao iniciar uma instância, você pode configurá-la automaticamente para usar o IMDSv2 por padrão (o parâmetro `HttpTokens` é definido como `required`) iniciando-a com uma AMI configurada com o parâmetro `ImdsSupport` definido como `v2.0`. É possível definir o parâmetro `ImdsSupport` como `v2.0` ao registrar a AMI usando o comando register-image da CLI, ou modificar uma AMI existente usando o comando modify-image-attribute da CLI. Para ter mais informações, consulte Configurar a AMI.

Políticas do IAM e SCPs

Você pode usar uma política do IAM ou uma política de controle de serviços (SCP) do AWS Organizations para controlar os usuários como se segue:

- Não é possível iniciar uma instância usando a API RunInstances, a menos que a instância esteja configurada para usar o IMDSv2.
- Não é possível modificar uma instância em execução usando a API ModifyInstanceMetadataOptions para reabilitar o IMDSv1.

A política do IAM ou a SCP devem conter as seguintes chaves de condição do IAM:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Se um parâmetro da chamada de API ou CLI não corresponder ao estado especificado na política que contém a chave de condição, a chamada de API ou CLI falhará com uma resposta `UnauthorizedOperation`.

Além disso, é possível escolher uma camada adicional de proteção para exigir a alteração do IMDSv1 para o IMDSv2. Na camada de gerenciamento de acesso com relação às APIs chamadas por meio de credenciais de função do EC2, é possível usar uma nova chave de condição nas políticas do IAM ou nas políticas de controle de serviço (SCPs) do AWS Organizations. Especificamente, usando a chave de condição da política `ec2:RoleDelivery` com um valor `2.0` nas políticas do IAM, as chamadas de API feitas com as credenciais do perfil do EC2 obtidas do IMDSv1 receberão uma resposta `Unauthorized0peration`. A mesma coisa pode ser obtida de forma mais ampla com essa condição exigida por uma SCP. Isso garante que as credenciadas entregues por meio do IMDSv1 não podem ser realmente usadas para chamar APIs porque todas as chamadas à API que não corresponderem à condição especificada receberão um erro `Unauthorized0peration`.

Para obter exemplos de políticas do IAM, consulte Trabalhar com metadados de instância. Para obter mais informações sobre SCPs, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Caminho recomendado para exigir IMDSv2

Usando as ferramentas acima, recomendamos que você siga este caminho para fazer a transição para o IMDSv2.

Etapa 1: No início

Atualize os SDKs, as CLIs e os programas de software que usam credenciais do perfil nas instâncias do EC2 para versões compatíveis com o IMDSv2. Para obter informações sobre como atualizar a CLI, consulte Atualização para a versão mais recente da AWS CLI no Guia do usuário da AWS Command Line Interface.

Depois, altere o software que acessa os metadados da instância diretamente (ou seja, que não usa um SDK) usando as solicitações do IMDSv2. Você pode usar o IMDS Packet Analyzer para identificar o software que você precisa alterar para usar as solicitações IMDSv2.

Etapa 2: acompanhar o andamento da transição

Acompanhe o andamento da transição usando a métrica do CloudWatch `MetadataNoToken`. Esta métrica mostra o número de chamadas IMDSv1 para o IMDS em suas instâncias. Para ter mais informações, consulte Métricas de instância.

Etapa 3: quando a utilização do IMDSv1 é zero

Quando a métrica `MetadataNoToken` do CloudWatch registra uma utilização zero do IMDSv1, as instâncias estão prontas para passar a usar o IMDSv2. Nessa fase, é possível fazer o seguinte:

- Padrão da conta

  Você pode definir o IMDSv2 como obrigatório como o padrão da conta. Quando uma instância é executada, a configuração da instância é definida automaticamente como a conta padrão.

  Para definir a conta padrão, faça o seguinte:

  - Console do Amazon EC2: no painel do EC2, em Atributos da conta, Proteção e segurança de dados, em Padrões do IMDS, defina Serviço de metadados da instância como Habilitado e Versão de metadados como Somente V2 (requer token). Para ter mais informações, consulte Definir o IMDSv2 como o padrão para a conta.
  - AWS CLI: use o comando modify-instance-metadata-defaults da CLI e especifique `--http-tokens required` e `--http-put-response-hop-limit 2`.
- Instâncias novas

  Ao iniciar uma nova instância, você pode fazer o seguinte:

  - No console do Amazon EC2: no assistente de inicialização de instância, defina Metadata accessible (Metadados acessíveis) como Enabled (Habilitado) e Metadata version (Versão de metadados) como V2 only (token required) (Apenas V2 [token obrigatório]). Para ter mais informações, consulte Configurar a instância na inicialização.
  - AWS CLI: use o comando run-instances da CLI e especifique que o IMDSv2 é obrigatório.
- Instâncias existentes

  Para instâncias existentes, é possível fazer o seguinte:

  - Console do Amazon EC2: na página Instâncias, selecione sua instância, escolha Ações, Configurações da instância, Modificar opções de metadados da instância e, para IMDSv2, escolha Obrigatório. Para ter mais informações, consulte Exigir o uso de IMDSv2.
  - AWS CLI: use o comando modify-instance-metadata-options da CLI para especificar que apenas o IMDSv2 deverá ser usado.

  É possível modificar as opções de metadados da instância em instâncias em execução, e você não precisará reiniciá-las depois de modificar as opções de metadados da instância.

Etapa 4: verificar se suas instâncias fizeram a transição para o IMDSv2

É possível verificar se alguma instância ainda não está configurada para exigir o uso do IMDSv2, em outras palavras, se o IMDSv2 ainda está configurado como `optional`. Se alguma instância ainda estiver configurada como `optional`, será possível modificar as opções de metadados da instância para tornar o IMDSv2 `required`. Para isso, repita a Etapa 3.

Para filtrar suas instâncias:

- Console do Amazon EC2: na página Instâncias, filtre suas instâncias usando o filtro IMDSv2 = opcional. Para obter mais informações sobre filtragem, consulte Filtrar recursos usando o console. Você também pode ver se o IMDSv2 é obrigatório ou opcional para cada instância: na janela Preferências. Ative o IMDSv2 para adicionar a coluna IMDSv2 à tabela Instâncias.
- AWS CLI: use o comando describe-instances da CLI e filtre por `metadata-options.http-tokens = optional`, da seguinte forma:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output
 text
```

Etapa 5: quando todas as suas instâncias tiverem feito a transição para o IMDSv2

É possível usar as chaves de condição `ec2:MetadataHttpTokens`, `ec2:MetadataHttpPutResponseHopLimit` e `ec2:MetadataHttpEndpoint` do IAM para controlar o uso de RunInstances e das API ModifyInstanceMetadataOptions e das CLIs correspondentes. Se uma política for criada, e um parâmetro na chamada à API não corresponder ao estado especificado na política usando a chave de condição, a chamada à API ou à CLI falhará com uma resposta `UnauthorizedOperation`. Para obter exemplos de políticas do IAM, consulte Trabalhar com metadados de instância.

Mais ainda, após desabilitar o IMDSv1, é possível usar a métrica `MetadataNoTokenRejected` do CloudWatch para rastrear o número de vezes que uma chamada do IMDSv1 foi tentada e rejeitada. Se, após você desabilitar o IMDSv1, algum software não estiver funcionando corretamente e a métrica `MetadataNoTokenRejected` registrar as chamadas do IMDSv1, é provável que esse software precise ser atualizado para usar o IMDSv2.

Usar um AWS SDK compatível

Para usar o IMDSv2, as instâncias do EC2 devem usar uma versão do AWS SDK compatível com o uso do IMDSv2. As versões mais recentes de todos os AWS SDKs permitem usar o IMDSv2.

> **Important**
>
> Recomendamos que você se mantenha atualizado com as versões do SDK para acompanhar os recursos, as atualizações de segurança e as dependências subjacentes mais recentes. O uso contínuo de uma versão não compatível do SDK não é recomendado e é feito a seu critério. Para obter mais informações, consulte a Política de manutenção de SDKs e ferramentas da AWS no Guia de referência de SDKs e ferramentas da AWS.

Veja a seguir as versões mínimas que são compatíveis com o uso do IMDSv2:

- AWS CLI: 1.16.289
- AWS Tools for Windows PowerShell: 4.0.1.0
- AWS SDK for .NET: 3.3.634.1
- AWS SDK for C++: 1.7.229
- AWS SDK for Go: 1.25.38
- AWS SDK para Go v2: 0.19.0
- AWS SDK for Java: 1.11.678
- AWS SDK for Java 2.x: 2.10.21
- AWS SDK para JavaScript em Node.js: 2.722.0
- AWS SDK for PHP: 3.147.7
- AWS SDK para Python (Botocore) – 1.13.25
- AWS SDK for Python (Boto3): 1.12.6
- AWS SDK for Ruby: 3.79.0

Configurar as opções de metadados da instância

O serviço de metadados de instância (IMDS) é executado localmente em cada instância do EC2. As opções de metadados de instância se referem a um conjunto de configurações que controlam a acessibilidade e o comportamento do IMDS em uma instância do EC2.

Você pode configurar as seguintes opções de metadados da instância em cada instância:

Serviço de metadados de instância (IMDS): `enabled` | `disabled`

É possível habilitar ou desabilitar o IMDS em uma instância. Quando desabilitado, os metadados da instância não poderão ser acessados por você ou por nenhum outro código.

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. Se quiser habilitar o endpoint IPv6, você precisará fazer isso explicitamente.

Endpoint IPv6 do IMDS: `enabled` | `disabled`

Você pode habilitar explicitamente o endpoint IPv6 do IMDS em uma instância. Quando o endpoint IPv6 estiver habilitado, o endpoint IPv4 permanecerá habilitado. O endpoint IPv6 só é compatível com instâncias baseadas no AWS Nitro System e em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas).

Versão de metadados: `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Ao solicitar metadados de instância, as chamadas do IMDSv2 exigem um token. As chamadas do IMDSv1 não exigem um token. É possível configurar uma instância para permitir chamadas do IMDSv1 ou do IMDSv2 (quando um token for opcional) ou para permitir somente chamadas do IMDSv2 (quando um token for obrigatório).

Limite de salto de resposta de metadados: 1–64

O limite de saltos é o número de saltos de rede que a resposta PUT pode fazer. Você pode definir o limite de saltos para um mínimo de 1 e um máximo de 64. Em um ambiente de contêiner, recomendamos definir o limite de saltos como 2. Para ter mais informações, consulte Considerações.

Acesso a tags nos metadados da instância: `enabled` | `disabled`

É possível habilitar ou desabilitar o acesso às tags de uma instância nos metadados de uma instância. Para ter mais informações, consulte Trabalho com tags de instância em metadados de instância.

Onde configurar as opções de metadados da instância

É possível configurar as opções de metadados da instância em diferentes níveis, da seguinte forma:

- Conta: você pode definir valores padrão para as opções de metadados da instância por conta para cada Região da AWS. Quando uma instância for executada, as opções de metadados da instância serão definidas automaticamente para os valores na conta. Você pode alterar esses valores na execução. Os valores padrão por conta não afetam as instâncias existentes.
- AMI: ao registrar ou modificar uma AMI, é possível definir o parâmetro `imds-support` como `v2.0`. Quando uma instância for executada com essa AMI, a versão dos metadados da instância será definida automaticamente como IMDSv2 e o limite de saltos será definido como 2.
- Instância: você pode alterar todas as opções de metadados de uma instância na execução, substituindo as configurações padrão. Também é possível alterar as opções de metadados da instância após a execução em uma instância em execução ou parada. Observe que as alterações poderão sofrer restrições de uma política do IAM ou SCP.

Para ter mais informações, consulte Configurar opções de metadados da instância para novas instâncias e Modificar as opções de metadados de instância para as instâncias existentes.

Ordem de precedência das opções de metadados da instância

O valor de cada opção de metadados da instância é determinado na inicialização da instância, seguindo uma ordem hierárquica de precedência. A hierarquia, com a maior precedência no topo, é a seguinte:

- Precedência 1: configuração da instância na execução: é possível especificar os valores no modelo de execução ou na configuração da instância. Todos os valores especificados aqui substituirão os valores especificados por conta ou na AMI.
- Precedência 2: configurações da conta: se não houver um valor especificado na inicialização da instância, ele será determinado pelas configurações por conta (que são definidas para cada Região da AWS). As configurações por conta incluem um valor para cada opção de metadados ou não indicam nenhuma preferência.
- Precedência 3: configuração da AMI: se não houver um valor especificado na execução da instância ou por conta, ele será determinado pela configuração da AMI. Isso se aplica somente a `HttpTokens` e `HttpPutResponseHopLimit`.

Cada opção de metadados é avaliada separadamente. É possível configurar a instância com uma combinação de configuração direta da instância, padrões por conta e a configuração da AMI.

A menos que as alterações sejam restringidas por uma política do IAM ou SCP, você poderá alterar o valor de qualquer opção de metadados após a execução em uma instância em execução ou parada.

Determinar valores para opções de metadados: exemplo 1

Neste exemplo, uma instância do EC2 é iniciada em uma região na qual `HttpPutResponseHopLimit` está definido como 1 para a conta. A AMI especificada tem `ImdsSupport` definido como `v2.0`. Nenhuma opção de metadados é especificada diretamente na instância na execução. A instância é executada com as seguintes opções de metadados:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Esses valores foram determinados da seguinte manneira:

- Nenhuma opção de metadados especificada na execução: durante a execução da instância, não se forneceu valores específicos para as opções de metadados nos parâmetros de execução da instância nem no modelo de execução.
- As configurações da conta têm a próxima precedência: na ausência da definição de valores específicos na execução, as configurações por conta na região terão precedência. Isso significa que os valores padrão configurados por conta serão aplicados. Nesse caso, o `HttpPutResponseHopLimit` foi definido como `1`.
- As configurações da AMI têm a última precedência: na ausência de um valor específico definido na inicialização ou no nível da conta para `HttpTokens` (a versão de metadados da instância), a configuração da AMI é aplicada. Nesse caso, a configuração da AMI `ImdsSupport: v2.0` determinou que `HttpTokens` estava definido como `required`. Observe que, embora a configuração da AMI `ImdsSupport: v2.0` tenha sido projetada para definir `HttpPutResponseHopLimit: 2`, ela foi substituída pela configuração no nível da conta `HttpPutResponseHopLimit: 1`, que tem maior precedência.

Determinar valores para opções de metadados: exemplo 2

Neste exemplo, a instância do EC2 é executada com as mesmas configurações do Exemplo 1 anterior, mas com a configuração `HttpTokens` definida como `optional` diretamente na instância na execução. A instância é executada com as seguintes opções de metadados:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

O valor de `HttpPutResponseHopLimit` é determinado da mesma forma que no Exemplo 1. No entanto, o valor de `HttpTokens` é determinado da seguinte forma: as opções de metadados configuradas na instância na execução terão precedência. Embora a AMI tenha sido configurada com `ImdsSupport: v2.0` (em outras palavras, `HttpTokens` esteja definido como `required`), o valor especificado na instância na execução (`HttpTokens` definido como `optional`) teve precedência.

Definir a versão de metadados da instância

Quando uma instância é executada, o valor da versão de metadados da instância é `IMDSv1 or IMDSv2 (token optional)` ou `IMDSv2 only (token required)`.

Na execução da instância, é possível especificar manualmente o valor da versão de metadados ou usar o valor padrão. Se você especificar o valor manualmente, ele substituirá todos os padrões. Se você optar por não especificar o valor manualmente, ele será determinado por uma combinação de configurações padrão, conforme descrito na tabela a seguir.

A tabela mostra como a versão dos metadados de uma instância na execução (indicada pela Configuração resultante da instância na coluna 4) é determinada pelas configurações nos diferentes níveis de configuração. A ordem de precedência é da esquerda para a direita, com a primeira coluna tendo a maior precedência, da seguinte maneira:

- Coluna 1: Parâmetro de inicialização: representa a configuração na instância que você especifica manualmente na execução.
- Coluna 2: Padrão por conta: representa a configuração da conta.
- Coluna 3: Padrão da AMI: representa a configuração na AMI.

Parâmetro de execução	Padrão por conta	Padrão da AMI	Configuração resultante da instância
Somente V2 (requer token)	Sem preferência	Somente V2	Somente V2
Somente V2 (requer token)	Somente V2	Somente V2	Somente V2
Somente V2 (requer token)	V1 ou V2	Somente V2	Somente V2
V1 ou V2 (token opcional)	Sem preferência	Somente V2	V1 ou V2
V1 ou V2 (token opcional)	Somente V2	Somente V2	V1 ou V2
V1 ou V2 (token opcional)	V1 ou V2	Somente V2	V1 ou V2
Não definido	Sem preferência	Somente V2	Somente V2
Não definido	Somente V2	Somente V2	Somente V2
Não definido	V1 ou V2	Somente V2	V1 ou V2
Somente V2 (requer token)	Sem preferência	nulo	Somente V2
Somente V2 (requer token)	Somente V2	nulo	Somente V2
Somente V2 (requer token)	V1 ou V2	nulo	Somente V2
V1 ou V2 (token opcional)	Sem preferência	nulo	V1 ou V2

Parâmetro de execução	Padrão por conta	Padrão da AMI	Configuração resultante da instância
V1 ou V2 (token opcional)	Somente V2	nulo	V1 ou V2
V1 ou V2 (token opcional)	V1 ou V2	nulo	V1 ou V2
Não definido	Sem preferência	nulo	V1 ou V2
Não definido	Somente V2	nulo	Somente V2
Não definido	V1 ou V2	nulo	V1 ou V2

Usar chaves de condição do IAM para restringir as opções de metadados da instância

É possível usar chaves de condição do IAM em uma política do IAM ou SCP da seguinte maneira:

- Permitir que uma instância seja executada somente se ela estiver configurada para exigir o uso do IMDSv2
- Restringir o número de saltos permitidos
- Desativar o acesso aos metadados da instância

Tarefas

- Configurar opções de metadados da instância para novas instâncias
- Modificar as opções de metadados de instância para as instâncias existentes

> **Note**
>
> Proceda com cautela e conduza testes cuidadosos antes de fazer qualquer alteração. Anote o seguinte:
>
> - Se você exigir o uso do IMDSv2, as aplicações ou agentes que usam o IMDSv1 para acesso aos metadados da instância falharão.

- Se você desativar todo o acesso aos metadados da instância, as aplicações ou agentes que contam com o acesso aos metadados da instância para funcionarem falharão.
- Para IMDSv2, use `/latest/api/token` ao recuperar o token.
- (Somente para o Windows) Se a versão do PowerShell for uma versão anterior à 4.0, você deverá atualizar para o Windows Management Framework 4.0 para exigir o uso do IMDSv2.

Configurar opções de metadados da instância para novas instâncias

É possível configurar as opções de metadados de instância a seguir em cada instância.

Opções

- Exigir o uso de IMDSv2
- Habilitar os endpoints IPv4 e IPv6 do IMDS
- Desativar o acesso aos metadados da instância

Exigir o uso de IMDSv2

É possível utilizar um dos métodos a seguir para exigir o uso do IMDSv2 nas novas instâncias.

Para exigir o IMDSv2

- Definir o IMDSv2 como o padrão para a conta
- Configurar a instância na inicialização
- Configurar a AMI
- Usar uma política do IAM

Definir o IMDSv2 como o padrão para a conta

É possível definir a versão padrão do serviço de metadados de instância (IMDS) em nível de conta para cada Região da AWS. Isso significa que, quando uma nova instância é executada, a versão dos metadados da instância é definida automaticamente para padrão do nível de conta. No entanto, você pode substituir manualmente o valor na execução ou após a execução. Para obter mais informações sobre como as configurações em nível de conta e as substituições manuais afetam uma instância, consulte Ordem de precedência das opções de metadados da instância.

> **Note**
>
> Definir o padrão no nível de conta não redefine as instâncias existentes. Por exemplo, se você definir o padrão no nível de conta como IMDSv2, as instâncias existentes definidas como IMDSv1 não serão afetadas. Se desejar alterar o valor nas instâncias existentes, altere manualmente o valor nas próprias instâncias.

É possível definir o padrão da conta para a versão dos metadados de instância como IMDSv2 para que todas as novas instâncias na conta sejam iniciadas com o IMDSv2 obrigatório. Nesse caso, o IMDSv1 será desabilitado. Com esse padrão da conta, quando você executar uma instância, os valores padrão da instância serão os seguintes:

- Console: a Versão de metadados estará definida como Somente V2 (requer token) e o Limite de salto de resposta de metadados como 2.
- AWS CLI: `HttpTokens` estará definido como `required` e `HttpPutResponseHopLimit` como `2`.

> **Note**
>
> Antes de definir a conta padrão para IMDSv2, certifique-se de que suas instâncias não dependam do IMDSv1. Para ter mais informações, consulte Caminho recomendado para exigir IMDSv2.

Console

Para definir o IMDSv2 como padrão para a conta da região especificada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Ao lado de Padrões do IMDS, escolha Gerenciar.
6. Na página Gerenciar padrões do IMDS, faça o seguinte:

a. Em Serviço de metadados de instância, escolha Habilitado.
b. Em Metadata version (Versão de metadados), selecione V2 only (token required) (Apenas V2 [token obrigatório]).
c. Em Limite de salto de resposta de metadados, especifique 2 se suas instâncias forem hospedar contêineres. Caso contrário, selecione Sem preferência. Quando não houver uma preferência especificada, na execução, o valor padrão será 2 se a AMI exigir IMDSv2. Caso contrário, o padrão será 1 por padrão.
d. Selecione Atualizar.

AWS CLI

Para definir o IMDSv2 como padrão para a conta da região especificada

Use o comando modify-instance-metadata-defaults e especifique a região na qual deseja modificar as configurações do IMDS por conta. Inclua `--http-tokens` definido como `required` e `--http-put-response-hop-limit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (sem preferência) for especificado, na execução, o valor padrão será 2 se a AMI exigir IMDSv2. Caso contrário, o padrão será 1 por padrão.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Saída esperada

```
{
    "Return": true
}
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para a região especificada

Use o comando get-instance-metadata-defaults e especifique a região.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Exemplo de saída

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    }
}
```

PowerShell

Para definir o IMDSv2 como padrão para a conta da região especificada

Use o comando Edit-EC2InstanceMetadataDefault e especifique a região na qual deseja modificar as configurações do IMDS por conta. Inclua `-HttpToken` definido como `required` e `-HttpPutResponseHopLimit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (sem preferência) for especificado, na execução, o valor padrão será 2 se a AMI exigir IMDSv2. Caso contrário, o padrão será 1 por padrão.

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Saída esperada

```
True
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para a região especificada

Use o comando Get-EC2InstanceMetadataDefault e especifique a região.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Exemplo de saída

```
HttpEndpoint            :
```

```
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Configurar a instância na inicialização

Quando você inicia uma instância, pode configurá-la para exigir o uso do IMDSv2, configurando os seguintes campos:

- Console do Amazon EC2: defina Metadata version (Versão de metadados) como V2 only (token required) (Apenas V2 [token obrigatório]).
- AWS CLI: defina `HttpTokens` como `required`.

Quando você especificar que o IMDSv2 é obrigatório, também deverá habilitar o endpoint do Serviço de metadados da instância (IMDS) definindo Metadados acessíveis como Habilitado (console) ou `HttpEndpoint` como `enabled` (AWS CLI).

Em um ambiente de contêiner, quando o IMDSv2 for necessário, recomendamos definir o limite de saltos como 2. Para ter mais informações, consulte Considerações.

New console

Como exigir o uso do IMDSv2 em uma nova instância

- Ao executar uma nova instância no console do Amazon EC2, expanda Advanced details (Detalhes avançados) e faça o seguinte:
  - Para Metadata acessible (Metadados acessíveis), escolha Enabled (Habilitado).
  - Em Metadata version (Versão de metadados), selecione V2 only (token required) (Apenas V2 [token obrigatório]).
  - (Ambiente de contêiner) Em Limite de salto de resposta dos metadados, escolha 2.

  Para ter mais informações, consulte Detalhes avançados.

Old console

Como exigir o uso do IMDSv2 em uma nova instância

- Ao executar uma nova instância no console do Amazon EC2, selecione as seguintes opções na página Configure Instance Details (Configurar detalhes da instância):
  - Em Advanced Details (Detalhes avançados), em Metadata accessible (Metadados acessíveis), selecione Enabled (Habilitado).
  - Em Metadata version (Versão de metadados), selecione V2 (token required) V2 (token obrigatório).

Para ter mais informações, consulte Etapa 3: configurar detalhes da instância.

AWS CLI

Como exigir o uso do IMDSv2 em uma nova instância

O exemplo de run-instances a seguir executa uma instância `c6i.large` com `--metadata-options` definido como `HttpTokens=required`. Quando você especifica um valor para `HttpTokens`, também deve definir `HttpEndpoint` como `enabled`. Como o cabeçalho de token seguro é definido como `required` para solicitações de recuperação de metadados, é necessário que a instância use o IMDSv2 ao solicitar metadados da instância.

Em um ambiente de contêiner, quando o IMDSv2 for necessário, recomendamos definir o limite de saltos como 2 com `HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Como exigir o uso do IMDSv2 em uma nova instância

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `c6i.large` com `MetadataOptions_HttpEndpoint` definido como `enabled` e o parâmetro

`MetadataOptions_HttpTokens` como `required`. Quando você especifica um valor para `HttpTokens`, também deve definir `HttpEndpoint` como `enabled`. Como o cabeçalho de token seguro é definido como `required` para solicitações de recuperação de metadados, é necessário que a instância use o IMDSv2 ao solicitar metadados da instância.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Para especificar as opções de metadados de uma instância usando AWS CloudFormation, consulte a propriedade AWS::EC2::LaunchTemplate MetadataOptions no Guia do usuário do AWS CloudFormation.

Configurar a AMI

Ao registrar uma nova AMI ou modificar uma AMI existente, é possível definir o parâmetro `imds-support` como `v2.0`. As instâncias iniciadas a partir dessa AMI terão Metadata version (Versão de metadados) definido como V2 only (token required) (Apenas V2 [token obrigatório]) (console) ou `HttpTokens` definido como `required` (AWS CLI). Com essas configurações, a instância exige que o IMDSv2 seja usado ao solicitar metadados da instância.

Observe que quando você configura `imds-support` como `v2.0`, as instâncias iniciadas a partir dessa AMI também têm Metadata response hop limit (Limite de saltos na resposta de metadados) (console) ou `http-put-response-hop-limit` (AWS CLI) definido como 2.

Important

Não use esse parâmetro, a menos que seu software AMI ofereça suporte ao IMDSv2. Após definir o valor como `v2.0`, você não poderá desfazer essa ação. A única maneira de "redefinir" sua AMI é criando uma nova AMI a partir do snapshot subjacente.

Para configurar uma nova AMI para o IMDSv2

Use um dos métodos a seguir para configurar uma nova AMI para o IMDSv2.

AWS CLI

O exemplo de register-image a seguir registra uma AMI usando o snapshot especificado de um volume raiz do EBS como `/dev/xvda` de dispositivo. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

O exemplo de Cmdlet Register-EC2Image a seguir registra uma AMI usando o snapshot especificado de um volume raiz do EBS como dispositivo `/dev/xvda`. Especifique `v2.0` para o parâmetro `ImdsSupport`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
Import-Module AWS.Tools.EC2  # Required for Amazon.EC2.Model object creation.
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example';
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Para configurar uma AMI existente para o IMDSv2

Use um dos métodos a seguir para configurar uma AMI para IMDSv2 existente.

AWS CLI

O exemplo de modify-image-attribute a seguir modifica uma AMI existente para IMDSv2 somente. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
aws ec2 modify-image-attribute \
    --image-id ami-0123456789example \
    --imds-support v2.0
```

PowerShell

O exemplo de Cmdlet Edit-EC2ImageAttribute a seguir só modifica uma AMI existente para IMDSv2. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Usar uma política do IAM

Você pode criar uma política do IAM que impeça que os usuários iniciem novas instâncias, a menos que exijam o IMDSv2 na nova instância.

Para impor o uso do IMDSv2 em todas as novas instâncias usando uma política do IAM

Para garantir que os usuários possam executar apenas instâncias que requeiram o uso do IMDSv2 ao solicitar metadados da instância, é possível especificar que a condição para exigir o IMDSv2 deve ser atendida para que uma instância possa ser executada. Para ver um exemplo de política do IAM, consulte Trabalhar com metadados de instância.

Habilitar os endpoints IPv4 e IPv6 do IMDS

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. O endpoint IPv6 permanece desabilitado mesmo que você inicie uma instância em uma sub-rede IPv6 apenas. Para habilitar o endpoint IPv6, você precisa fazer isso explicitamente. Quando você habilita o endpoint IPv6, o endpoint IPv4 permanece habilitado.

Você pode habilitar o endpoint iPv6 ao iniciar a instância ou posteriormente.

Requisitos para habilitação do endpoint iPv6

- O tipo de instância selecionado é baseado no AWS Nitro Systen.
- A sub-rede selecionada é compatível com IPv6, no qual a sub-rede é de pilha dupla ou IPv6 apenas.

Use um dos métodos a seguir para iniciar uma instância com o endpoint IPv6 do IMDS habilitado.

New console

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

- Inicie a instância no console do Amazon EC2 com o valor a seguir especificado em Advanced details (Detalhes avançados):
  - Para o endpoint IPv6 de metadados, escolha Habilitado.

Para ter mais informações, consulte Detalhes avançados.

AWS CLI

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

O exemplo de run-instances a seguir inicia uma instância `c6i.large` com o endpoint IPv6 habilitado para o IMDS. Para habilitar o endpoint IPv6, no parâmetro `--metadata-options`, especifique `HttpProtocolIpv6=enabled`. Quando você especifica um valor para `HttpProtocolIpv6`, também deve definir `HttpEndpoint` como `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `c6i.large` com o endpoint IPv6 habilitado para IMDS. Para habilitar o endpoint IPv6, especifique `MetadataOptions_HttpProtocolIpv6` como `enabled`. Quando você especifica um valor para `MetadataOptions_HttpProtocolIpv6`, também deve definir `MetadataOptions_HttpEndpoint` como `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Desativar o acesso aos metadados da instância

Você pode desativar o acesso aos metadados da instância desativando o IMDS ao executar uma instância. Você pode ativar o acesso mais tarde reativando o IMDS. Para ter mais informações, consulte Ativar o acesso aos metadados da instância.

Important

É possível desativar o IMDS na execução ou após a execução. Se você desativar o IMDS na execução, os seguintes problemas poderão ocorrer:

- Talvez você não tenha acesso SSH à sua instância. A `public-keys/0/openssh-key`, que é a chave SSH pública da sua instância, não estará acessível porque a chave normalmente é fornecida e acessada nos metadados da instância do EC2.
- Os dados do usuário do EC2 não estarão disponíveis e não serão executados no início da instância. Os dados do usuário do EC2 são hospedados no IMDS. Caso desative o IMDS, você desativará efetivamente o acesso aos dados do usuário.

Para acessar essa funcionalidade, você pode reativar o IMDS após a execução.

New console

Desativar o acesso aos metadados da instância na execução

- Inicie a instância no console do Amazon EC2 com o valor a seguir especificado em Advanced details (Detalhes avançados):
  - Para Metadata acessible (Metadados acessíveis), escolha Disabled (Desabilitado).

Para ter mais informações, consulte Detalhes avançados.

Old console

Desativar o acesso aos metadados da instância na execução

- Inicie a instância no console do Amazon EC2 com a opção a seguir selecionada na página Configure Instance Details (Configurar detalhes da instância):
  - Em Advanced Details (Detalhes avançados), em Metadata accessible (Metadados acessíveis), selecione Disabled (Desabilitado).

Para ter mais informações, consulte Etapa 3: configurar detalhes da instância.

AWS CLI

Desativar o acesso aos metadados da instância na execução

Inicie a instância com `--metadata-options` definido como `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Desativar o acesso aos metadados da instância na execução

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `MetadataOptions_HttpEndpoint` definida como `disabled`.

```
New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Para especificar as opções de metadados de uma instância usando AWS CloudFormation, consulte a propriedade AWS::EC2::LaunchTemplate MetadataOptions no Guia do usuário do AWS CloudFormation.

Modificar as opções de metadados de instância para as instâncias existentes

É possível modificar as opções de metadados da instância para instâncias existentes.

Também é possível criar uma política do IAM que impeça que os usuários modifiquem as opções de metadados em instâncias existentes. Para controlar quais usuários podem modificar as opções de metadados em uma instância, especifique uma política que impeça que todos os usuários que não tenham um perfil especificado usem a API ModifyInstanceMetadataOptions. Para ver um exemplo de política do IAM, consulte Trabalhar com metadados de instância.

Consultar as opções de metadados da instância para as instâncias existentes

Você pode consultar as opções de metadados da instância para suas instâncias existentes usando um dos métodos a seguir.

Console

Para consultar as opções de metadados da instância para uma instância existente, usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Analise as opções de metadados da instância atual na caixa de diálogo Modificar opções de metadados da instância.

AWS CLI

Para consultar as opções de metadados da instância para uma instância existente, usando o AWS CLI

Use o comando da CLI describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Para consultar as opções de metadados da instância para uma instância existente, usando o Tools for PowerShell

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Exigir o uso de IMDSv2

Use um dos seguintes métodos para modificar as opções de metadados da instância para exigir que o IMDSv2 seja usado ao solicitar metadados da instância. Quando o IMDSv2 for necessário, o IMDSv1 não poderá ser usado.

> **Note**
>
> Antes de exigir que o IMDSv2 seja usado, certifique-se de que a instância não esteja fazendo chamadas do IMDSv1. A métrica `MetadataNoToken` do CloudWatch rastreia as chamadas do IMDSv1. Quando `MetadataNoToken` registra zero uso do IMDSv1 para uma instância, a instância está pronta para exigir o IMDSv2.

Console

Para exigir o uso do IMDSv2 em uma instância existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, selecione Habilitar.
   b. Em IMDSv2, escolha Obrigatório.
   c. Escolha Salvar.

AWS CLI

Para exigir o uso do IMDSv2 em uma instância existente

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-tokens` como `required`. Quando você especifica um valor para `http-tokens`, também deve definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Para exigir o uso do IMDSv2 em uma instância existente

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpTokens`como `required`. Quando você especifica um valor para `HttpTokens`, também deve definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Restaurar o uso do IMDSv1

Quando o IMDSv2 for necessário, o IMDSv1 não funcionará ao solicitar metadados de instância. Quando o IMDSv2 for opcional, tanto o IMDSv2 quanto o IMDSv1 funcionarão. Portanto, para restaurar o IMDSv1, torne o IMDSv2 opcional usando um dos métodos a seguir.

Console

Para restaurar o uso do IMDSv1 em uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, certifique-se de que a opção Habilitar esteja selecionada.
   b. Em IMDSv2, escolha Opcional.
   c. Escolha Salvar.

AWS CLI

Para restaurar o uso do IMDSv1 em uma instância

É possível usar o comando da CLI modify-instance-metadata-options com `http-tokens` definido como `optional` para restaurar o uso de IMDSv1 ao solicitar metadados de instância.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Para restaurar o uso do IMDSv1 em uma instância

Você pode usar o cmdlet Edit-EC2InstanceMetadataOption com o `HttpTokens` configurado como `optional` para restaurar o uso do IMDSv1 ao solicitar metadados da instância.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Alterar o limite de salto de resposta PUT

Para instâncias existentes, é possível alterar as configurações do limite de saltos de resposta de PUT.

Atualmente, somente os SDKs AWS CLI e AWS oferecem suporte à alteração do limite de salto de resposta PUT.

AWS CLI

Como alterar o limite de salto de resposta PUT

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-put-response-hop-limit` como o número de saltos necessário. No exemplo a seguir, o limite de saltos está definido como 3. Observe que ao especificar um valor para `http-put-response-hop-limit`, também é necessário definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Como alterar o limite de salto de resposta PUT

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpPutResponseHopLimit`para o número necessário de saltos. No exemplo a seguir, o limite de saltos está definido como 3. Observe que ao especificar um valor para `HttpPutResponseHopLimit`, também é necessário definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Habilitar os endpoints IPv4 e IPv6 do IMDS

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. O endpoint IPv6 permanece desabilitado mesmo que você inicie uma instância em uma sub-rede IPv6 apenas. Para habilitar o endpoint IPv6, você precisa fazer isso explicitamente. Quando você habilita o endpoint IPv6, o endpoint IPv4 permanece habilitado.

Você pode habilitar o endpoint iPv6 ao iniciar a instância ou posteriormente.

Requisitos para habilitação do endpoint iPv6

- O tipo de instância selecionado é baseado no AWS Nitro Systen.
- A sub-rede selecionada é compatível com IPv6, no qual a sub-rede é de pilha dupla ou IPv6 apenas.

Atualmente, apenas a AWS CLI e os SDKs da AWS são compatíveis com a habilitação do endpoint IPv6 do IMDS após a inicialização da instância.

AWS CLI

Para habilitar o endpoint de IPv6 do IMDS para a instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-protocol-ipv6` como `enabled`. Observe que ao especificar um valor para `http-protocol-ipv6`, também é necessário definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Para habilitar o endpoint de IPv6 do IMDS para a instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpProtocolIpv6`como `enabled`. Observe que ao especificar um valor para `HttpProtocolIpv6`, também é necessário definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
```

```
    -InstanceId i-1234567898abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ativar o acesso aos metadados da instância

É possível ativar o acesso aos metadados da instância habilitando o endpoint de HTTP do IMDS na sua instância, independentemente da versão do IMDS que esteja sendo usada. É possível reverter essa alteração a qualquer momento desabilitando o endpoint de HTTP.

Use um dos métodos a seguir para ativar o acesso aos metadados da instância em uma instância.

Console

Para ativar o acesso aos metadados da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, selecione Habilitar.
   b. Escolha Salvar.

AWS CLI

Para ativar o acesso aos metadados da instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

PowerShell

Para ativar o acesso aos metadados da instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpEndpoint`como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Desativar o acesso aos metadados da instância

É possível desativar o acesso aos metadados da instância desabilitando o endpoint de HTTP do IMDS na sua instância, independentemente da versão do IMDS que esteja sendo usada. É possível reverte essa alteração a qualquer momento habilitando o HTTP endpoint.

Use um dos métodos a seguir para desativar o acesso aos metadados da instância em uma instância.

Console

Como desabilitar o acesso aos metadados da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, desmarque Habilitar.
   b. Escolha Salvar.

AWS CLI

Como desabilitar o acesso aos metadados da instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-endpoint` como `disabled`.

```
aws ec2 modify-instance-metadata-options \
```

```
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

PowerShell

Como desabilitar o acesso aos metadados da instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpEndpoint`como `disabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Recuperar metadados da instância

Como os metadados da instância estão disponíveis na sua instância em execução, você não precisa usar o console do Amazon EC2 nem a AWS CLI. Isso pode ser útil quando você for elaborar scripts a serem executados a partir de sua instância. Por exemplo, é possível acessar o endereço IP local de sua instância a partir dos metadados da instância para gerenciar uma conexão com uma aplicação externa.

Os metadados da instância são divididos em categorias. Para obter uma descrição de cada categoria de metadados de instância, consulte Categorias de metadados da instância

Para visualizar todas as categorias de metadados da instância dentro de uma instância em execução, obtenha os dados dos seguintes URIs IPv4 ou IPv6: Esses endereços IP são endereços locais de link e são válidos apenas a partir da instância. Para ter mais informações, consulte Endereços locais de link.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Definição de preço

Você não será cobrado pelas solicitações HTTP usadas para recuperar os metadados da instância e os dados do usuário.

Considerações

Para evitar problemas com a recuperação de metadados de instância, considere os aspectos a seguir.

Formato do comando

O formato do comando é diferente dependendo de se IMDSv1 ou IMDSv2 é usado. Por padrão, é possível usar as duas versões do IMDS. Para exigir o uso do IMDSv2, consulte Usar IMDSv2.

(IMDSv2) Se o IMDSv2 for necessário, o IMDSv1 não funcionará

Para verificar se o IMDSv2 é necessário, selecione a instância para visualizar seus detalhes. O valor para IMDSv2 é Obrigatório (você deve usar IMDSv2) ou Opcional (é possível usar IMDSv2 ou IMDSv1).

(IMDSv2) Use /latest/api/token para recuperar o token

Emitir solicitações `PUT` para qualquer caminho específico da versão, por exemplo `/2021-03-23/api/token`, faz com que o serviço de metadados retorne erros 403 Forbidden. Este é o comportamento pretendido.

Suporte a IPv6

Para recuperar metadados da instância usando um endereço IPv6, certifique-se de habilitar e usar `[fd00:ec2::254]` em vez do endereço IPv4. A instância deve ser criada no AWS Nitro System e executada em uma sub-rede compatível com IPv6.

(Windows) Criar AMIs personalizadas usando o Sysprep do Windows.

Para garantir que o IMDS funcione quando você iniciar uma instância usando uma AMI personalizada do Windows, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows. Caso contrário, o IMDS não funcionará. Para obter mais informações, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.

Em um ambiente de contêiner, defina o limite de saltos como 2.

Os SDKs da AWS usam chamadas IMDSv2 por padrão. Se a chamada IMDSv2 não receber resposta, o SDK tenta novamente o atendimento e, se houver falha, usa IMDSv1. Isso pode resultar em um atraso, especialmente em um ambiente de contêiner. Em um ambiente de

contêiner, se o limite de salto for 1, a resposta de IMDSv2 não retorna porque ir ao contêiner é considerado um salto de rede adicional. Para evitar o processo de recuar para IMDSv1 e o atraso resultante, em um ambiente de contêiner recomendamos que você defina o limite de salto como 2. Para ter mais informações, consulte Configurar as opções de metadados da instância.

Versão de metadados

Para evitar ter que atualizar seu código sempre que o Amazon EC2 lançar uma nova compilação de metadados de instância, recomendamos que você use `latest` no caminho em vez do número da versão.

Respostas e mensagens de erro

Todos os metadados de instância são retornados como texto (tipo de conteúdo HTTP `text/plain`).

Uma solicitação para um recurso de metadados específico retorna o valor apropriado, ou um código de erro de HTTP `404 - Not Found` se o recurso não estiver disponível.

Uma solicitação de um recurso de metadados geral (o URI termina com /) retorna uma lista de recursos disponíveis, ou um código de erro de HTTP `404 - Not Found` se não houver esse recurso. Os itens da lista estão em linhas separadas que são delimitadas por caracteres de alimentação de linha (ASCII 10).

Para solicitações feitas usando o Serviço de metadados da instância versão 2, os seguintes códigos de erro HTTP podem ser retornados:

- `400 - Missing or Invalid Parameters` – a solicitação PUT não é válida.
- `401 - Unauthorized` – a solicitação `GET` usa um token inválido. A ação recomendada é gerar um novo token.
- `403 - Forbidden`: a solicitação não é permitida ou o IMDS está desativado.

Exemplos para IMDSv2

Execute os exemplos a seguir na sua instância do Amazon EC2 para recuperar os metadados da instância para o IMDSv2.

Em instâncias do Windows, é possível usar o Windows PowerShell ou instalar cURL ou wget. Se você instalar uma ferramenta de terceiros em uma instância do Windows, leia a documentação que a acompanha, pois as chamadas e a saída podem ser diferentes do que é descrito aqui.

Exemplos

- Obter as versões disponíveis dos metadados da instância
- Obter itens de metadados de nível superior.
- Obtenção dos valores dos itens de metadados
- Obter a lista de chaves públicas disponíveis
- Mostrar os formatos nos quais a chave pública 0 está disponível
- Obter a chave pública 0 (no formato de chave OpenSSH)
- Obter o ID de sub-rede de uma instância
- Obter as tags de instância de uma instância de uma instância

Obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Cada versão indica uma compilação de metadados de instância quando novas categorias de metadados de instância foram lançadas. As versões de compilação de metadados de instância não têm correlação com as versões de API do Amazon EC2. As versões anteriores estarão disponíveis caso você tenha scripts que contam com a estrutura e as informações presentes em uma versão anterior.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
```

```
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obter itens de metadados de nível superior.

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações sobre os itens na resposta, consulte Categorias de metadados da instância.

Observe que as tags serão incluídas nessa saída somente se você tiver permitido o acesso. Para ter mais informações, consulte the section called “Permitir acesso a tags em metadados de instância”.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
```

```
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenção dos valores dos itens de metadados

Esses exemplos obtêm os valores de alguns dos itens de metadados de nível superior obtidos no exemplo anterior. Essas solicitações usam o token armazenado que foi criado usando o comando no exemplo anterior. O token não pode estar expirado.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obter a lista de chaves públicas disponíveis

Este exemplo obtém uma lista de chaves públicas disponíveis.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Mostrar os formatos nos quais a chave pública 0 está disponível

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obter a chave pública 0 (no formato de chave OpenSSH)

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
```

```
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obter o ID de sub-rede de uma instância

Este exemplo obtém o ID de sub-rede para uma instância.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obter as tags de instância de uma instância de uma instância

Estes exemplos acessam as tags de uma instância. É necessário permitir o acesso às tags antes de usar esses exemplos.

cURL

Este exemplo obtém todas as chaves de tag para uma instância.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

O exemplo a seguir obtém o valor da chave `Name` que foi obtida no exemplo anterior. A solicitação de IMDSv2 usa o token armazenado que foi criado com o comando no exemplo anterior. O token não pode estar expirado.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Este exemplo obtém todas as chaves de tag para uma instância.

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

O exemplo a seguir obtém o valor da chave `Name` que foi obtida no exemplo anterior. A solicitação de IMDSv2 usa o token armazenado que foi criado com o comando no exemplo anterior. O token não pode estar expirado.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

Exemplos para IMDSv1

Execute os exemplos a seguir na sua instância do Amazon EC2 para recuperar os metadados da instância para o IMDSv1.

Em instâncias do Windows, é possível usar o Windows PowerShell ou instalar cURL ou wget. Se você instalar uma ferramenta de terceiros em uma instância do Windows, leia a documentação que a acompanha, pois as chamadas e a saída podem ser diferentes do que é descrito aqui.

Exemplos

- Obter as versões disponíveis dos metadados da instância
- Obter itens de metadados de nível superior.
- Obtenção dos valores dos itens de metadados
- Obter a lista de chaves públicas disponíveis
- Mostrar os formatos nos quais a chave pública 0 está disponível
- Obter a chave pública 0 (no formato de chave OpenSSH)
- Obter o ID de sub-rede de uma instância
- Obter as tags de instância de uma instância de uma instância

Obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Cada versão indica uma compilação de metadados de instância quando novas categorias de metadados de instância foram

lançadas. As versões de compilação de metadados de instância não têm correlação com as versões de API do Amazon EC2. As versões anteriores estarão disponíveis caso você tenha scripts que contam com a estrutura e as informações presentes em uma versão anterior.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
```

```
2015-10-20
2016-04-19
...
latest
```

Obter itens de metadados de nível superior.

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações sobre os itens na resposta, consulte Categorias de metadados da instância.

Observe que as tags serão incluídas nessa saída somente se você tiver permitido o acesso. Para ter mais informações, consulte the section called “Permitir acesso a tags em metadados de instância”.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenção dos valores dos itens de metadados

Esses exemplos obtêm os valores de alguns dos itens de metadados de nível superior obtidos no exemplo anterior.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
```

```
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obter a lista de chaves públicas disponíveis

Este exemplo obtém uma lista de chaves públicas disponíveis.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Mostrar os formatos nos quais a chave pública 0 está disponível

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Obter a chave pública 0 (no formato de chave OpenSSH)

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
```

```
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obter o ID de sub-rede de uma instância

Este exemplo obtém o ID de sub-rede para uma instância.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obter as tags de instância de uma instância de uma instância

Estes exemplos acessam as tags de uma instância. É necessário permitir o acesso às tags antes de usar esses exemplos.

cURL

Este exemplo obtém todas as chaves de tag para uma instância.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
```

```
Environment
```

O exemplo a seguir obtém o valor da chave Name que foi obtida no exemplo anterior.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Este exemplo obtém todas as chaves de tag para uma instância.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

O exemplo a seguir obtém o valor da chave Name que foi obtida no exemplo anterior.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/
instance/Name
MyInstance
```

Limitação de consulta

Controlamos a utilização de consultas ao IMDS em uma base por instância, e limitamos o número de conexões simultâneas de uma instância com o IMDS.

Se você estiver usando o IMDS para recuperar as credenciais de segurança da AWS, evite consultar as credenciais durante cada transação ou simultaneamente em um número elevado de threads ou processos, pois isso pode levar a uma limitação. Em vez disso, recomendamos que você armazene em cache as credenciais até elas começarem a se aproximar da data de expiração. Para obter mais informações sobre o perfil do IAM e as credenciais de segurança associadas ao perfil, consulte Recuperar credenciais de segurança dos metadados da instância.

Se você ficar limitado ao acessar o IMDS, tente a consulta novamente com uma estratégia de recuo exponencial.

Limite de acesso ao IMDS

É possível considerar o uso de regras do firewall local para desabilitar o acesso de alguns ou de todos os processos para o IMDS.

Para instâncias desenvolvidas no AWS Nitro System, o IMDS pode ser acessado usando a própria rede quando um dispositivo de rede na VPC, como um roteador virtual, encaminha pacotes para o endereço do IMDS e a verificação de origem e de destino padrão na instância está desabilitada. Para evitar que uma fonte externa à VPC acesse o IMDS, recomendamos que você modifique a configuração do dispositivo de rede para descartar pacotes com o endereço IPv4 de destino do IMDS `169.254.169.254` e, se você tiver habilitado o endpoint IPv6, o endereço IPv6 do IMDS `[fd00:ec2::254]`.

Instâncias do Linux

Usar iptables para limitar o acesso

O exemplo a seguir usa iptables do Linux e seu módulo `owner` para impedir que o servidor Web do Apache (com base no ID de usuário da instalação padrão do `apache`) acesse 169.254.169.254. Ele usa uma regra de negação para rejeitar todas as solicitações de metadados de instância (IMDSv1 ou IMDSv2) de qualquer processo que execute como esse usuário.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Ou é possível considerar permitir o acesso apenas a usuários ou grupos específicos usando regras de permissão. As regras de permissão podem ser mais fáceis de gerenciar de uma perspectiva de segurança, porque elas exigem que você decida qual software precisa acessar os metadados de instância. Se você usar regras de permissão, haverá menos probabilidade de você permitir acidentalmente que o software acesse o serviço de metadados (que você não queria que tivesse acesso) se você alterar o software ou a configuração posteriormente em uma instância. Também é possível combinar o uso de grupos com regras de permissão, para que você possa adicionar ou remover usuários de um grupo com permissão sem precisar alterar a regra do firewall.

O exemplo a seguir impede o acesso ao IMDS por todos os processos, exceto os processos em execução na conta do usuário `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.

- Por padrão, as regras de iptables não são persistentes em todas as reinicializações do sistema. Elas podem ser transformadas em persistentes usando recursos do SO não descritos aqui.
- O módulo `owner` das iptables só corresponderá à associação do grupo se o grupo for o grupo primário de um determinado usuário local. Outros grupos não são correspondidos.

Usar PF ou IPFW para limitar o acesso

Se você estiver usando FreeBSD ou OpenBSD, poderá considerar também o uso de PF ou IPFW. Os exemplos a seguir limitam o acesso ao IMDS apenas ao usuário raiz.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> A ordem dos comandos PF e IPFW é importante. O padrão de PF e a regra correspondente mais recente, e o padrão de IPFW é a primeira regra correspondente.

Instâncias do Windows

Usar o firewall do Windows para limitar o acesso

O seguinte PowerShell de exemplo usa o firewall interno do Windows para impedir que o servidor Web do Servidor de informações da Internet (com base no ID de usuário de sua instalação padrão de

NT AUTHORITY\IUSR) acesse 169.254.169.254. Ele usa uma regra de negação para rejeitar todas as solicitações de metadados de instância (IMDSv1 ou IMDSv2) de qualquer processo que execute como esse usuário.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Ou é possível considerar permitir o acesso apenas a usuários ou grupos específicos usando regras de permissão. As regras de permissão podem ser mais fáceis de gerenciar de uma perspectiva de segurança, porque elas exigem que você decida qual software precisa acessar os metadados de instância. Se você usar regras de permissão, haverá menos probabilidade de você permitir acidentalmente que o software acesse o serviço de metadados (que você não queria que tivesse acesso) se você alterar o software ou a configuração posteriormente em uma instância. Também é possível combinar o uso de grupos com regras de permissão, para que você possa adicionar ou remover usuários de um grupo com permissão sem precisar alterar a regra do firewall.

O exemplo a seguir impede o acesso aos metadados da instância por todos os processos em execução como um grupo do SO especificado na variável `blockPrincipal` (neste exemplo, o grupo `Everyone` do Windows), exceto os processos especificados em `exceptionPrincipal` (neste exemplo, um grupo chamado `trustworthy-users`). Especifique as entidades de negação e de permissão porque o Firewall do Windows, ao contrário da regra `! --uid-owner trustworthy-user` nas iptables do Linux, não fornece um mecanismo de atalho para permitir somente uma entidade específica (usuário ou grupo) negando todas as outras.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
```

```
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.

Usar regras de netsh para limitar o acesso

É possível considerar o bloqueio de todos os softwares usando regras de `netsh`, mas essas regras são muito menos flexíveis.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.
> - As regras de `netsh` devem ser definidas em um prompt de comando elevado e não podem ser definidas para negar ou permitir principais específicos.

Trabalhar com dados do usuário da instância

Você pode usar os dados do usuário da instância para personalizar as instâncias. Quando você inicia uma instância, pode armazenar parâmetros ou scripts como dados do usuário. Todos os scripts nos dados do usuário são executados ao iniciar a instância. Você pode visualizar os dados do usuário como um atributo da instância. Você também pode visualizar os dados do usuário da instância por meio do serviço de metadados de instância (IMDS).

Considerações

- Os dados do usuário são tratados como dados opacos: o que você especifica é o que receberá de volta na recuperação. Cabe à instância interpretar e agir com base nos dados do usuário.

- Os dados do usuário devem ser codificados por base64. Dependendo da ferramenta ou do SDK que você está usando, a codificação base64 pode ser executada para você. Por exemplo:
  - O console do Amazon EC2 pode executar a codificação base64 para você ou aceitar a entrada codificada por base64.
  - A AWS CLI versão 2 executa a codificação base64 de parâmetros binários para você por padrão. A AWS CLI versão 1 executa a codificação base64 do `--user-data` parâmetro para você.
  - O AWS SDK for Python (Boto3) executa a codificação base64 do parâmetro `UserData` para você.
- Os dados do usuário são limitados a 16 KB, na forma bruta, antes de serem codificados em base64. O tamanho de uma string de comprimento n depois que a codificação em base64 for ceil (n/3)*4.
- Os dados do usuário devem ser decodificados em base64 quando você os recupera. Se você recuperar os dados usando o console ou os metadados da instância, eles serão decodificados automaticamente para você.
- Se você interromper uma instância, modificar os dados do usuário e iniciar a instância, os dados do usuário atualizados não serão executados automaticamente quando você iniciar a instância. Com as instâncias do Windows, é possível definir configurações para que os scripts de dados do usuário atualizados sejam executados uma vez quando você inicia a instância ou sempre que você reinicia ou inicia a instância.
- Os dados do usuário são um atributo da instância. Se você criar uma AMI a partir de uma instância, os dados do usuário da instância não serão incluídos na AMI.

Especificar os dados do usuário da instância no lançamento

É possível especificar dados do usuário quando você executar uma instância. Para obter instruções para o console, consulte Especificar os dados do usuário da instância no lançamento. Para obter um exemplo do Linux que usa a AWS CLI, consulte the section called “Dados do usuário e AWS CLI”. Para obter um exemplo do Windows que usa o Tools for Windows PowerShell, consulte the section called “Dados do usuário e Tools for Windows PowerShell”.

Modificar os dados do usuário da instância

Você pode modificar os dados do usuário das instâncias com um volume raiz do EBS. A instância deve estar no estado interrompido. Para obter instruções para o console, consulte Visualizar e atualizar os dados do usuário da instância. Para obter um exemplo do Linux que usa a AWS CLI,

consulte modify-instance-attribute. Para obter um exemplo do Windows que usa o Tools for Windows PowerShell, consulte the section called “Dados do usuário e Tools for Windows PowerShell”.

Recuperar os dados do usuário da instância da sua instância

Para recuperar os dados do usuário de uma instância, use um dos URIs a seguir. Para recuperar dados do usuário usando o endereço IPv6, você deve habilitá-lo, e a instância deve ser uma instância criada no AWS Nitro System em uma sub-rede compatível com IPv6.

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Uma solicitação de dados do usuário retorna os dados no estado em que se encontram (tipo de conteúdo `application/octet-stream`). Se a instância não tiver dados do usuário, a solicitação retornará `404 - Not Found`.

Exemplo: Recuperar texto separado por vírgula

Este exemplo recupera dados do usuário que foram especificados como texto separado por vírgulas.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod
 -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Exemplo: recuperar um script

Este exemplo retorna dados do usuário que foram especificados como um script.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
```

```
service httpd start
chkconfig httpd on
```

Powershell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Recuperar os dados do usuário da instância do seu computador

Você pode recuperar os dados do usuário de uma instância do seu próprio computador. Para obter instruções para o console, consulte Visualizar e atualizar os dados do usuário da instância. Para obter um exemplo que usa a AWS CLI, consulte Dados do usuário e AWS CLI. Para obter um exemplo que usa o Tools for Windows PowerShell, consulte Dados do usuário e Tools for Windows PowerShell.

Execução de comandos na instância do Amazon EC2 na inicialização

Ao iniciar uma instância do Amazon EC2, é possível transferir dados do usuário para a instância que é usada para executar tarefas de configuração automatizadas ou para executar scripts após o início da instância.

Se você estiver interessado em cenários de automação mais complexos, considere usar AWS CloudFormation e AWS OpsWorks. Para obter mais informações, consulte as informações a seguir.

- Implantar aplicações no Amazon EC2 com AWS CloudFormation no Guia do usuário do AWS CloudFormation.
- Manual do usuário do AWS OpsWorks.

Em instâncias do Linux, é possível transferir dois tipos de dados do usuário para o Amazon EC2, nomeadamente, os scripts de shell e diretivas do cloud-init. Além disso, é possível transferir esses dados para o assistente de inicialização de instâncias como texto simples, como um arquivo (isso é útil para iniciar instâncias com as ferramentas de linha de comando) ou como texto codificado em base64 (para chamadas de API).

Nas instâncias do Windows, os agentes de inicialização gerenciam os scripts de dados do usuário. As seções apresentadas a seguir abordam as diferenças na forma em que os dados do usuário são tratados em cada sistema operacional.

Como o Amazon EC2 lida com os dados dos usuários para instâncias do Linux

Nos exemplos a seguir, os comandos de Instalar um servidor LAMP no Amazon Linux 2 são convertidos em um script de shell e um conjunto de diretivas de cloud-init que são executados quando a instância é iniciada. Em cada exemplo, as seguintes tarefas são executadas pelos dados do usuário:

- Os pacotes de distribuição de software são atualizados.
- O servidor web necessário, `php`, e os pacotes `mariadb` são instalados.
- O serviço `httpd` é iniciado e ativado por systemctl.
- O grupo de segurança `ec2-user` é adicionado ao grupo apache.
- As permissões de propriedade e de arquivos apropriadas são definidas para o diretório Web e os arquivos contidos nele.
- Uma página Web simples é criada para testar o servidor Web e o mecanismo de PHP.

Conteúdos

- Pré-requisitos
- Dados de usuário e scripts de shell

- Dados do usuário e console
- Diretivas de cloud-init e dados de usuário
- Dados do usuário e AWS CLI
- Combinar scripts de shell e diretivas de cloud-init

Pré-requisitos

Para os exemplos deste tópico, suponha o seguinte:

- Sua instância tem um nome DNS público que é acessível pela Internet.
- O grupo de segurança associado à sua instância é configurado para permitir tráfego SSH (porta 22), de modo que você possa se conectar à instância para visualizar os arquivos de log de saída.
- Sua instância é iniciada com uma AMI do Amazon Linux 2. Essas instruções são para serem usadas com o Amazon Linux 2, e os comandos e as diretivas podem não funcionar para outras distribuições do Linux. Para obter mais informações sobre outras distribuições, como suporte para cloud-init, consulte a documentação específica.

Dados de usuário e scripts de shell

Se você estiver familiarizado com scripts de shell, esta é a maneira mais fácil e completa de enviar instruções para uma instância na execução. Se você adicionar essas tarefas no momento da inicialização, será necessário mais tempo para iniciar a instância. É necessário reservar alguns minutos extras para que as tarefas sejam concluídas antes de testar se o script de usuário foi concluído com êxito.

> **Important**
>
> Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. É possível atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? (Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância do Linux do Amazon EC2?) na Central de Conhecimento da AWS.

Os scripts de shell de dados de usuário devem ser iniciados pelos caracteres `#!` e pelo caminho para o intérprete que você deseja que leia o script (geralmente /bin/bash). Para uma introdução sobre scripts de shell, consulte o Manual de referência do Bash no site do Sistema operacional GNU.

Os scripts inseridos como dados de usuário são executados como usuário raiz,, portanto, não use o comando sudo no script. Lembre-se de que todos os arquivos que você criar serão de propriedade do usuário raiz. Caso precise que um usuário não raiz tenha acesso aos arquivos, modifique as permissões em conformidade com o script. Além disso, como o script não é executado interativamente, você não pode incluir os comandos que exigem feedback do usuário (como yum update sem o sinalizador `-y`).

Se você usar uma API da AWS, incluindo a CLI da AWS em um script de dados de usuário, deverá usar um perfil de instância ao inicializar a instância. Um perfil de instância fornece as credenciais apropriadas da AWS exigidas pelo script de dados do usuário para emitir a chamada de API. Para obter mais informações, consulte Usar perfis de instâncias no Guia do usuário do IAM. As permissões que atribui à função do IAM dependem de quais serviços você chama com a API. Para ter mais informações, consulte Funções do IAM para Amazon EC2.

O arquivo de log de saída de cloud-init captura a saída do console para facilitar a depuração de seus scripts após uma execução se a instância não se comportar da maneira desejada. Para exibir o arquivo de log, conecte-se à instância e abra `/var/log/cloud-init-output.log`.

Quando um script de dados do usuário é processado, ele é copiado para e executado a partir deste diretório `/var/lib/cloud/instances/`*`instance-id`*`/`. O script não é excluído depois de ser executado. Certifique-se de excluir os scripts de dados do usuário de `/var/lib/cloud/instances/`*`instance-id`*`/` antes de criar uma AMI a partir da instância. Caso contrário, o script existirá nesse diretório em qualquer instância iniciada na AMI.

Dados do usuário e console

É possível especificar os dados do usuário da instância ao executar uma instância. Se o volume raiz da instância for um volume do EBS, também é possível parar a instância e atualizar os dados de usuário.

Especificar os dados do usuário da instância no lançamento

Siga o procedimento para iniciar uma instância. O campo User data (Dados do usuário) está localizado na seção Detalhes avançados do assistente de inicialização de instância. Insira seu script shell no campo User data (Dados do usuário) e conclua o procedimento de inicialização de instância.

Este script de exemplo cria e configura nosso servidor Web.

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Reserve tempo suficiente para executar a instância e execute os comandos do script. Depois, verifique se o script concluiu as tarefas previstas.

Em nosso exemplo, em um navegador Web, insira o URL do arquivo de teste PHP criado pelo script. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

É necessário consultar a página de informações do PHP. Caso não seja possível visualizar a página de informações do PHP, verifique se o security group que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para ter mais informações, consulte Adicionar regras a um grupo de segurança.

(Opcional) Se o script não tiver realizado as tarefas você esperava ou se você quiser simplesmente verificar se o script foi concluído sem erros, conecte-se à instância, examine o arquivo de log de saída de cloud-init (`/var/log/cloud-init-output.log`) e procure mensagens de erro na saída.

Para informações adicionais de depuração, é possível criar um arquivo multiparte Mime que inclua uma seção de dados de cloud-init com a seguinte diretiva:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Essa diretiva envia a saída do comando do script para `/var/log/cloud-init-output.log`. Para obter mais informações sobre os formatos de dados de cloud-init e a criação de arquivos multiparte Mime, consulte Formatos de cloud-init.

Visualizar e atualizar os dados do usuário da instância

Para atualizar os dados do usuário da instância, primeiro é necessário interromper a instância. Se a instância estiver em execução, será possível visualizar os dados do usuário, mas não modificá-los.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Para modificar os dados do usuário da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.
4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário).
6. Modifique os dados do usuário conforme necessário e escolha Save (Salvar).
7. Inicie a instância. Os novos dados do usuário ficam visíveis na instância depois que você a inicia. Contudo, os scripts dos dados do usuário não são executados.

Diretivas de cloud-init e dados de usuário

O pacote de cloud-init configura aspectos específicos de uma nova instância do Amazon Linux quando ela é executada. Em particular, ele configura o arquivo `.ssh/authorized_keys` para o usuário ec2 para que você possa se conectar com sua própria chave privada. Para obter mais informações sobre as tarefas de configuração que o pacote de cloud-init executa para instâncias do Amazon Linux, consulte Using cloud-init on Amazon Linux 2 no Amazon Linux 2 User Guide.

As diretivas de cloud-init podem ser passadas a uma instância em execução da mesma forma que um script é passado, embora a sintaxe seja diferente. Para obter mais informações sobre o cloud-init, consulte http://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. É possível atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? (Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância Linux do Amazon EC2?) na Central de Conhecimento da AWS.

Se você adicionar essas tarefas no momento da inicialização, será necessário mais tempo para iniciar uma instância. É necessário reservar alguns minutos extras para que as tarefas sejam concluídas antes de testar se as diretivas de dados de usuário foram concluídas.

Para passar diretivas de cloud-init para uma instância com dados de usuário

1. Siga o procedimento para iniciar uma instância. O campo User data (Dados do usuário) está localizado na seção Detalhes avançados do assistente de inicialização de instância. Insira o texto da diretiva cloud-init no campo User data (Dados do usuário) e conclua o procedimento de inicialização de instância.

   No exemplo a seguir, as diretivas criam e configuram um servidor Web no Amazon Linux 2. A linha `#cloud-config` na parte superior é necessária para identificar os comandos como diretrizes cloud-init.

   ```
   #cloud-config
   repo_update: true
   repo_upgrade: all

   packages:
   - httpd
   - mariadb-server

   runcmd:
   ```

```
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Reserve tempo suficiente para que a instância seja executada e execute as diretivas nos dados de usuário. Depois, verifique se as diretivas concluíram as tarefas previstas.

   Para este exemplo, em um navegador da Web, insira a URL do arquivo de teste PHP criado pelas diretivas. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   É necessário consultar a página de informações do PHP. Caso não seja possível visualizar a página de informações do PHP, verifique se o security group que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para ter mais informações, consulte Adicionar regras a um grupo de segurança.

3. (Opcional) Se as diretivas não tiverem realizado as tarefas que você esperava ou se você quiser simplesmente verificar se as diretivas foram concluídas sem erros, conecte-se à instância, examine o arquivo de log de saída (`/var/log/cloud-init-output.log`) e procure mensagens de erro na saída. Para informações adicionais de depuração, é possível adicionar a seguinte linha às diretivas:

   ```
   output : { all : '| tee -a /var/log/cloud-init-output.log' }
   ```

   Essa diretiva orientadora envia a saída runcmd para `/var/log/cloud-init-output.log`.

Dados do usuário e AWS CLI

É possível usar AWS CLI para especificar, modificar e ver os dados do usuário para sua instância. Para obter informações sobre como visualizar os dados do usuário da sua instância usando metadados de instância, consulte Recuperar os dados do usuário da instância da sua instância.

No Windows, é possível usar o AWS Tools for Windows PowerShell em vez de usar a AWS CLI. Para obter mais informações, consulteDados do usuário e Tools for Windows PowerShell

Exemplo: especificar dados do usuário na execução

Para especificar dados de usuário ao executar a instância, use o comando run-instances com o parâmetro `--user-data`. Com run-instances, a AWS CLI executa codificação de base64 dos dados de usuário para você.

O exemplo a seguir mostra como especificar um script como uma string na linha de comando:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

O exemplo a seguir mostra como especificar um script usando um arquivo de texto. Certifique-se de usar o prefixo `file://` para especificar o arquivo.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

A seguir, temos um exemplo de arquivo de texto com um script de shell.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Exemplo: modificar os dados do usuário de uma instância interrompida

É possível modificar os dados de usuário de uma instância interrompida usando o comando modify-instance-attribute. Com modify-instance-attribute, a AWS CLI não executa a codificação de base64 dos dados de usuário para você.

- Em um computador Linux, use o comando base64 para codificar os dados de usuário.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Em um computador Windows, use o comando certutil para codificar os dados de usuário. Para poder usar esse arquivo com a AWS CLI, é necessário remover as primeiras (INICIAR CERTIFICADO) e últimas (ENCERRAR CERTIFICADO) linhas.

```
certutil -encode my_script.txt my_script_base64.txt
notepad my_script_base64.txt
```

Use os parâmetros `--attribute` e `--value` para usar o arquivo de texto codificado para especificar os dados de usuário. Certifique-se de usar o prefixo `file://` para especificar o arquivo.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Exemplo: limpar os dados do usuário de uma instância interrompida

Para excluir os dados do usuário existentes, use o comando modify-instance-attribute da seguinte maneira:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Exemplo: visualizar dados do usuário

Para recuperar os dados de usuário de uma instância, use o comando describe-instance-attribute. Com describe-instance-attribute, a AWS CLI não executa a decodificação de base64 dos dados de usuário para você.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Esta é uma saída de exemplo com dados de usuário com codificação base64.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Em um computador Linux, use a opção `--query` para obter os dados de usuário codificados e o comando base64 para descodificá-los.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" | base64 --decode
```

- Em um computador Windows, use a opção `--query` para obter os dados de usuário codificados e o comando certutil para descodificá-los. Observe que a saída codificada está armazenada em um arquivo e a saída descodificada está armazenada em outro arquivo.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" >my_output.txt
certutil -decode my_output.txt my_output_decoded.txt
type my_output_decoded.txt
```

O seguinte é um exemplo de saída.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combinar scripts de shell e diretivas de cloud-init

Por padrão, você só pode incluir um tipo de conteúdo em dados de usuário de cada vez. Porém, você pode usar os tipos de conteúdo `text/cloud-config` e `text/x-shellscript` em um arquivo mime-multi part para incluir um script de shell e diretivas de cloud-init nos dados de usuário.

O exemplo a seguir mostra o formato mime-multi part.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
```

```
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Por exemplo, os seguintes dados de usuário incluem diretivas cloud-init e um script de shell bash. As diretivas cloud-init criam um arquivo (`/test-cloudinit/cloud-init.txt`) e gravam `Created by cloud-init` nesse arquivo. O script de shell bash cria um arquivo (`/test-userscript/userscript.txt`) e grava `Created by bash shell script` nesse arquivo.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
```

```
--//--
```

Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows

Nas instâncias do Windows, os agentes de inicialização padrão para a versão do seu sistema operacional tratam os dados do usuário da maneira descrita a seguir.

- O EC2Launch v2 executa os scripts de dados do usuário no Windows Server 2022
- O EC2Launch executa os scripts de dados do usuário no Windows Server 2016 e 2019
- O Serviço EC2Config executa os scripts de dados do usuário em versões do Windows Server anteriores ao Windows Server 2016

Para obter exemplos de assembly de uma propriedade `UserData` em um modelo do AWS CloudFormation, consulte Propriedade UserData codificada em Base64 e Propriedade UserData codificada em Base64 com AccessKey e SecretKey.

Para obter um exemplo de comandos de execução em uma instância dentro de um grupo do Auto Scaling que funciona com ganchos do ciclo de vida, consulte Tutorial: Configure user data to retrieve the target lifecycle state through instance metadata no Guia do usuário do Amazon EC2 Auto Scaling.

Conteúdo

- Scripts de dados do usuário
- Execução de dados do usuário
- Dados do usuário e console
- Dados do usuário e Tools for Windows PowerShell

Scripts de dados do usuário

Para que o `EC2Config` ou o `EC2Launch` execute scripts, é necessário colocar o script em uma etiqueta especial ao adicioná-lo aos dados do usuário. A tag usada depende de os comandos serem executados em uma janela de prompt de comando (comandos de lote) ou usando o Windows PowerShell.

Se você especificar um script em lote e um script do Windows PowerShell, o script em lote é executado primeiro e o script do Windows PowerShell é executado em seguida, independentemente da ordem em que eles aparecem nos dados do usuário da instância.

Se você usar uma API da AWS, incluindo a AWS CLI, em um script de dados de usuário, deverá usar um perfil de instância ao inicializar a instância. Um perfil de instância fornece as credenciais apropriadas da AWS exigidas pelo script de dados do usuário para executar a chamada de API. Para ter mais informações, consulte Perfis de instância. As permissões que atribui à função do IAM dependem de quais serviços você chama com a API. Para ter mais informações, consulte Funções do IAM para Amazon EC2.

Tipo de script

- Sintaxe para scripts em lote
- Sintaxe para scripts do Windows PowerShell
- Sintaxe para scripts de configuração YAML
- Codificação base64

Sintaxe para scripts em lote

Especifique um script em lote usando a tag `script`. Separe os comandos usando quebras de linha, conforme mostrado no exemplo a seguir.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

Agente do EC2Launch v2

Para executar um script de dados do usuário XML como um processo separado com a tarefa executeScript do EC2Launch v2 no estágio `UserData`, adicione `<detach>true</detach>` aos dados do usuário.

> **Note**
>
> A tag detach não é compatível com agentes de inicialização anteriores.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Sintaxe para scripts do Windows PowerShell

As AMIs do Windows da AWS incluem o AWS Tools for Windows PowerShell para que você possa especificar esses cmdlets nos dados do usuário. Se você associar uma função do IAM à sua instância, não será necessário especificar as credenciais para os cmdlets, pois os aplicações em execução na instância usam as credenciais da função para acessar os recursos da AWS (por exemplo, buckets do Amazon S3).

Especifique um script do Windows PowerShell usando a tag `<powershell>`. Separe os comandos usando quebras de linha. A tag `<powershell>` não diferencia maiúsculas de minúsculas.

Por exemplo:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

É possível especificar um ou mais argumentos do PowerShell com tag `<powershellArguments>`. Se nenhum argumento for passado, o EC2Launch e o EC2Launch v2 adicionarão o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

Exemplo:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Agente do EC2Launch v2

Para executar um script de dados do usuário XML como um processo separado com a tarefa executeScript do EC2Launch v2 no estágio `UserData`, adicione `<detach>true</detach>` aos dados do usuário.

> **Note**
>
> A tag detach não é compatível com agentes de inicialização anteriores.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Sintaxe para scripts de configuração YAML

Se você estiver usando o EC2Launch v2 para executar scripts, poderá usar o formato YAML. Para visualizar tarefas de configuração, detalhes e exemplos do EC2Launch v2, consulte Configuração de tarefas do EC2Launch v2.

Especifique um script YAML com a tarefa `executeScript`.

Exemplo de sintaxe do YAML para executar um script do PowerShell

```
version: 1.0
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: powershell
        runAs: localSystem
        content: |-
          $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
          New-Item $file -ItemType file
```

Exemplo de sintaxe do YAML para executar um script em lote

```
version: 1.1
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: batch
        runAs: localSystem
        content: |-
          echo Current date and time >> %SystemRoot%\Temp\test.log
          echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codificação base64

Se você estiver usando a API do Amazon EC2 ou uma ferramenta que não execute codificação base64 dos dados do usuário, codifique você mesmo os dados do usuário. Caso contrário, será registrado um erro sobre não ser possível encontrar as tags `script` ou `powershell` para executar. A seguir está um exemplo que codifica usando o Windows PowerShell.

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

A seguir está um exemplo que decodifica usando o PowerShell.

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Para obter mais informações sobre a codificação base64, consulte https://www.ietf.org/rfc/rfc4648.txt.

Execução de dados do usuário

Por padrão, todas as AMIs do Windows da AWS têm a execução de dados de usuário habilitada para a execução inicial. É possível especificar que os scripts de dados do usuário sejam executados na próxima vez que a instância for reiniciada. Também é possível especificar que os scripts de dados do usuário sejam executados toda vez que a instância for reiniciada.

> **Note**
>
> Os dados do usuário não são habilitados para execução por padrão após a inicialização inicial. Para permitir que os dados do usuário sejam executados ao reinicializar ou iniciar a instância, consulte Reinicializações ou inicializações subsequentes.

Os scripts de dados do usuário são executados na conta do administrador local quando uma senha aleatória é gerada. Caso contrário, os scripts de dados do usuário são executados na conta do sistema.

Execução da instância

Os scripts nos dados do usuário da instância são executados durante a execução inicial da instância. Se a tag `persist` for localizada, a execução de dados do usuário será habilitada para reinicializações ou inicializações subsequentes. Os arquivos de log do EC2Launch v2, EC2Launch e EC2Config contêm a saída da saída padrão e dos fluxos de erro padrão.

EC2Launch v2

O arquivo de log para EC2Launch v2 é `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> A pasta `C:\ProgramData` pode estar oculta. Para visualizar a pasta, é necessário mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Info: Converting user-data to yaml format` – Se os dados do usuário tiverem sido fornecidos no formato XML

- `Info: Initialize user-data state`: o início da execução de dados do usuário
- `Info: Frequency is: always` – Se a tarefa de dados do usuário estiver sendo executada em cada inicialização
- `Info: Frequency is: once` – Se a tarefa de dados do usuário estiver sendo executada apenas uma vez
- `Stage: postReadyUserData execution completed` – O final da execução de dados do usuário

EC2Launch

O arquivo de log do EC2Launch é `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

A pasta `C:\ProgramData` pode estar oculta. Para visualizar a pasta, é necessário mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Userdata execution begins`: o início da execução de dados do usuário
- `<persist> tag was provided: true` –se a etiqueta persist for encontrada
- `Running userdata on every boot` –se a etiqueta persist for encontrada
- `<powershell> tag was provided.. running powershell content`: se a tag powershell for encontrada
- `<script> tag was provided.. running script content` – se a etiqueta script for encontrada
- `Message: The output from user scripts` – Se os scripts de dados do usuário forem executados, a saída será registrada

EC2Config

O arquivo de log do EC2Config é `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. As informações a seguir são registradas quando os dados do usuário são executados.

- `Ec2HandleUserData: Message: Start running user scripts`: o início da execução de dados do usuário

- `Ec2HandleUserData: Message: Re-enabled userdata execution` –se a etiqueta persist for encontrada
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>`: se a tag persist não for encontrada
- `Ec2HandleUserData: Message: The output from user scripts` – Se os scripts de dados do usuário forem executados, a saída será registrada

Reinicializações ou inicializações subsequentes

Quando você atualiza os dados do usuário da instância, os scripts de dados do usuário não são executados automaticamente ao reiniciar ou iniciar a instância. No entanto, é possível habilitar a execução de dados do usuário para que eles sejam executados uma vez ao reiniciar ou iniciar a instância, ou sempre que reiniciar ou iniciar a instância.

Se você escolher a opção Shutdown with Sysprep (Desativar com Sysprep), os scripts de dados do usuário serão executados na próxima vez que a instância for reiniciada ou iniciada, mesmo que você não tenha habilitado a execução de dados do usuário para reinicializações ou inicializações subsequentes. Os scripts de dados do usuário não serão executados em reinicializações ou inicializações subsequentes.

Como habilitar a execução de dados do usuário com o EC2Launch v2 (Visualizar AMIs)

- Para executar uma tarefa nos dados do usuário na primeira inicialização, defina `frequency` como `once`.
- Para executar uma tarefa nos dados do usuário em cada inicialização, defina `frequency` como `always`.

Como habilitar a execução de dados do usuário com o EC2Launch (Windows Server 2016 ou versões posteriores)

1. Conecte-se à sua instância do Windows.
2. Abra uma janela de comando do PowerShell e execute o comando a seguir:

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário.

Como habilitar a execução de dados do usuário com EC2Config (Windows Server 2012 R2 e versões anteriores)

1. Conecte-se à sua instância do Windows.
2. Aberto `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Em User Data (Dados do usuário), selecione Enable UserData execution for next service start (Habilitar execução de dados do usuário para o próximo início de serviço).
4. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário.

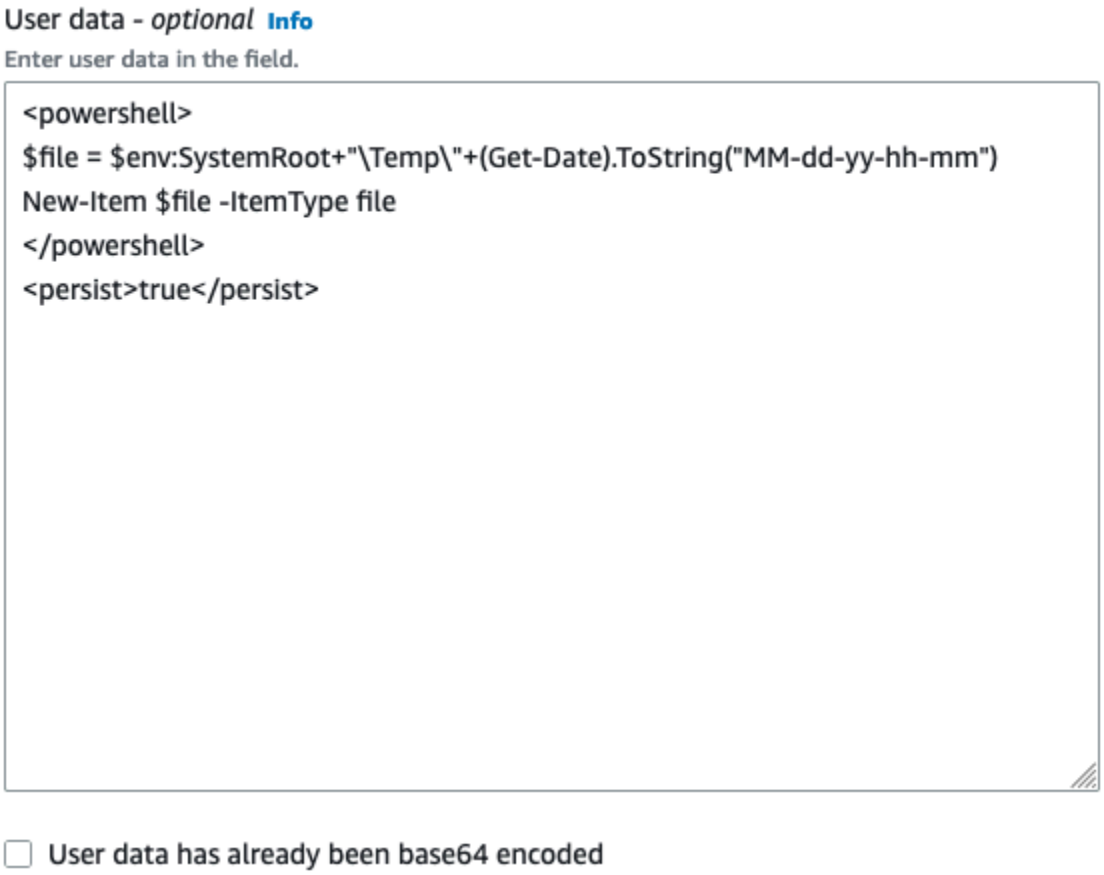
Dados do usuário e console

É possível especificar os dados do usuário da instância ao executar uma instância. Se o volume raiz da instância for um volume do EBS, também é possível parar a instância e atualizar os dados de usuário.

Especificar os dados do usuário da instância no lançamento

Siga o procedimento para iniciar uma instância. O campo User data (Dados do usuário) está localizado na seção Detalhes avançados do assistente de inicialização de instância. Insira seu script do PowerShell no campo Dados do usuário e conclua o procedimento de execução de instância.

Na seguinte captura de tela do campo Dados do usuário, o script de exemplo cria um arquivo na pasta temporária do Windows usando a data e a hora atuais no nome de arquivo. Ao incluir `<persist>true</persist>`, o script é executado sempre que você reiniciar ou iniciar a instância. Se você deixar a caixa de seleção Os dados do usuário já foram codificados em base64 vazia, o console do Amazon EC2 executará a codificação base64 para você.



Visualizar e atualizar os dados do usuário da instância

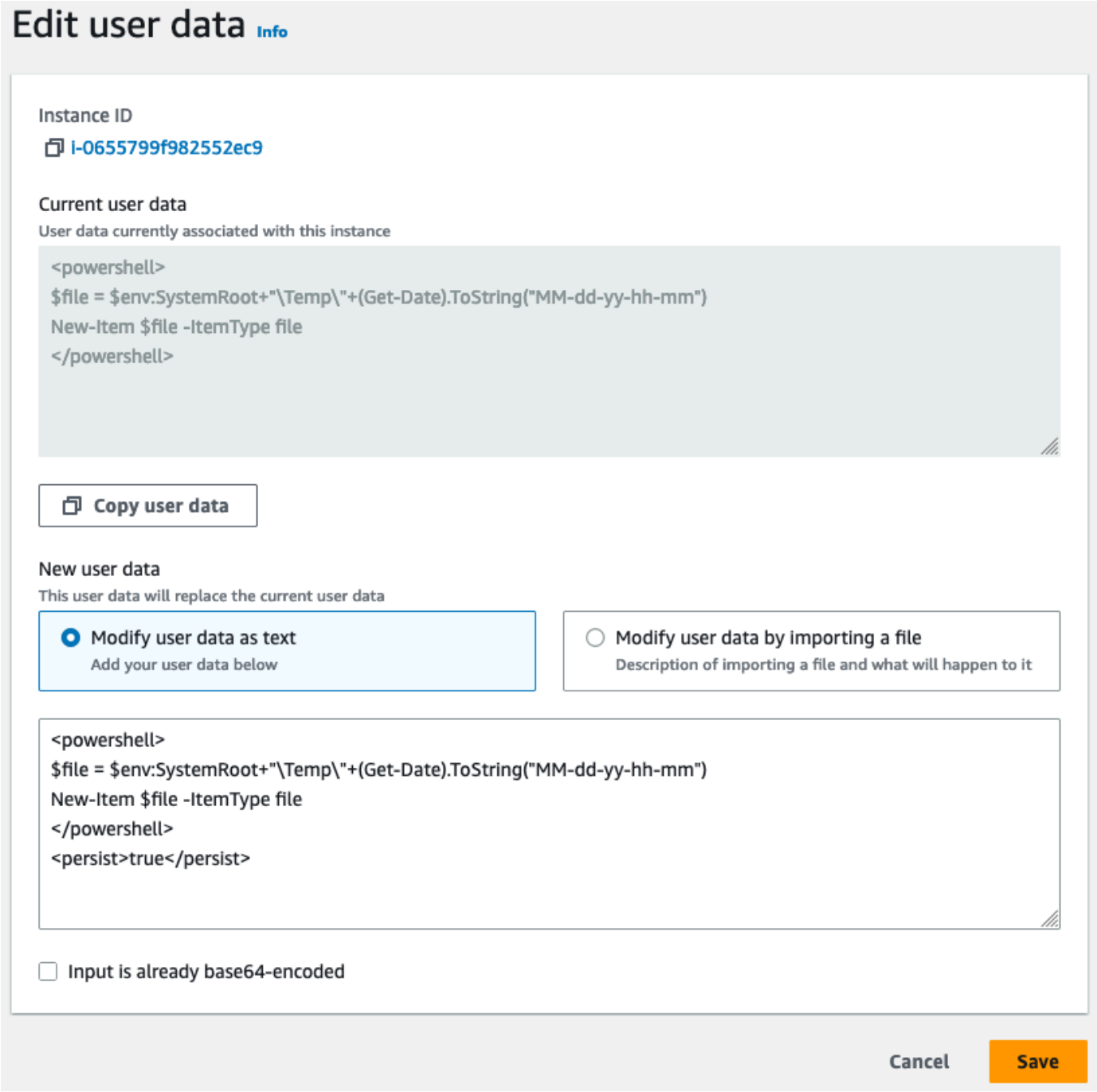
É possível visualizar dados do usuário da instância para qualquer instância e atualizar dados do usuário da instância para uma instância interrompida.

Para atualizar os dados do usuário para uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância).

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário). Não é possível alterar os dados do usuário se a instância estiver em execução, mas é possível visualizá-la.
6. Na caixa de diálogo Edit user data (Editar dados do usuário), atualize os dados do usuário e escolha Save (Salvar). Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>`, como mostrado no exemplo a seguir:



7. Inicie a instância. Se você habilitou a execução de dados do usuário para reinicializações ou inicializações subsequentes, os scripts de dados do usuário atualizados serão executados como parte do processo de inicialização da instância.

Dados do usuário e Tools for Windows PowerShell

É possível usar Tools for Windows PowerShell para especificar, modificar e ver os dados do usuário para sua instância. Para obter informações sobre como visualizar os dados do usuário da sua instância usando metadados de instância, consulte Recuperar os dados do usuário da instância da sua instância. Para obter informações sobre os dados do usuário e a AWS CLI, consulte Dados do usuário e AWS CLI.

Exemplo: especifique os dados do usuário da instância no lançamento

Crie um arquivo de texto com dados do usuário da instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>`, como mostrado no exemplo a seguir:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Para especificar dados do usuário da instância ao executar a instância, use o comando New-EC2Instance. Esse comando não executa a codificação base64 dos dados do usuário para você. Use os comandos a seguir para codificar os dados do usuário em um arquivo de texto denominado `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Use o parâmetro `-UserData` para passar os dados do usuário para o comando New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Exemplo: atualizar dados do usuário da instância para uma instância interrompida

É possível modificar os dados do usuário de uma instância interrompida usando o comando Edit-EC2InstanceAttribute.

Crie um arquivo de texto com o novo script. Use os comandos a seguir para codificar os dados do usuário no arquivo de texto denominado `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Use os parâmetros `-UserData` e `-Value` para especificar os dados do usuário.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Exemplo: visualizar dados do usuário da instância

Para recuperar os dados do usuário para uma instância, use o comando Get-EC2InstanceAttribute.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

A seguir está um exemplo de saída. Observe que os dados do usuário são codificados.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Use os comandos a seguir para armazenar os dados de usuário codificados em uma variável e decodifique-os.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

A seguir está um exemplo de saída.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Exemplo: renomear a instância para corresponder ao valor da tag

É possível usar o comando Get-EC2Tag para ler o valor da tag. Renomeie a instância na primeira inicialização para corresponder ao valor da tag e reinicialize. Para executar esse comando com êxito, é necessário ter uma função com permissões `ec2:DescribeTags` vinculadas à instância, pois as informações de tag são recuperadas pela chamada de API. Para obter mais informações sobre as permissões de configuração ao usar perfis do IAM, consulte Anexar uma função do IAM a uma instância.

```
<powershell>
 $instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id -
UseBasicParsing).content
 $nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Também é possível renomear a instância usando tags em metadados de instância, se sua instância estiver configurada para acessar tags a partir dos metadados da instância. Para ter mais informações, consulte Trabalho com tags de instância em metadados de instância.

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
```

```
    {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Recuperar dados dinâmicos da sua instância

Para recuperar dados dinâmicos de uma instância em execução, use um dos seguintes URIs. Para recuperar dados do usuário usando o endereço IPv6, você deve habilitá-lo, e a instância deve ser uma instância criada no AWS Nitro System em uma sub-rede compatível com IPv6.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Este exemplo recupera as categorias de identidade de instância de alto nível.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
```

```
dsa2048
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Para obter mais informações sobre dados dinâmicos e os exemplos de como recuperá-los, consulte Documentos de identidade da instância.

Categorias de metadados da instância

Os metadados da instância são divididos em categorias. Para recuperar metadados de instância, especifique a categoria na solicitação. Os metadados serão retornados na resposta.

Quando novas categorias forem lançadas, uma nova compilação de metadados de instância será criada com um novo número de versão. Na tabela a seguir, a coluna Version when category was released (Versão quando a categoria foi lançada) especifica a versão da compilação quando uma categoria de metadados de instância foi lançada. Para evitar ter que atualizar seu código sempre que o Amazon EC2 lançar uma nova compilação de metadados de instância, use `latest` em vez do número da versão em suas solicitações de metadados. Para ter mais informações, consulte Obter as versões disponíveis dos metadados da instância.

Quando o Amazon EC2 libera uma nova categoria de metadados de instância, os metadados de instância da nova categoria podem não estar disponíveis para instâncias existentes. Com instâncias criadas no sistema Nitro, é possível recuperar metadados de instância somente para as categorias que estavam disponíveis ao iniciar. Para instâncias com o hipervisor Xen, é possível interromper e iniciar a instância para atualizar as categorias que estão disponíveis para a instância.

A tabela a seguir lista as categorias de metadados da instância. Alguns dos nomes de categoria incluem espaços reservados para dados exclusivos da instância. Por exemplo, *mac* representa o endereço MAC para a interface de rede. É necessário substituir os espaços reservados pelos valores reais ao recuperar os metadados da instância.

Categoria	Descrição	Versão quando a categoria foi lançada
`ami-id`	O ID da AMI usada para executar a instância.	1,0
`ami-launch-index`	Se você executar várias instâncias usando a mesma chamada `RunInstances` , esse valor indicará a ordem de execução de cada instância. O valor da primeira instância executada é 0. Se você executar instâncias usando uma frota do Auto Scaling ou do EC2, esse valor será sempre 0.	1,0
`ami-manifest-path`	O caminho para o arquivo de manifesto da AMI no Amazon S3. Se você usou uma AMI baseada no Amazon EBS para executar a instância, o resultado retornado será `unknown`.	1,0
`ancestor-ami-ids`	Os IDs das AMIs de todas as instâncias que foram reagrupadas para criar essa AMI. Este valor existirá somente se o arquivo de	10/10/2007

Categoria	Descrição	Versão quando a categoria foi lançada
	manifesto de AMIs continham uma chave `ancestor-amis` .	
`autoscaling/target-lifecycle-state`	Valor mostrando o estado de destino do ciclo de vida do Auto Scaling para o qual uma instância do Auto Scaling está fazendo a transição. Presente quando a instância faz a transição para um dos estados de destino do ciclo de vida após 10 de março de 2022. Valores possíveis: `Detached | InService | Standby | Terminated | Warmed:Hibernated | Warmed:Running | Warmed:Stopped | Warmed:Terminated` . Consulte Retrieve the target lifecycle state through instance metadata (Recuperar o estado de destino do ciclo de vida por meio de metadados da instância) no Guia do usuário do Amazon EC2 Auto Scaling.	15/7/2021
`block-device-mapping/ami`	O dispositivo virtual que contém o sistema de arquivos de inicialização/raiz.	15/12/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`block-device-mapping/ebs` N	Os dispositivos virtuais associados a quaisquer volumes do Amazon EBS. Os volumes do Amazon EBS estarão disponíveis somente em metadados se estiverem presentes no momento da execução ou quando a instância foi iniciada pela última vez. O N indica o índice do volume do Amazon EBS (como `ebs1` ou `ebs2`).	15/12/2007
`block-device-mapping/ephemeral` N	Os dispositivos virtuais para qualquer volume de armazenamento de instâncias não NVMe. O N indica o índice de cada volume. O número dos volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos pode não corresponder ao número real de volumes de armazenamento de instâncias da instância. O tipo de instância determina o número de volumes de armazenamento de instâncias que estão disponíveis para uma instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número disponível para uma instância, os volumes de armazenamento de instâncias adicionais serão ignorados.	15/12/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`block-device-mapping/root`	Os dispositivos virtuais ou as partições associadas aos dispositivos raiz, ou as partições no dispositivo virtual, onde o sistema de arquivos raiz (/ ou C:) está associado à instância específica.	15/12/2007
`block-device-mapping/swap`	Os dispositivos virtuais associados a `swap`. Nem sempre presente.	15/12/2007
`elastic-gpus/associations/` *`elastic-gpu-id`*	Se houver um Elastic GPU anexado à instância, ele contém uma string JSON com informações sobre o Elastic GPU, incluindo suas informações de ID e conexão.	30/11/2016
`elastic-inference/associations/` *`eia-id`*	Se houver um acelerador do Elastic Inference anexado à instância, ele conterá uma string JSON com informações sobre o acelerador do Elastic Inference, incluindo o ID e o tipo.	29/11/2018
`events/maintenance/history`	Se houver eventos de manutenção da instância concluídos ou cancelados, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados.	17/08/2018

Categoria	Descrição	Versão quando a categoria foi lançada
`events/maintenance/scheduled`	Se houver eventos de manutenção da instância ativos, contém uma string JSON com informações sobre os eventos. Para ter mais informações, consulte Visualizar eventos agendados.	17/08/2018
`events/recommendations/rebalance`	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalanceamento da instância do EC2 é emitida para a instância. Veja a seguir um exemplo dos metadados para esta categoria: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Esta categoria só está disponível após a emissão da notificação. Para ter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.	27/10/2020

Categoria	Descrição	Versão quando a categoria foi lançada
`hostname`	Se a instância do EC2 estiver usando a nomenclatura baseada em IP (IPBN), esse é o hostname DNS de IPv4 privado da instância. Se a instância do EC2 estiver usando nomenclatura baseada em recursos (RBN), esse é o RBN. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0). Para obter mais informações sobre IPBN e RBN, consulte Tipos de nome de host de instância do Amazon EC2.	1,0
`iam/info`	Se houver uma função do IAM associada à instância, conterá informações sobre a última vez que o perfil de instância foi atualizado, incluindo a data LastUpdated, InstanceProfileArn e InstanceProfileId. Caso contrário, não estará presente.	12/01/2012

Categoria	Descrição	Versão quando a categoria foi lançada
`iam/security-credentials/role-name`	Se houver uma função do IAM associada à instância, *`role-name`* será o nome da função, e *`role-name`* conterá as credenciais de segurança temporárias associadas à função (para obter mais informações, consulte Recuperar credenciais de segurança dos metadados da instância). Caso contrário, não estará presente.	12/01/2012
`identity-credentials/ec2/info`	Informações sobre as credenciais no `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018
`identity-credentials/ec2/security-credentials/ec2-instance`	As credenciais do perfil de identidade da instância que permitem que o software na instância se identifique para a AWS para oferecer suporte a recursos como o EC2 Instance Connect e à Configuração padrão de gerenciamento de host do AWS Systems Manager. Essas credenciais não têm políticas anexadas, portanto, não têm permissões adicionais de APIs da AWS além de identificar a instância para o recurso da AWS. Para ter mais informações, consulte Perfis de identidade da instância.	23/05/2018

Categoria	Descrição	Versão quando a categoria foi lançada
`instance-action`	Notifica a instância que ela deve ser reinicializada em preparação para o empacotamento. Valores válidos: `none` | `shutdown` | `bundle-pending` .	01/09/2008
`instance-id`	O ID dessa instância.	1,0
`instance-life-cycle`	A opção de compra desta instância . Para ter mais informações, consulte Opções de compra de instância.	01/10/2019
`instance-type`	O tipo da instância. Para ter mais informações, consulte Tipos de instância do Amazon EC2.	29/08/2007
`ipv6`	O endereço IPv6 da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo cujo número de dispositivo é 0) na interface de rede e o primeiro endereço iPv6 atribuído. Se nenhum endereço IPv6 existir na interface de rede[0], esse item não será definido e gerará uma resposta HTTP 404.	3/1/2021
`kernel-id`	O ID do kernel executado com essa instância, se aplicável.	01/02/2008

Categoria	Descrição	Versão quando a categoria foi lançada
`local-hostname`	Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0). Se a instância do EC2 estiver usando a nomenclatura baseada em IP (IPBN), esse é o hostname DNS de IPv4 privado da instância. Se a instância do EC2 estiver usando nomenclatura baseada em recursos (RBN), esse é o RBN. Para obter mais informações sobre IPBN, RBN e nomenclatura de instâncias do EC2, consulte Tipos de nome de host de instância do Amazon EC2.	19/01/2007
`local-ipv4`	O endereço IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0). Se esta for uma instância somente IPv6, esse item não será definido e gerará uma resposta HTTP 404.	1,0

Categoria	Descrição	Versão quando a categoria foi lançada
`mac`	O endereço Media Access Control (MAC) da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	01/01/2011
`metrics/vhostmd`	Não está mais disponível.	01/05/2011
`network/interfaces/macs/mac/device-number`	O número de dispositivo exclusivo associado a essa interface. O número do dispositivo correspon de ao nome do dispositivo; por exemplo, um `device-number` de 2 é para o dispositivo eth2. Essa categoria corresponde aos campos `DeviceIndex` e `device-index` que são usados pelos comandos da API do Amazon EC2 e do EC2 para a AWS CLI.	01/01/2011
`network/interfaces/macs/mac/interface-id`	O ID da interface de rede.	01/01/2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Os endereços IPv4 privados que estão associados a cada endereço IP público e estão atribuídos a essa interface.	01/01/2011
`network/interfaces/macs/mac/ipv6s`	Os endereços IPv6 atribuídos à interface.	30/06/2016

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/ipv6-prefix`	O prefixo IPv6 atribuído à interface de rede.	
`network/interfaces/macs/mac/local-hostname`	O nome de host DNS IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0). Se esta for uma instância somente IPv6, esse será o nome baseado em recursos. Para obter mais informações sobre IPBN e RBN, consulte Tipos de nome de host de instância do Amazon EC2.	19/01/2007
`network/interfaces/macs/mac/local-ipv4s`	Os endereços IPv4 privados associados à interface. Se esta for uma interface de rede somente IPv6, esse item não será definido e gerará uma resposta HTTP 404.	01/01/2011
`network/interfaces/macs/mac/mac`	O endereço MAC da instância.	01/01/2011
`network/interfaces/macs/`*`mac`*`/network-card`	O índice da placa de rede. Alguns tipos de instância suportam várias placas de rede.	01-11-2020

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/owner-id`	O ID do proprietário da interface de rede. Em ambientes de várias interfaces, um terceiro pode anexar uma interface, como o Elastic Load Balancing . O tráfego em uma interface é sempre cobrado do proprietário da interface.	01/01/2011
`network/interfaces/macs/mac/public-hostname`	O DNS público da interface (IPv4). Essa categoria só será retornada se o atributo `enableDnsHostnames` for definido como `true`. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC. Se a instância tiver apenas um endereço IPv6 público e nenhum endereço IPv4 público, esse item não será definido e gerará uma resposta HTTP 404.	01/01/2011
`network/interfaces/macs/mac/public-ipv4s`	Os endereços IP públicos ou os endereços IP elásticos associados à interface. Pode haver vários endereços IPv4 em uma instância.	01/01/2011
`network/interfaces/macs/mac/security-groups`	Grupos de segurança aos quais a interface de rede pertence.	01/01/2011
`network/interfaces/macs/mac/security-group-ids`	Os IDs dos grupos de segurança aos quais a interface de rede pertence.	01/01/2011

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/subnet-id`	O ID da sub-rede na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	O bloco CIDR IPv4 da sub-rede na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	O bloco CIDR IPv6 da sub-rede na qual a interface reside.	30/06/2016
`network/interfaces/macs/mac/vpc-id`	O ID da VPC na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	O bloco CIDR IPv4 principal da VPC.	01/01/2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Os blocos CIDR IPv4 da VPC.	30/06/2016
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	O bloco CIDR IPv6 da VPC na qual a interface reside.	30/06/2016
`placement/availability-zone`	A zona de disponibilidade na qual a instância foi executada.	01/02/2008

Categoria	Descrição	Versão quando a categoria foi lançada
`placement/availability-zone-id`	O ID estático da zona de disponibilidade em que a instância é executada. O ID da zona de disponibilidade é consistente entre as contas. No entanto, pode ser diferente da zona de disponibilidade, que pode variar de acordo com a conta.	01/10/2019
`placement/group-name`	O nome do grupo de posicionamento no qual a instância é executada.	24/08/2020
`placement/host-id`	O ID do host no qual a instância é executada. Aplicável apenas a Hosts dedicados.	24/08/2020
`placement/partition-number`	O número da partição na qual a instância é executada.	24/08/2020
`placement/region`	A região da AWS na qual a instância é executada.	24/08/2020
`product-codes`	AWS Marketplace Os códigos de produtos associados com a instância, se houver.	01/03/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`public-hostname`	O DNS público da instância (IPv4). Essa categoria só será retornada se o atributo `enableDnsHostnames` for definido como `true`. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC. Se a instância tiver apenas um endereço IPv6 público e nenhum endereço IPv4 público, esse item não será definido e gerará uma resposta HTTP 404.	19/01/2007
`public-ipv4`	O endereço IPv4 público. Se um endereço IP elástico estiver associado à instância, o valor retornado será o endereço IP elástico.	19/01/2007
`public-keys/0/openssh-key`	Chave pública. Disponível somente se fornecido no momento da execução da instância.	1,0
`ramdisk-id`	O ID do disco de RAM no momento da execução, se aplicável.	10/10/2007
`reservation-id`	O ID da reserva.	1,0

Categoria	Descrição	Versão quando a categoria foi lançada
`security-groups`	Os nomes dos grupos de segurança aplicados à instância. Após a execução, você só pode alterar os grupos de segurança das instâncias. Essas alterações estão refletidas aqui e em network/interfaces/macs/*mac*/security-groups.	1,0
`services/domain`	O domínio dos recursos da AWS para a região.	25/02/2014
`services/partition`	A partição na qual o recurso está. Para regiões padrão da AWS a partição é `aws`. Se você tem recursos em outras partições, a partição é `aws-`*partition name*. Por exemplo, a partição de recursos na região China (Pequim) é `aws-cn`.	20/10/2015
`spot/instance-action`	A ação (hibernar, interromper ou encerrar) e o tempo aproximado, em UTC, em que a ação ocorrerá. Esse item estará presente somente se a instância spot tiver sido marcada para hibernar, interromper ou encerrar. Para ter mais informações, consulte instance-action.	15/11/2016

Categoria	Descrição	Versão quando a categoria foi lançada
`spot/termination-time`	O tempo aproximado, em UTC, no qual o sistema operacional para sua instância spot receberá o sinal de desligamento. Esse item está presente e contém um valor de tempo (por exemplo, 2015-01-05T18:02:00Z) somente se a instância spot tiver sido marcada para término pelo Amazon EC2. O item hora de encerramento não está definido como uma hora se você mesmo encerrou a instância spot. Para ter mais informações, consulte termination-time.	05/11/2014
`tags/instance`	As tags de instância associadas à instância. Somente disponível se você permitir explicitamente acesso a etiquetas em metadados de instância. Para ter mais informações, consulte Permitir acesso a tags em metadados de instância.	23/3/2021

Categorias de dados dinâmicos

A tabela a seguir lista as categorias de dados dinâmicos.

Categoria	Descrição	Versão quando a categoria foi lançada
`fws/instance-monitoring`	O valor que mostra se o cliente habilitou o monitoramento de um minuto detalhado no CloudWatch. Valores válidos: `enabled | disabled`	04/04/2009
`instance-identity/document`	O JSON que contém os atributos da instância, como o ID da instância, o endereço IP privado, etc. Consulte Documentos de identidade da instância.	04/04/2009
`instance-identity/pkcs7`	Usado para verificar a autenticidade e o conteúdo do documentos em relação à assinatura. Consulte Documentos de identidade da instância.	04/04/2009
`instance-identity/signature`	Os dados que podem ser usados por outras partes para verificar sua origem e autenticidade. Consulte Documentos de identidade da instância.	04/04/2009

Exemplo do Linux: valor do índice de execução da AMI

Este exemplo demonstra como é possível usar dados do usuário e metadados de instância para configurar as instâncias do Linux.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do IMDS: `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias do EC2 pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `[fd00:ec2::254]`. O endereço IPv6 do IMDS é compatível com comandos IMDSv2. O endereço IPv6 só pode ser acessado em instâncias baseadas no AWS Nitro System e em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas).

Alice deseja executar quatro instâncias de sua AMI de banco de dados favorita, em que a primeira atua como a instância original e as três restantes como réplicas. Ao executá-las, ela deseja adicionar dados do usuário sobre a estratégia de replicação para cada réplica. Ela sabe que esses dados estarão disponíveis para todas as quatro instâncias, então, ela precisa estruturar os dados do usuário de forma que permita a cada instância reconhecer quais partes são aplicáveis a ela. Ela pode fazer isso usando o valor de metadados da instância `ami-launch-index`, que será exclusivo para cada instância. Se você iniciar mais de uma instância ao mesmo tempo, o `ami-launch-index`indicará a ordem em que as instâncias foram executadas. O valor da primeira instância iniciada é `0`.

Veja a seguir os dados de usuário construídos por Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Os dados `replicate-every=1min` definem a configuração da primeira réplica, `replicate-every=5min` definem a configuração da segunda réplica e assim por diante. Alice decide fornecer esses dados como uma string ASCII com um símbolo de pipe (`|`) que limita os dados para as instâncias separadas.

Alice executa quatro instâncias usando o comando run-instances e especificando os dados do usuário.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Depois de executadas, todas as instâncias têm uma cópia dos dados do usuário e os metadados comuns mostrados aqui:

- ID da AMI: ami-0abcdef1234567890
- ID da reserva: r-1234567890abcabc0
- Chaves públicas: nenhuma
- Nome do security group: padrão
- Tipo de instância: t2.micro

No entanto, cada instância tem metadados exclusivos, conforme mostrado nas tabelas a seguir.

Metadados	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadados	Valor
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadados	Valor
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225

Metadados	Valor
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Metadados	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice pode usar o valor `ami-launch-index` para determinar qual parte dos dados do usuário é aplicável a uma instância específica.

1. Ela se conecta a uma das instâncias e recupera o `ami-launch-index` dessa instância para garantir que ela seja uma das réplicas:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

   Para as etapas a seguir, as solicitações do IMDSv2 usam o token armazenado do comando anterior do IMDSv2, supondo-se que o token não tenha expirado.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

2. Ela salva o `ami-launch-index` como uma variável.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. Ela salva os dados do usuário como uma variável.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Finalmente, Alice usa o comando cut para extrair a parte dos dados do usuário aplicável à instância.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Documentos de identidade da instância

Cada instância iniciada tem um documento de identidade da instância que fornece informações sobre a própria instância. É possível usar o documento de identidade da instância para validar os atributos da instância.

O documento de identidade da instância é gerado quando a instância é interrompida e iniciada, reiniciada ou lançada. O documento de identidade da instância é exposto (no formato JSON de texto simples) por meio do Serviço de metadados de instância (IMDS). O endereço IPv4 do `169.254.169.254` é um endereço local de link e é válido apenas a partir da instância. Para obter mais informações, consulte Endereço de link local na Wikipedia. O endereço IPv6 do `[fd00:ec2::254]` é um endereço local único e é válido apenas a partir da instância. Para obter mais informações, consulte Endereço local único na Wikipédia.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do IMDS: `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias do EC2 pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `[fd00:ec2::254]`. O endereço IPv6 do IMDS é compatível com comandos IMDSv2. O endereço IPv6 só pode ser acessado em instâncias baseadas no AWS Nitro System e em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas).

É possível recuperar o documento de identidade da instância de uma instância em execução a qualquer momento. O documento de identidade da instância inclui as seguintes informações:

Dados	Descrição
`accountId`	O ID da conta da AWS que iniciou a instância.
`architecture`	A arquitetura da AMI usada para iniciar a instância (i386 | x86_64 | arm64).
`availabilityZone`	A zona de disponibilidade na qual a instância está em execução.
`billingProducts`	Os produtos de faturamento da instância.

Dados	Descrição
`devpayProductCodes`	Suspenso.
`imageId`	A ID do AMI usado para executar a instância.
`instanceId`	O ID da instância.
`instanceType`	O tipo de instância da instância.
`kernelId`	O ID do kernel associado à instância, se aplicável.
`marketplaceProductCodes`	O código do produto AWS Marketplace da AMI usada para iniciar a instância.
`pendingTime`	A data e a hora em que a instância foi iniciada.
`privateIp`	O endereço IPv4 privado da instância.
`ramdiskId`	O ID do disco de RAM associado a essa instância, se aplicável.
`region`	A região em que a instância está em execução.
`version`	A versão do formato do documento de identidade da instância.

Recuperar o documento de identidade da instância de texto sem formatação

Como recuperar o documento de identidade da instância de texto simples

Conecte-se à instância e execute o comando a seguir.

Linux

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token}
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

O seguinte é um exemplo de saída.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verifique o documento de identidade da instância

Se você pretende usar o conteúdo do documento de identidade da instância para um propósito importante, deve verificar seu conteúdo e autenticidade antes de usá-lo.

O documento de identidade da instância de texto simples é acompanhado por três assinaturas hash e criptografadas. É possível usar essas assinaturas para verificar a origem e a autenticidade do documento de identidade da instância e as informações incluídas nele. São fornecidas as seguintes assinaturas:

- Assinatura codificada em base64 – trata-se de um hash SHA256 codificado em base64 do documento de identidade da instância que é criptografado usando um par de chaves RSA.
- Assinatura PKCS7 – trata-se de um hash SHA1 do documento de identidade da instância que é criptografado usando um par de chaves DSA.
- Assinatura RSA-2048 – trata-se de um hash SHA256 do documento de identidade da instância que é criptografado usando um par de chaves RSA-2048.

Cada assinatura está disponível em um endpoint diferente nos metadados da instância. É possível usar qualquer uma dessas assinaturas dependendo dos requisitos de hash e criptografia. Para verificar as assinaturas, é necessário usar o certificado público da AWS correspondente.

Os tópicos a seguir fornecem etapas detalhadas para validar o documento de identidade da instância usando cada assinatura.

- Usar a assinatura PKCS7 para verificar o documento de identidade da instância
- Usar a assinatura codificada em base64 para verificar o documento de identidade da instância
- Usar a assinatura RSA-2048 para verificar o documento de identidade da instância

Usar a assinatura PKCS7 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público DSA da AWS.

Instâncias do Linux

Para verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público AWS DSA

1. Conecte-se à instância.
2. Recupere a assinatura PKCS7 dos metadados da instância e adicione-a a um arquivo chamado `pkcs7` junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Encontre o certificado público DSA da sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo chamado `certificate`.
4. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Se a assinatura for válida, a mensagem `Verification successful` será exibida.

O comando também grava o conteúdo do documento de identidade da instância em um novo arquivo denominado `document`. É possível comparar o conteúdo do documento de identidade da instância dos metadados da instância com o conteúdo desse arquivo usando os comandos a seguir.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se não for possível verificar a assinatura, entre em contato com o AWS Support.

Instâncias do Windows

Pré-requisitos

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Para verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público AWS DSA

1. Conecte-se à instância.
2. Recupere a assinatura PKCS7 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/pkcs7).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público DSA da sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo chamado `certificate.pem`.

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifique a assinatura.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se não for possível validar o documento de identidade da instância, entre em contato com o AWS Support.

Usar a assinatura codificada em base64 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura codificada em base64 e o certificado público RSA da AWS.

Instâncias do Linux

Para validar o documento de identidade da instância usando a assinatura codificada em base64 e do certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em binário e adicione-o a um arquivo chamado `signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância e adicione-o a um arquivo chamado `document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Encontre o certificado público RSA para a sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo denominado `certificate`.

5. Extraia a chave pública do certificado público RSS da AWS e salve-a em um arquivo denominado `key`.

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Use o comando OpenSSL dgst para verificar o documento de identidade da instância.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

Se a assinatura for válida, a mensagem `Verification successful` será exibida.

O comando também grava o conteúdo do documento de identidade da instância em um novo arquivo denominado `document`. É possível comparar o conteúdo do documento de identidade da instância dos metadados da instância com o conteúdo desse arquivo usando os comandos a seguir.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se não for possível verificar a assinatura, entre em contato com o AWS Support.

Instâncias do Windows

Para validar o documento de identidade da instância usando a assinatura codificada em base64 e do certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a à variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público RSA para a sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo denominado `certificate.pem`.

5. Verifique o documento de identidade da instância.

   ```
   PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
   Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
   ```

   Se a assinatura for válida, o comando retornará `True`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

Usar a assinatura RSA-2048 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS.

Instâncias do Linux

Para verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS

1. Conecte-se à instância.
2. Recupere a assinatura RSA-2048 dos metadados da instância e adicione-a a um novo arquivo chamado `rsa2048` junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/rsa2048 >> rsa2048 \
   && echo "" >> rsa2048 \
   && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
    >> rsa2048 \
   && echo "" >> rsa2048 \
   && echo "-----END PKCS7-----" >> rsa2048
   ```

3. Encontre o certificado público RSA-2048 para a sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo denominado `certificate`.
4. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Se a assinatura for válida, a mensagem `Verification successful` será exibida. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

Instâncias do Windows

Pré-requisitos

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Para verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS

1. Conecte-se à instância.
2. Recupere a assinatura RSA-2048 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público RSA-2048 para a sua região em Certificados públicos da AWS e adicione o conteúdo a um novo arquivo denominado `certificate.pem`.

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifique a assinatura.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

   Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se não for possível validar o documento de identidade da instância, entre em contato com o AWS Support.

Certificados públicos da AWS

Os seguintes certificados públicos da AWS podem ser usados para verificar o conteúdo do documento de identidade da instância de uma instância, conforme descrito nestes tópicos:

- Verificar usando a assinatura PKCS7
- Verificar usando a assinatura codificada em base64
- Verificar usando a assinatura RSA-2048

Certifique-se de usar o certificado correto para a sua região e para o procedimento de verificação que está sendo usado. Se você estiver verificando a assinatura PKCS7, use o certificado DSA. Se você estiver verificando a assinatura codificada em base6, use o certificado RSA. Se você estiver verificando a assinatura RSA-2048, use o certificado RSA-2048.

Expanda cada região abaixo para visualizar os certificados específicos da região.

Leste dos EUA (Ohio): us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
```

```
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

Leste dos EUA (Virgínia): us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

Oeste dos EUA (Norte da Califórnia): us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

Oeste dos EUA (Oregon): us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
```

```
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

África (Cidade do Cabo): af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Ásia-Pacífico (Hong Kong): ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Ásia-Pacífico (Hyderabad): ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
```

```
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Jacarta): ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
```

```
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
```

```
-----END CERTIFICATE-----
```

Ásia-Pacífico (Melbourne): ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
```

```
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Mumbai): ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asia Pacific (Osaka): ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Ásia-Pacífico (Seul): ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
```

```
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Ásia-Pacífico (Singapura): ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
```

```
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Sydney): ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Tóquio): ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
```

```
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canadá (Central): ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Oeste do Canadá (Calgary): ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
```

```
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Europa (Frankfurt): eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irlanda): eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (Londres): eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
```

```
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Milão): eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Paris): eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europa (Espanha): eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
```

```
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Estocolmo): eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
```

```
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europa (Zurique): eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv): il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
```

```
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Oriente Médio (Bahrein): me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
```

```
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Oriente Médio (EAU): me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8mo0hqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

América do Sul (São Paulo): sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

China (Pequim): cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
```

```
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

China (Ningxia): cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

AWS GovCloud (Leste dos EUA): us-gov-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (Oeste dos EUA): us-gov-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
```

```
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Perfis de identidade da instância

Cada instância iniciada tem um perfil de identidade da instância que representa sua identidade. Um perfil de identidade de instância é um tipo de perfil do IAM. Serviços da AWS e recursos integrados para usar o perfil de identidade da instância podem usá-lo para identificar a instância com o serviço.

As credenciais do perfil de identidade da instância podem ser acessadas no Serviço de metadados da instância (IMDS) em `/identity-credentials/ec2/security-credentials/ec2-instance`. As credenciais consistem em um par temporário de chave de acesso da AWS e um token de sessão. Eles são usados para assinar solicitações AWS Sigv4 para os serviços da AWS que usam o perfil de identidade da instância. As credenciais estão presentes nos metadados da instância, independentemente de um serviço ou recurso que faça uso dos perfils de identidade da instância estar habilitado na instância.

Os perfis de identidade da instância são criados automaticamente quando uma instância é iniciada, não possuem nenhum documento de política de confiança de perfil e não estão sujeitos a nenhuma política de identidade ou de recursos.

Serviços com suporte

Os serviços da AWS a seguir usam o perfil de identidade da instância:

- Amazon EC2: o EC2 Instance Connect usa o perfil de identidade da instância para atualizar as chaves de host de uma instância do Linux.
- Amazon GuardDuty: o monitoramento do tempo de execução usa o perfil de identidade da instância para permitir que o agente de runtime envie telemetria de segurança para o endpoint da VPC do GuardDuty.
- AWS Security Token Service (AWS STS): as credenciais do perfil de identidade da instância podem ser usadas com a ação AWS STS `GetCallerIdentity`.

- AWS Systems Manager: ao usar a Configuração padrão de gerenciamento de host, o AWS Systems Manager usa a identidade fornecida pelo perfil de identidade da instância para registrar instâncias do EC2. Depois de identificar sua instância, o Systems Manager pode passar seu perfil do IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole` para sua instância.

Os perfis de identidade da instância não podem ser usados com outros serviços ou recursos da AWS, pois eles não têm uma integração com os perfis de identidade da instância.

ARN de perfil de identidade da instância

O ARN de perfil de identidade da instância assume o seguinte formato:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Por exemplo:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Para obter mais informações sobre ARNs, consulte Nome do recurso da Amazon (ARN) no Guia do usuário do IAM.

Conexão com a instância do EC2

Esta seção do Guia do usuário do Amazon EC2 fornece informações para ajudar você a se conectar à sua instância do Amazon EC2 após iniciá-la. Além disso, a seção fornece informações para ajudar você a conectar a instância a outro recurso da AWS.

Tópicos

- Conecte-se à sua instância do Linux
- Conectar-se à sua instância do Windows do
- Conectar-se usando o Gerenciador de sessões
- Conectar-se a suas instâncias usando o EC2 Instance Connect Endpoint
- Conectar sua instância do EC2 a um recurso da AWS

Conecte-se à sua instância do Linux

Há muitas formas de se conectar à instância do Linux. Algumas variam em função do sistema operacional da máquina local a partir da qual você se conecta. Outros, como EC2 Instance Connect ou AWS Systems Manager Session Manager, não variam. Nesta seção, você aprenderá a se conectar a uma instância do Linux e a transferir arquivos entre seu computador local e a instância.

Antes de você se conectar à sua instância do Linux, preencha os pré-requisitos a seguir.

- Obter informações sobre a instância
- Localizar a chave privada e definir permissões
- (Opcional) Obter a impressão digital da instância

Em seguida, escolha uma das opções a seguir para se conectar à sua instância do Linux.

Opções para se conectar com base no sistema operacional local

- Conectar de uma máquina local Linux ou macOS usando SSH
- Conectar de uma máquina local Windows

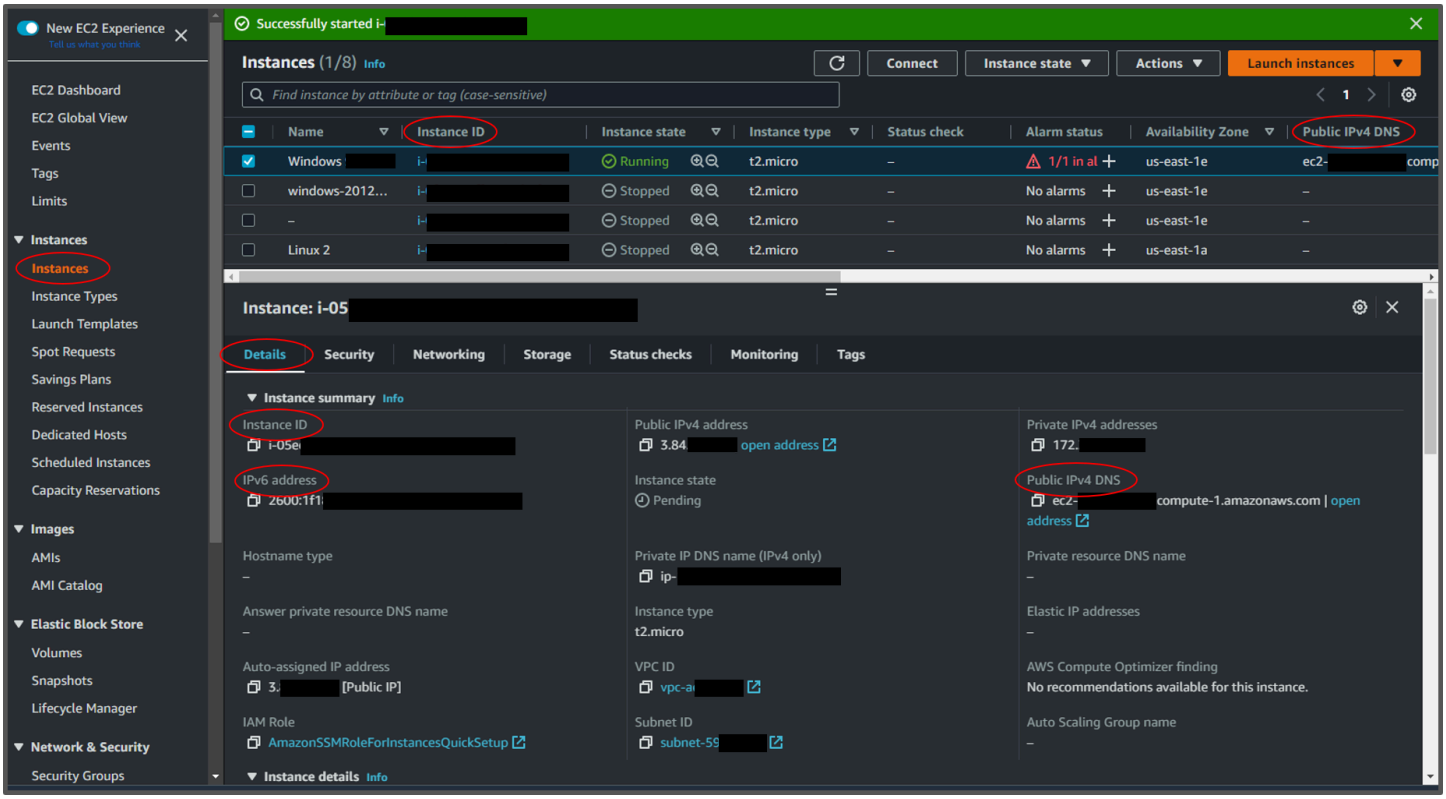
Opções para se conectar de qualquer sistema operacional local

- Conectar-se usando o Gerenciador de sessões
- Conectar-se à instância do Linux com o EC2 Instance Connect.

> **Note**
>
> Para obter dicas de solução de problemas de conexão, consulte Solução de problemas de conexão com a instância do Linux.
> Para solucionar problemas de inicialização, configuração de rede e outros problemas de instâncias criadas no AWS Nitro System, você pode usar o Console de Série do EC2 para as instâncias do Amazon EC2.

Obter informações sobre a instância

Para preparar para se conectar a uma instância, obtenha as seguintes informações no console do Amazon EC2 ou usando a AWS CLI.



- Obtenha o nome do DNS público da instância.

  É possível obter o DNS público da instância usando o console do Amazon EC2. Verifique a coluna DNS IPv4 público do painel Instâncias. Se essa coluna estiver oculta, escolha o ícone de configurações (⚙) no canto superior direito da tela e selecione DNS público (IPv4). Você também pode encontrar o DNS público na seção de informações da instância do painel Instâncias. Quando você seleciona a instância no painel Instâncias do console do Amazon EC2, as informações sobre essa instância aparecem na metade inferior da página. Na guia Detalhes, procure DNS IPv4 público.

  Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell).

  Se nenhum DNS IPv4 público for exibido, verifique se o estado da instância é em execução e se você não iniciou a instância em uma sub-rede privada. Se você iniciou a instância usando o

assistente de inicialização de instância, talvez tenha editado o campo Atribuição automática de IP público em Configurações de rede e alterado o valor para Desabilitar. Se você desabilitar a opção Atribuição automática de IP públic, a instância não receberá um endereço IP público quando for iniciada.

- (Somente IPv6) Obtenha o endereço IPv6 da instância.

  Se você atribuiu um endereço IPv6 à instância, terá a opção de se conectar a ela usando o endereço IPv6 em vez de um endereço IPv4 ou o nome de host DNS público. Seu computador local deve ter um endereço IPv6 e configurado para usar IPv6. É possível obter o endereço IPv6 da instância no console do Amazon EC2. Verifique a coluna IPs IPv6 do painel Instâncias. Ou você pode encontrar o endereço IPv6 na seção de informações da instância. Quando você seleciona a instância no painel Instâncias do console do Amazon EC2, as informações sobre essa instância aparecem na metade inferior da página. Na guia Detalhes, procure Endereço IPv6.

  Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell). Para obter mais informações sobre IPv6, consulte Endereços IPv6.

- Obtenha o nome de usuário para a instância.

  É possível se conectar à instância usando o nome de usuário da sua conta de usuário ou o nome de usuário padrão da AMI que você usou para iniciar a instância.

  - Obtenha o nome de usuário da sua conta de usuário.

    Para obter mais informações sobre como criar uma conta de usuário, consulte Gerenciamento de usuários do sistema na instância do Linux.

  - Obtenha o nome de usuário padrão da AMI usada para iniciar a instância:

A AMI usada para iniciar a instância	Nome de usuário padrão
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`

A AMI usada para iniciar a instância	Nome de usuário padrão
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

Localizar a chave privada e definir permissões

Você deve saber a localização do arquivo de chave privada para se conectar à instância. Para conexões SSH, você deve definir as permissões para que somente você possa ler o arquivo.

Para obter informações sobre como os pares de chaves funcionam ao usar o Amazon EC2, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

- Encontrar a chave privada

  Obtenha o caminho totalmente qualificado para o local em seu computador do arquivo `.pem` para o par de chaves que você especificou quando executou a instância. Para ter mais informações, consulte the section called “Identifique a chave pública que foi especificada na inicialização”.

  Se você não conseguir encontrar seu arquivo de chave privada, consulte

  Se você perder a chave privada de uma instância com EBS, poderá recobrar o acesso à sua instância. É necessário parar a instância, separar seu volume raiz e associá-lo a outra instância como um volume de dados, modificar o arquivo `authorized_keys` com uma nova chave pública, mover o volume de volta para a instância original e reiniciar a instância. Para obter mais informações sobre executar, conectar e parar instâncias, consulte Ciclo de vida da instância.

Este procedimento é compatível apenas com instâncias com volumes raiz do EBS. Se o dispositivo raiz for um volume de armazenamento de instâncias, você não poderá usar esse procedimento para recuperar o acesso à instância. É necessário ter a chave privada para se conectar à instância. Para determinar o tipo de dispositivo raiz da instância, abra o console do Amazon EC2, escolha Instâncias, selecione a instância, escolha a guia Armazenamento e, na seção Detalhes do dispositivo raiz, verifique o valor de Tipo de dispositivo raiz.

O valor é `EBS` ou `INSTANCE-STORE`.

Além das etapas a seguir, há outras formas de se conectar à instância do Linux em caso de perda da chave privada. Para obter mais informações, consulte Como posso me conectar à instância do Amazon EC2 se tiver perdido meu par de chaves SSH após o lançamento inicial?

Etapas para se conectar a uma instância com EBS com um par de chaves diferente

- Etapa 1: Criar um novo par de chaves
- Etapa 2: Obter informações sobre a instância original e seu volume raiz
- Etapa 3: Interromper a instância original
- Etapa 4: Executar uma instância temporária
- Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária
- Etapa 6: Adicionar a nova chave pública authorized_keys no volume original montado à instância temporária
- Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original
- Etapa 8: Conectar-se à instância original usando o novo par de chaves
- Etapa 9: Limpeza

Etapa 1: Criar um novo par de chaves

Crie um novo par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros. Se você quiser nomear seu novo par de chaves exatamente igual ao par de chaves privadas perdido, primeiro exclua o par de chaves existente. Para obter mais informações sobre como criar um par de chaves, consulte Criar um par de chaves usando o Amazon EC2 ou Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.

Etapa 2: Obter informações sobre a instância original e seu volume raiz

Anote as seguintes informações, porque elas serão necessárias para a conclusão deste procedimento.

Como obter informações sobre a instância original

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias no painel de navegação e selecione a instância à qual você deseja se conectar. (Nós a chamamos de instância original.)
3. Na guia Details (Detalhes) , anote o ID da instância e a ID da AMI.
4. Na guia Networking (Redes), anote a zona de disponibilidade.
5. Na guia Storage (Armazenamento), em Root device name (Nome do dispositivo raiz), anote o nome do dispositivo para o volume raiz (por exemplo, `/dev/xvda`). Em seguida, em Block devices (Dispositivos de bloco), encontre este nome do dispositivo e anote o ID do volume (por exemplo, vol-0a1234b5678c910de).

Etapa 3: Interromper a instância original

Escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Etapa 4: Executar uma instância temporária

New console

Para executar uma instância temporária

1. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
2. Na seção Name and tags (Nome e etiquetas), em Name (Nome), insira Temporary (Temporário).
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a mesma AMI usada para iniciar a instância original. Se essa AMI estiver indisponível, será possível criar uma AMI que pode usar a partir da instância interrompida. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
4. Na seção Instance type (Tipo de instância), mantenha o tipo de instância padrão.
5. Na seção Key pair (Par de chaves), em Key pair name (Nome do par de chaves), selecione o par de chaves existente para usar ou crie um novo.
6. Na seção Network settings (Configurações de rede), selecione Edit (Editar), e, em seguida, em Subnet (Sub-rede), selecione uma sub-rede na mesma zona de disponibilidade que a instância original.
7. No painel Summary (Resumo) painel, escolha Launch (Iniciar).

Old console

Escolha Launch Instance (Executar instância) e use o assistente de execução para executar uma instância temporária com as seguintes opções:

- Na página Escolha uma AMI, selecione a mesma AMI usada para executar a instância original. Se essa AMI estiver indisponível, será possível criar uma AMI que pode usar a partir da instância interrompida. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
- Na página Escolher um tipo de instância, deixe o tipo de instância padrão que o assistente seleciona para você.

- Na página Configure Instance Details (Configurar detalhes da instância) especifique a mesma zona de disponibilidade que a instância original. Se você estiver executando uma instância em uma VPC, selecione uma sub-rede nesta zona de disponibilidade.
- Na página Adicionar tags, adicione a tag `Name=Temporary` à instância para indicar que isso é uma instância temporária.
- Na página Revisar, escolha Iniciar. Escolha o par de chaves criado na Etapa 1 e selecione Iniciar instâncias.

Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária

1. No painel de navegação, selecione Volumes e selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior). Escolha Actions (Ações), Detach Volume (Desanexar volume) e Yes, Detach (Sim, desanexar). Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)
2. Com o volume ainda selecionado, escolha Actions (Ações) e, em seguida, Attach volume (Anexar volume). Selecione o ID de instância da instância temporária, anote o nome do dispositivo especificado em Device (Dispositivo) (por exemplo, `/dev/sdf`) e selecione Attach (Anexar).

   > **Note**
   >
   > Se você tiver executado a instância original a partir de uma AMI de AWS Marketplace e seu volume contiver códigos de AWS Marketplace, você deverá primeiro parar a instância temporária antes de associar o volume.

Etapa 6: Adicionar a nova chave pública **`authorized_keys`** no volume original montado à instância temporária

1. Conecte-se à instância temporária.
2. Na instância temporária, monte o volume que você associou à instância de forma que possa acessar seu sistema de arquivos. Por exemplo, se o nome do dispositivo for `/dev/sdf`, use os comandos a seguir para montar o volume como `/mnt/tempvol`.

> **Note**
>
> O nome de dispositivo pode aparecer de forma diferente em sua instância. Por exemplo, dispositivos montados como `/dev/sdf` podem ser exibidos como `/dev/xvdf` na instância. Algumas versões do Red Hat (ou suas variantes, como o CentOS) podem até mesmo incrementar a letra final com 4 caracteres, em que `/dev/sdf` torna-se `/dev/xvdk`.

a. Use o comando lsblk determinar se o volume é particionado.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

No exemplo acima, `/dev/xvda` e `/dev/xvdf` são volumes particionados, e `/dev/xvdg` não é. Se seu volume estiver particionado, você montará a partição (`/dev/xvdf1`) em vez do dispositivo raw (`/dev/xvdf`) nas próximas etapas.

b. Crie um diretório temporário para montar o volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Monte o volume (ou a partição) no ponto de montagem temporário usando o nome do volume ou do dispositivo identificado anteriormente. O comando necessário depende do sistema de arquivos do sistema operacional. Observe que o nome de dispositivo pode aparecer de forma diferente em sua instância. Consulte note na etapa 6 para obter mais informações.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se você receber um erro informando que o sistema de arquivos está corrompido, execute o seguinte comando para usar o utilitário fsck para verificar o sistema de arquivos e reparar quaisquer problemas:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Pela instância temporária, use o comando a seguir para atualizar `authorized_keys` no volume montado com a nova chave pública nova de `authorized_keys` para a instância temporária.

> **Important**
>
> Os exemplos a seguir usam o nome de usuário do Amazon Linux `ec2-user`. É possível precisar substituir um nome de usuário diferente, como `ubuntu` para instâncias Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se essa cópia tiver sido bem-sucedida, será possível passar para a próxima etapa.

(Opcional) Caso contrário, se você não tiver permissão para editar arquivos em `/mnt/tempvol`, será necessário atualizar o arquivo usando sudo e conferir as permissões no arquivo para verificar se é possível fazer login na instância original. Use o comando a seguir para verificar as permissões no arquivo:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Nesta saída de exemplo, *222* é o ID do usuário e *500* é o ID do grupo. Em seguida, use sudo para executar novamente o comando de cópia que falhou.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Execute o comando a seguir novamente para determinar se as permissões foram alteradas.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se o ID do usuário e do grupo tiverem sido alterados, use o comando a seguir para restaurá-los.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original

1. Na instância temporária, desmonte o volume que você associou para que possa reassociá-lo à instância original. Por exemplo, use o comando a seguir para desmontar o volume em `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Desanexe o volume da instância temporária (você o desmontou na etapa anterior): no console do Amazon EC2, selecione Volumes (Volumes) no painel de navegação, selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior), escolha Actions (Ações), Detach Volume (Desanexar volume) e, depois, Detach (Desanexar). Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)
3. Associe o volume novamente à instância original: com o volume ainda selecionado, escolha Actions (Ações), Attach Volume (Anexar volume). Selecione o ID de instância da instância original, especifique o nome do dispositivo anotado anteriormente na etapa 2 para o anexo do dispositivo raiz original (`/dev/sda1` ou `/dev/xvda`) e selecione Attach volume (Anexar volume).

> **Important**
>
> Se você não especificar o mesmo nome do dispositivo do anexo original, não poderá iniciar a instância original. O Amazon EC2 espera que o volume raiz seja `sda1` ou `/dev/xvda`.

Etapa 8: Conectar-se à instância original usando o novo par de chaves

Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após a instância entrar no estado `running`, é possível se conectar a ela usando o arquivo de chave privada do seu novo par de chaves.

> **Note**
>
> Se o nome do novo par de chaves e do arquivo de chaves privadas correspondente for diferente do nome do par de chaves original, especifique o nome do novo arquivo de chave privada conectado à sua instância.

Etapa 9: Limpeza

(Opcional) É possível encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

.

Se você estiver se conectando à instância usando o Putty e precisar converter o arquivo `.pem` em `.ppk`, consulte Converta a chave privada usando o PuTTYgen no tópico Conectar à instância do Linux a partir do Windows usando PuTTY desta seção.

- Definir as permissões do arquivo de chave privada de modo que só você possa lê-lo
  - Conectar do macOS ou do Linux

    (Instâncias do Linux) Se você planeja usar um cliente SSH em um computador macOS ou Linux para se conectar à instância do Linux, use o comando apresentado a seguir para definir as permissões do arquivo de chave privada para que somente você possa lê-lo.

```
chmod 400 key-pair-name.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para ter mais informações, consulte Erro: arquivo de chave privada desprotegido.

- Conectar do Windows

  Abra o Explorador de Arquivos e clique com o botão direito do mouse no arquivo `.pem`. Selecione a guia Propriedades > Segurança e escolha Avançado. Escolha Desabilitar herança. Remova o acesso para todos os usuários, exceto para o usuário atual.

(Opcional) Obter a impressão digital da instância

Para se proteger de ataques “man-in-the-middle”, você poderá verificar a autenticidade da instância à qual está prestes a se conectar, conferindo a impressão digital exibida. A verificação da impressão digital será útil se você executar a instância usando uma AMI pública fornecida por terceiros.

Visão geral da tarefa

Primeiro, obtenha a impressão digital da instância diretamente da instância. Em seguida, quando você se conectar à instância e receber a solicitação para verificar a impressão digital, compare a impressão digital que obteve nesse procedimento com a impressão digital exibida. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se elas corresponderem, será possível se conectar à instância com confiança.

Pré-requisitos para obter a impressão digital da instância

- A instância não deve estar no estado `pending`. A impressão digital só estará disponível após a conclusão da primeira inicialização da instância.
- Você deve ser o proprietário da instância para obter a saída do console.
- Há várias maneiras de obter a impressão digital da instância. Se você quiser usar a AWS CLI, ela deverá estar instalada no seu computador local. Para obter informações sobre como instalar a AWS CLI, consulte Instalação da AWS Command Line Interface no Guia do usuário da AWS Command Line Interface.

Para obter a impressão digital da instância

Na Etapa 1, você obtém a saída do console, que inclui a impressão digital da instância. Na Etapa 2, você encontra a impressão digital da instância na saída do console.

1. Use um dos métodos a seguir para obter a saída do console.

   Console

   1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   2. No navegador à esquerda, escolha Instâncias.
   3. Selecione sua instância e escolha Ações, Monitorar e solucionar problemas e Obter log do sistema.

   AWS CLI

   No computador local (e não na instância com a qual você está se conectando), use o comando get-console-output (AWS CLI). Se a saída for grande, você poderá redirecioná-la para um arquivo de texto, onde poderá ser mais fácil lê-la. Você deve especificar uma Região da AWS ao usar a AWS CLI, explicitamente ou definindo uma região padrão. Para obter informações sobre como definir ou especificar uma região, consulte Princípios básicos da configuração no Guia do usuário do AWS Command Line Interface.

   ```
   aws ec2 get-console-output --instance-id instance_id --query Output --output
    text > temp.txt
   ```

2. Na saída do console, encontre a impressão digital da instância (host), localizada abaixo de `BEGIN SSH HOST KEY FINGERPRINTS`. Pode haver impressões digitais de várias instâncias. Quando você se conecta à sua instância, ela exibe somente uma das impressões digitais.

   A saída exata pode variar de acordo com o sistema operacional, a versão da AMI e se a AWS criou o par de chaves. O seguinte é um exemplo de saída.

   ```
   ec2:#############################################################
   ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
   ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
   ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
   ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
   ec2: -----END SSH HOST KEY FINGERPRINTS-----
   ```

```
ec2: ##############################################################
```

> **Note**
>
> Você vai mencionar essa impressão digital quando se conectar à instância.

Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH.

Você pode usar o Secure Shell (SSH) para se conectar à instância do Linux a partir de uma máquina local que execute um sistema operacional Linux ou macOS, ou pode usar uma ferramenta de conexão independente de plataforma, como o EC2 Instance Connect ou o AWS Systems Manager Session Manager. Para obter mais informações sobre ferramentas independentes de plataforma, consulte Conecte-se à sua instância do Linux

Esta página explica como se conectar à sua instância com um cliente SSH. Para se conectar à instância do Linux a partir do Windows, consulte Conectar do Windows

> **Note**
>
> Se você receber um erro ao tentar se conectar à instância, certifique-se de que a instância atenda a todos os Pré-requisitos de conexão via SSH. Se ela atender a todos os pré-requisitos e, mesmo assim, você não conseguir se conectar à instância do Linux, consulte Solução de problemas de conexão com a instância do Linux.

Conteúdo

- Pré-requisitos de conexão via SSH
- Conectar-se à instância do Linux usando um cliente SSH
- Transfira arquivos para instâncias do Linux usando um cliente SCP

Pré-requisitos de conexão via SSH

Antes de você se conectar à sua instância do Linux, preencha os pré-requisitos a seguir.

Verificar o status da instância

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

Obter o nome público do DNS e o nome de usuário para fazer a conexão à sua instância

Para localizar o nome DNS público ou o endereço IP da instância e o nome de usuário que use para se conectar à instância, consulte Obter informações sobre a instância.

Encontrar a chave privada e definir as permissões

Para localizar a chave privada que é necessária para se conectar à sua instância e para definir as permissões de chave, consulte Localizar a chave privada e definir permissões.

Instale um cliente SSH no computador local conforme necessário

O computador local pode ter um cliente SSH instalado por padrão. Isso pode ser verificado ao digitar ssh na linha de comando. Se o seu computador não reconhecer o comando, é possível instalar um cliente SSH.

- Versões recentes do Windows Server 2019 e do Windows 10: o OpenSSH está incluído como um componente instalável. Para obter mais informações, consulte OpenSSH no Windows.
- Versões anteriores do Windows: baixe e instale o OpenSSH. Para obter mais informações, consulte Win32-OpenSSH.
- Linux e macOS X: baixe e instale o OpenSSH. Para obter mais informações, consulte https://www.openssh.com.

Conectar-se à instância do Linux usando um cliente SSH

Use o procedimento a seguir para se conectar à sua Instância do Linux usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Conectar a sua instância usando SSH

1. Em uma janela do terminal, use o comando ssh para se conectar à instância. Especifique o caminho e o nome do arquivo da chave privada (`.pem`), o nome de usuário da instância e o nome DNS público ou o endereço IPv6 da instância. Para obter mais informações sobre como localizar a chave privada, o nome de usuário da instância e o nome DNS ou o endereço IPv6

de uma instância, consulte Localizar a chave privada e definir permissões e Obter informações sobre a instância. Para se conectar à instância, use um dos comandos a seguir.

- (DNS público) Para se conectar usando o nome DNS público da instância, insira o comando a seguir.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Como alternativa, se sua instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, digite o comando a seguir.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se corresponderem, continue para a próxima etapa.
3. Digite **yes**.

   Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Transfira arquivos para instâncias do Linux usando um cliente SCP

O protocolo de cópia segura (SCP) é uma das alternativas para transferir arquivos entre seu computador local e uma instância do Linux. Esta seção descreve como transferir arquivos com o SCP. O procedimento é semelhante ao procedimento de conexão a uma instância com o SSH.

Pré-requisitos

- Verifique os pré-requisitos gerais para transferir arquivos à instância.

Antes de transferir arquivos entre a máquina local e sua instância, execute as ações a seguir para garantir que você tenha todas as informações necessárias.

- Obter informações sobre a instância
- Localizar a chave privada e definir permissões
- (Opcional) Obter a impressão digital da instância

- Instalação de um cliente SCP

  A maioria dos computadores com Linux, Unix e Apple incluem um cliente SCP por padrão. Se seu não incluir, o projeto OpenSSH oferece implantação grátis do pacote completo das ferramentas SSH, inclusive um cliente SCP. Para obter mais informações, consulte https://www.openssh.com.

O procedimento a seguir acompanha o uso do SCP para transferir um arquivo usando o nome DNS público da instância ou o endereço IPv6 se sua instância tiver um.

Para usar o SCP para transferir arquivos entre o computador e a sua instância

1. Determine a localização do arquivo de origem no seu computador e o caminho de destino na instância. Nos exemplos a seguir, o nome do arquivo de chave privada é `key-pair-name.pem`, o arquivo a ser transferido é `my-file.txt`, o nome de usuário da instância é ec2-user, o nome de DNS público da instância é `instance-public-dns-name` e o endereço IPv6 da instância é `instance-IPv6-address`.
   - (DNS público) Para transferir um arquivo para o destino na instância, insira o seguinte comando do seu computador.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```

   - (IPv6) Para transferir um arquivo para o destino na instância, se ela tiver um endereço IPv6, insira o seguinte comando no seu computador. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
     ```

2. Se ainda não tiver conectado à instância usando SSH, você verá uma resposta como a seguinte:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   ```

```
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Opcional) Também é possível verificar se a impressão digital no alerta de segurança corresponde à impressão digital da instância. Para ter mais informações, consulte (Opcional) Obter a impressão digital da instância.

Digite **yes**.

3. Se a transferência for bem-sucedida, a resposta será semelhante à seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Para transferir um arquivo na outra direção (de uma instância do Amazon EC2 para o seu computador), basta inverter a ordem dos parâmetros do host. Por exemplo, é possível transferir o `my-file.txt` da instância do EC2 para um destino no seu computador local `my-file2.txt`, conforme exibido nos exemplos a seguir.

   - (DNS Público) Para transferir um arquivo para um destino no seu computador, insira o seguinte comando do seu computador.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
     ```

   - (IPv6) Para transferir um arquivo para um destino no computador se a instância tiver um endereço IPv6, insira o seguinte comando do seu computador. O endereço IPv6 deve vir entre colchetes (`[ ]`), que devem ser recuados (\).

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-file.txt path/my-file2.txt
     ```

Conectar à instância do Linux a partir do Windows

Você pode usar os métodos a seguir para se conectar à instância do Linux a partir de uma máquina local com sistema operacional Windows.

Conectar à instância do Linux via Windows com OpenSSH

Os procedimentos a seguir mostram como é possível conectar à instância do Linux via Windows usando o OpenSSH, uma ferramenta de conectividade de código aberto para login remoto que utiliza o protocolo SSH. O OpenSSH é compatível com sistemas operacionais Windows Server 2019 e posteriores.

Sumário

- Pré-requisitos
- Instale o OpenSSH para Windows usando o PowerShell
- Conectar à instância do Linux via Windows com o OpenSSH
- Desinstalar o OpenSSH do Windows usando o PowerShell

Pré-requisitos

Antes de você se conectar à sua instância do Linux via Windows usando o OpenSSH, complete os pré-requisitos a seguir.

Verifique se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

Verifique os pré-requisitos gerais para se conectar à instância

Para localizar o nome de DNS público ou o endereço IP da instância e o nome de usuário utilizado para se conectar à instância, consulte Obter informações sobre a instância.

Verifique a versão do Windows

Para que você possa se conectar à instância do Linux via Windows com o OpenSSH, a versão do Windows deve ser Windows Server 2019 ou posterior.

Verifique os pré-requisitos do PowerShell

Para instalar o OpenSSH no sistema operacional Windows usando o PowerShell, é necessário executar o PowerShell versão 5.1 ou posterior e sua conta deve ser membro do grupo de administradores do sistema. Execute o comando `$PSVersionTable.PSVersion` no PowerShell para verificar a versão do PowerShell.

Para verificar se você é membro do grupo de administradores do sistema, execute o seguinte comando do PowerShell:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Se você for membro do grupo de administradores do sistema, a saída será `True`.

Instale o OpenSSH para Windows usando o PowerShell

Para instalar o OpenSSH para Windows usando o PowerShell, execute o seguinte comando do PowerShell:

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Saída esperada:

```
Path          :
Online        : True
RestartNeeded : False
```

Conectar à instância do Linux via Windows com o OpenSSH

Após instalar o OpenSSH, use o procedimento a seguir para se conectar à instância do Linux via Windows usando o OpenSSH. Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Para se conectar à instância usando o OpenSSH

1. No PowerShell ou no prompt de comando, use o comando ssh para se conectar à instância. Especifique o caminho e o nome do arquivo da chave privada (`.pem`), o nome de usuário da instância e o nome de DNS público ou o endereço IPv6 da instância. Para obter mais informações sobre como localizar a chave privada, o nome de usuário da instância e o nome de DNS ou o endereço IPv6 de uma instância, consulte Localizar a chave privada e definir permissões e Obter informações sobre a instância. Para se conectar à instância, use um dos comandos a seguir.
   - (DNS público) Para se conectar usando o nome DNS público da instância, insira o comando a seguir.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Como alternativa, se sua instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, digite o comando a seguir.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se corresponderem, continue para a próxima etapa.
3. Digite **`yes`**.

   Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Desinstalar o OpenSSH do Windows usando o PowerShell

Para instalar o OpenSSH do Windows usando o PowerShell, execute o seguinte comando do PowerShell:

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Saída esperada:

```
Path          :
Online        : True
RestartNeeded : True
```

Conectar à instância do Linux a partir do Windows usando PuTTY

Se você estiver executando o Windows Server 2019 ou posterior, recomendamos usar o OpenSSH, uma ferramenta de conectividade de código aberto para login remoto via protocolo SSH. Para conhecer as etapas para se conectar a uma instância do Linux via Windows usando o OpenSSH, consulte Conectar à instância do Linux via Windows com OpenSSH.

As instruções a seguir explicam como se conectar à sua instância usando PuTTY, um cliente SSH gratuito para Windows. Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Sumário

- Pré-requisitos
  - Converta a chave privada usando o PuTTYgen
- Conecte-se à sua instância do Linux
- Transferir arquivos da sua instância do Linux usando o cliente PuTTY Secure Copy
- Transferir arquivos uma sua instância do Linux usando WinSCP

Pré-requisitos

Antes de você se conectar à sua instância do Linux usando o PuTTY, preencha os pré-requisitos a seguir.

Verifique se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

Verifique os pré-requisitos gerais para se conectar à instância

Para localizar o nome de DNS público ou o endereço IP da instância e o nome de usuário utilizado para se conectar à instância, consulte Obter informações sobre a instância.

Instale o PuTTY no computador local

Faça download e instale o PuTTY pela página de download do PuTTY. Se já houver uma versão anterior do PuTTY instalada, recomendamos fazer download da versão mais recente. Instale o pacote inteiro.

Converter a chave privada .pem em .ppk usando o PuTTYgen

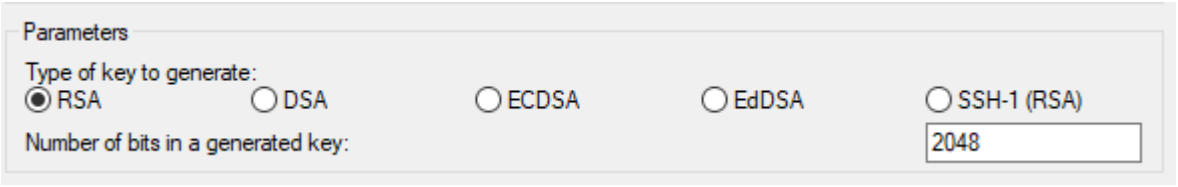
Para o par de chaves que você especificou ao iniciar a instância, se você escolher criar a chave privada no formato .pem, será necessário convertê-la em um arquivo .ppk para usá-la com PuTTY. Localize o arquivo .pem privado e siga as etapas da próxima seção.

Converta a chave privada usando o PuTTYgen

O PuTTY não é originalmente compatível com o formato PEM para chaves SSH. O PuTTY fornece uma ferramenta chamada PuTTYgen, que converte as chaves PEM para o formato PPK necessário para PuTTY. É necessário converter sua chave privada (arquivo .pem) nesse formato (arquivo .ppk) conforme a seguir para se conectar à sua instância usando PuTTY.

Para converter sua chave privada .pem para o formato .ppk

1. No menu Start (Iniciar), selecione All Programs (Todos os programas), PuTTY, PuTTYgen.
2. Em Tipo de chave a ser gerada, escolha RSA. Se a sua versão de PuTTYgen não inclui esta opção, escolha SSH-2 RSA.



3. Escolha Load. Por padrão, o PuTTYgen exibe somente arquivos com a extensão `.ppk`. Para localizar o arquivo `.pem`, escolha a opção para exibir arquivos de todos os tipos.

4. Selecione o arquivo `.pem` para o par de chaves que você especificou ao executar a instância e selecione Open (Abrir). A PuTTYgen exibe um aviso de que o arquivo `.pem` foi importado com êxito. Escolha OK.
5. Escolha Save private key (Salvar chave privada) para salvar a chave no formato PuTTY. A PuTTYgen exibe um aviso sobre salvar a chave sem uma senha. Escolha Sim.

> **Note**
>
> Uma senha em uma chave privada é uma camada extra de proteção. Mesmo se a chave privada for descoberta, ela não pode ser usada sem a senha. A desvantagem de se usar uma senha é que a automação se torna mais difícil porque a intervenção humana é necessária para fazer login em uma instância, ou para copiar arquivos a uma instância.

6. Especifique o mesmo nome da chave usado para o par de chaves (por exemplo, `key-pair-name`) e escolha Save (Salvar). O PuTTY adiciona automaticamente a extensão de arquivo `.ppk`.

Sua chave privada está agora no formato correto para uso com o PuTTY. Agora é possível conectar a sua instância usando o cliente SSH do PuTTY.

Conecte-se à sua instância do Linux

Use o procedimento a seguir para se conectar à sua Instância do Linux usando o PuTTY. Você precisa do arquivo `.ppk` que criou para sua chave privada. Para obter mais informações, consulte Converta a chave privada usando o PuTTYgen na seção anterior. Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Última versão testada do PuTTY: .78

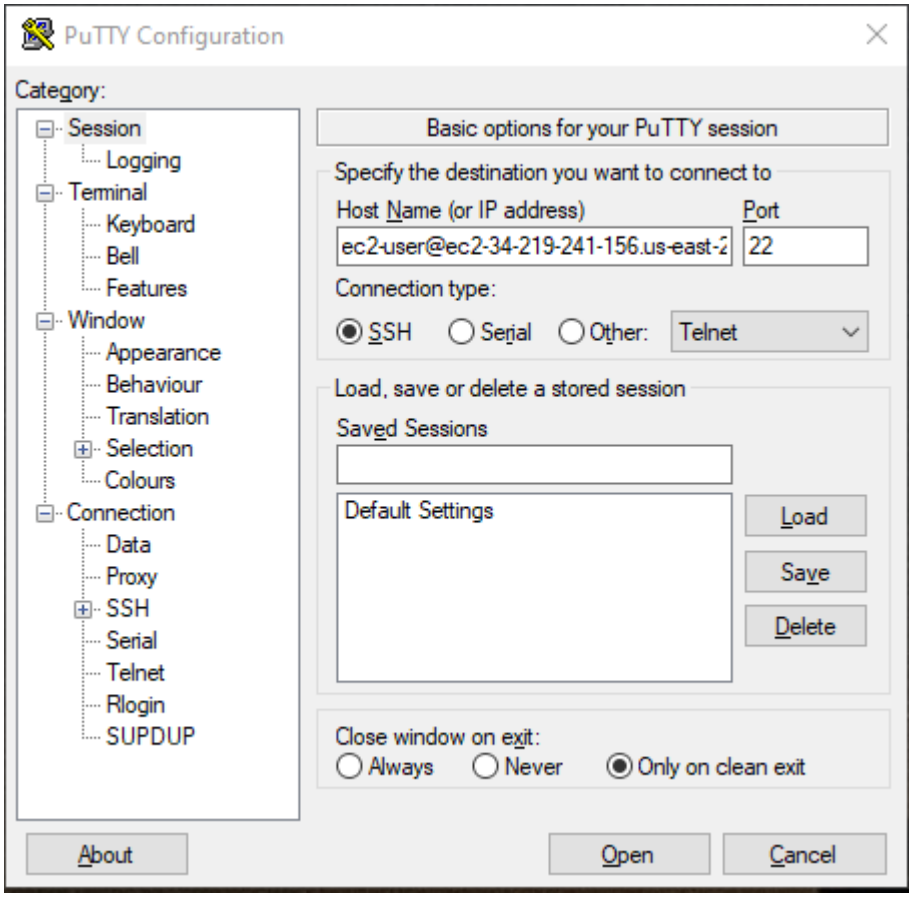
Para se conectar à instância usando PuTTY

1. Inicie o PuTTY (no menu Iniciar, pesquise PuTTY e escolha Abrir).
2. No painel Categoria, selecione Sessão e preencha os seguintes campos:
   a. Na caixa Host Name (Nome do host), execute uma das ações a seguir:
      - (DNS Público) Para se conectar usando o nome DNS público da instância, insira *instance-user-name*@*instance-public-dns-name*.
      - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, insira *instance-user-name*@*instance-IPv6-address*.

      Para obter informações sobre como obter o nome de usuário da instância e o nome de DNS público ou o endereço IPv6 da instância, consulte Obter informações sobre a instância.

b. Verifique se o valor do Port é 22.

c. Em Tipo de conexão, selecione SSH.



3. (Opcional) É possível configurar o PuTTY para enviar automaticamente dados "keepalive" em intervalos regulares para manter a sessão ativa. Isso é útil para evitar a desconexão da instância por inatividade da sessão. No painel Categoria, escolha Conexão e insira o intervalo necessário no campo Segundos entre keepalives. Por exemplo, se a sessão desconectar após 10 minutos de inatividade, insira 180 para configurar o PuTTY para enviar dados keepalive a cada 3 minutos.
4. No painel Categoria, expanda Conexão, SSH e Auth. Escolha Credenciais.
5. Ao lado de Arquivo de chave privada para autenticação, escolha Procurar. Na caixa de diálogo Selecionar arquivo de chave privada, selecione o arquivo `.ppk` que você gerou para seu par de chaves. Clique duas vezes no arquivo ou escolha Abrir na caixa de diálogo Selecionar arquivo de chave privada.

6. (Opcional) Se você planeja se conectar a esta instância novamente após esta sessão, poderá salvar as informações para uso futuro. No painel Categoria, escolha Sessão. Insira um nome para a sessão em Sessões salvas e, em seguida, escolha Salvar.
7. Para se conectar à instância, escolha Abrir.
8. Se essa for a primeira vez você se conectou a esta instância, o PuTTY exibirá uma caixa de diálogo de alerta de segurança perguntando se você confia no host ao qual está se conectando.

    a. (Opcional) Verifique se a impressão digital na caixa de diálogo do alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.

    b. Escolha Accept (Aceitar). Uma janela se abrirá e você estará conectado à sua instância.

    > **Note**
    >
    > Se você especificou uma senha ao converter sua chave privada em formato PuTTY, forneça essa senha ao efetuar o login na instância.

Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Transferir arquivos da sua instância do Linux usando o cliente PuTTY Secure Copy

O cliente PuTTY Secure Copy (PSCP) é uma ferramenta da linha de comando que é possível usar para transferir arquivos entre seu computador Windows e sua instância do Linux. Se você preferir uma interface gráfica de usuário (GUI), pode usar uma ferramenta de GUI de uso aberto chamada WinSCP. Para ter mais informações, consulte Transferir arquivos uma sua instância do Linux usando WinSCP.

Para usar o PSCP, você precisar da chave privada gerada em Converta a chave privada usando o PuTTYgen. Você também precisa do nome DNS público da instância do Linux ou do endereço IPv6 se a instância tiver um.

O exemplo a seguir transfere o arquivo `Sample_file.txt` da unidade C:\ em um computador Windows para o diretório inicial `instance-user-name` em uma instância do Amazon Linux. Para transferir um arquivo, use um dos comandos a seguir.

- (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para transferir um arquivo usando o endereço IPv6 da instância, insira o comando a seguir. O endereço IPv6 deve estar entre colchetes (`[ ]`).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

Transferir arquivos uma sua instância do Linux usando WinSCP

O WinSCP é um gerenciador de arquivos baseado em GUI para Windows que permite carregar e transferir arquivos a um computador remoto usando os protocolos SFTP, SCP, FTP e FTPS. Com o WinSCP, é possível arrastar e soltar arquivos do computador Windows para a instância do Linux ou sincronizar estruturas de diretório inteiras entre os dois sistemas.

Requisitos

- É necessário ter a chave privada gerada no Converta a chave privada usando o PuTTYgen.
- Também é necessário ter o nome DNS público da instância do Linux.
- Sua instância do Linux deve ter `scp` instalado. Para alguns sistemas operacionais, instale o pacote `openssh-clients`. Para outros, como a AMI otimizada para o Amazon ECS, instale o pacote `scp`. Verifique a documentação da sua distribuição do Linux.

Como se conectar à instância usando WinSCP

1. Faça download e instale WinSCP em http://winscp.net/eng/download.php. Para a maioria dos usuários, as opções de instalação padrão são OK.
2. Inicie o WinSCP.
3. Na tela de Login do WinSCP, em Nome do host, insira uma das seguintes opções:
    - (DNS público ou endereço IPv4) Para fazer login usando o nome DNS público ou o endereço IPv4 público da instância, insira o nome DNS público ou o endereço IPv4 público da instância.

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para fazer login usando o endereço IPv6 da instância, insira o endereço IPv6 para a instância.

4. Para Nome de usuário, insira o nome de usuário padrão para sua AMI.

   - Para AL2023, Amazon Linux 2 ou Amazon Linux AMI, o nome do usuário é `ec2-user`.
   - Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
   - Para uma AMI do Debian, o nome do usuário é `admin`.
   - Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
   - Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
   - Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
   - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
   - Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
   - Para uma AMI do Bitnami, o nome do usuário é `bitnami`.

   > **Note**
   >
   > Para encontrar o nome de usuário padrão para outras distribuições Linux, verifique com o fornecedor da AMI.

5. Especifique o arquivo de chave privada para sua instância.

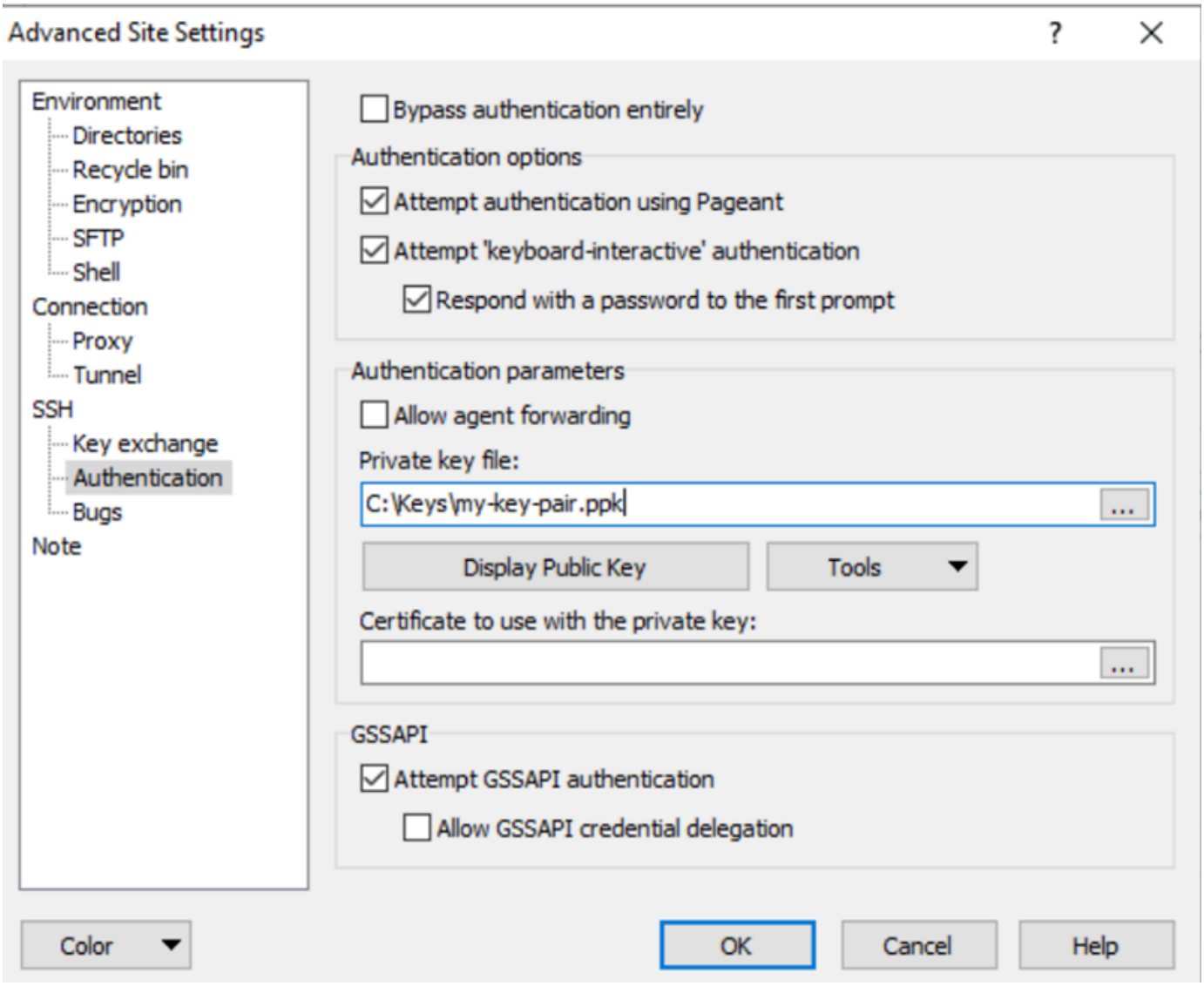
   a. Selecione o botão Avançado....

   b. Em SSH, selecione Autenticação.

   c. Especifique o caminho para o seu arquivo de chave privada ou selecione o botão ... para navegar até o arquivo do par de chaves.

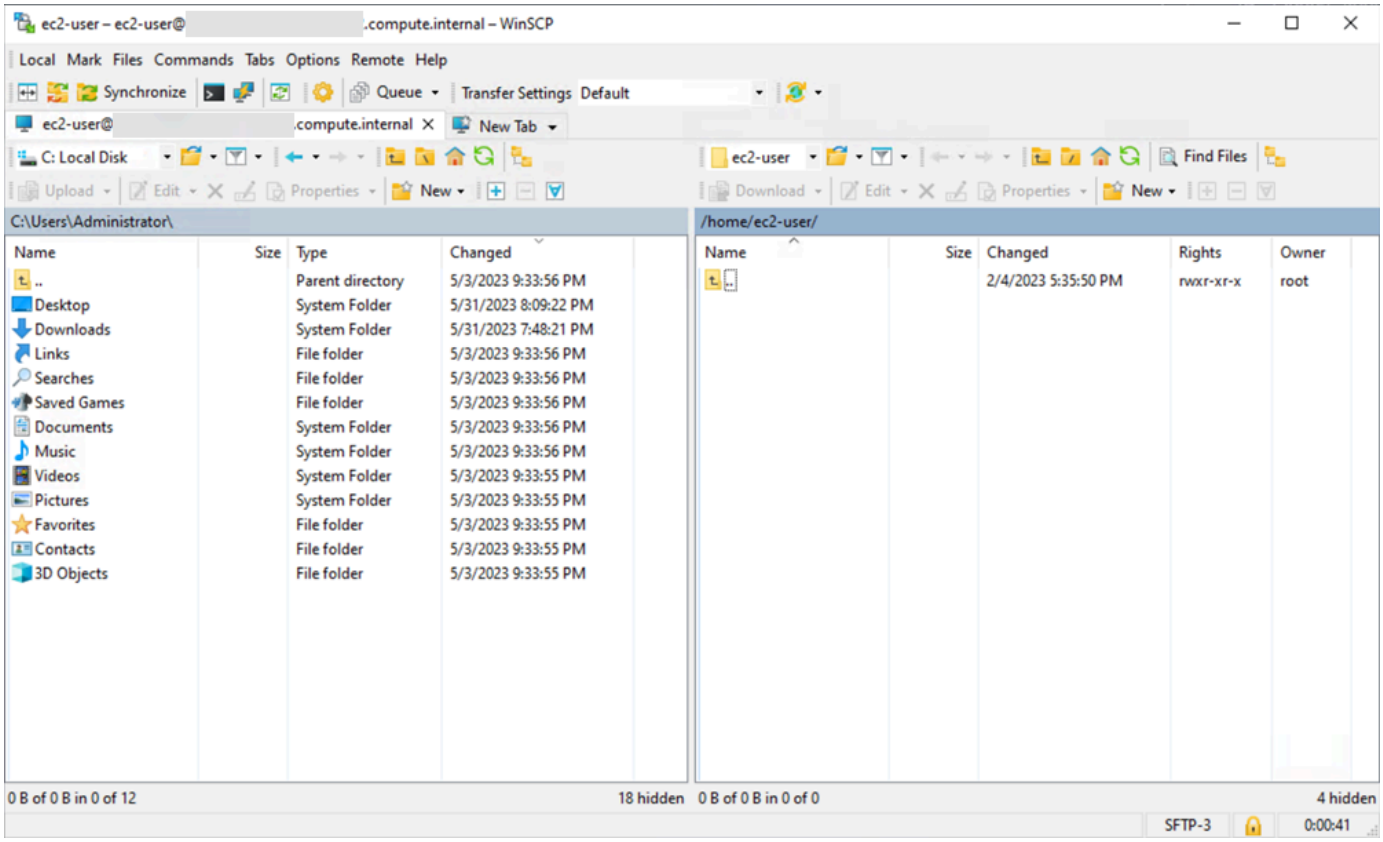
   d. Escolha OK.

   Aqui está uma captura de tela do WinSCP versão 6.1:



O WinSCP exige um arquivo de chave privada do PuTTY (`.ppk`). É possível converter um arquivo de chave de segurança `.pem` para o formato `.ppk` usando PuTTYgen. Para ter mais informações, consulte Converta a chave privada usando o PuTTYgen.

6. (Opcional) No painel à esquerda, selecione Directories (Diretórios). Para Remote directory (Diretório remoto), informe o caminho para o diretório ao qual adicionar arquivos. Para abrir as configurações avançadas do site, em busca de novas versões do WinSCP, selecione Advanced (Avançado). Para encontrar a configuração Remote directory (Diretório remoto), em Environment (Ambiente), selecione Directories (Diretórios).
7. Escolha Login (Fazer login). Para adicionar a impressão digital do host, selecione Yes (Sim).



8. Após a conexão ser estabelecida, na janela de conexão, sua instância do Linux está à direita e sua máquina local está à esquerda. É possível arrastar e soltar arquivos entre o sistema de arquivos remoto e a máquina local. Para obter mais informações sobre WinSCP, consulte a documentação do projeto em http://winscp.net/eng/docs/start.

   Se você receber um erro indicando não ser possível executar o SCP para iniciar a transferência, verifique se você instalou scp na instância do Linux.

Conecte-se à sua instância do Linux a partir do Windows usando o Windows Subsystem for Linux (WSL).

Depois que iniciar sua instância, será possível conectá-la e usá-la da forma como usaria um computador bem na sua frente.

As instruções a seguir explicam como se conectar à instância usando uma distribuição do Linux no Windows Subsystem for Linux (WSL). O WSL pode ser baixado gratuitamente e permite que você execute ferramentas da linha de comando diretamente no Windows, no desktop tradicional do Windows, sem as despesas gerais de uma máquina virtual.

Ao instalar o WSL, é possível usar um ambiente Linux nativo para se conectar às instâncias EC2 do Linux, em vez de usar o PuTTY ou o PuTTYgen. No ambiente Linux, é mais fácil conectar-se às instâncias do Linux porque ele oferece um cliente SSH nativo que é possível usar para se conectar a essas instâncias e alterar as permissões do arquivo de chave .pem. O console do Amazon EC2 fornece o comando SSH para você se conectar com a instância do Linux. Além disso, é possível obter uma saída mais detalhada do comando SSH para solução de problemas. Para obter mais informações, consulte a documentação do Subsistema do Windows para Linux.

> **Note**
>
> Ao instalar o WSL, todos os pré-requisitos e etapas são iguais aos descritos em Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH., e a experiência é exatamente igual a usar um Linux nativo.

Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Sumário

- Pré-requisitos
- Conectar-se à instância do Linux usando WSL
- Transferir arquivos para instâncias do Linux usando SCP
- Desinstalar o WSL

Pré-requisitos

Antes de você se conectar à sua instância do Linux, preencha os pré-requisitos a seguir.

Verifique se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

Verifique os pré-requisitos gerais para se conectar à instância

Para localizar o nome DNS público ou o endereço IP da instância e o nome de usuário que use para se conectar à instância, consulte Obter informações sobre a instância.

Instale o Subsistema Windows para Linux (WSL) e uma distribuição do Linux no computador local

Instale o WSL e uma distribuição do Linux usando as instruções do Guia de instalação do Windows 10. O exemplo fornecido nas instruções instala a distribuição Ubuntu do Linux, mas é possível instalar qualquer distribuição. Você é solicitado a reiniciar o computador para que as alterações sejam implementadas.

Cópia da chave privada do Windows para o WSL

Em uma janela de terminal do WSL, copie o arquivo `.pem` (para o par de chaves que você especificou ao executar a instância) do Windows para o WSL. Observe o caminho totalmente qualificado para o arquivo `.pem` no WSL, que use para se conectar à sua instância. Para obter informações sobre como especificar o caminho para o disco rígido do Windows, consulte How do I access my C drive?. Para obter mais informações sobre pares de chaves e instâncias do Windows, consulte Pares de chaves do Amazon EC2 e instâncias do Windows.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Conectar-se à instância do Linux usando WSL

Use o procedimento a seguir para se conecta à sua instância do Linux usando o Subsistema do Windows para Linux (WSL). Se você receber um erro ao tentar se conectar à instância, consulte Solução de problemas de conexão com a instância do Linux.

Para se conectar à sua instância usando SSH

1. Em uma janela do terminal, use o comando ssh para se conectar à instância. Especifique o caminho e o nome do arquivo da chave privada (`.pem`), o nome de usuário da instância e o nome DNS público ou o endereço IPv6 da instância. Para obter mais informações sobre como localizar a chave privada, o nome de usuário da instância e o nome DNS ou o endereço IPv6 de uma instância, consulte Localizar a chave privada e definir permissões e Obter informações sobre a instância. Para se conectar à instância, use um dos comandos a seguir.
   - (DNS público) Para se conectar usando o nome DNS público da instância, insira o comando a seguir.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
     ```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, será possível se conectar à instância usando seu endereço IPv6. Especifique o comando ssh com o caminho até o arquivo de chave privada (.pem), o nome de usuário apropriado e o endereço IPv6.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
3. Digite `yes`.

   Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

Transferir arquivos para instâncias do Linux usando SCP

O protocolo de cópia segura (SCP) é uma das alternativas para transferir arquivos entre seu computador local e uma instância do Linux. Esta seção descreve como transferir arquivos com o SCP. O procedimento é semelhante ao procedimento de conexão a uma instância com o SSH.

Pré-requisitos

- Verifique os pré-requisitos gerais para transferir arquivos à instância.

  Antes de transferir arquivos entre a máquina local e sua instância, execute as ações a seguir para garantir que você tenha todas as informações necessárias.

  - Obter informações sobre a instância
  - Localizar a chave privada e definir permissões

  - (Opcional) Obter a impressão digital da instância
- Instalação de um cliente SCP

  A maioria dos computadores com Linux, Unix e Apple incluem um cliente SCP por padrão. Se seu não incluir, o projeto OpenSSH oferece implantação grátis do pacote completo das ferramentas SSH, inclusive um cliente SCP. Para obter mais informações, consulte https://www.openssh.com.

As etapas de procedimento a seguir guiam você pelo uso de SCP para transferir o arquivo. Se você já tiver se conectado à instância com o SSH e tiver verificado suas impressões digitais, será possível começar com a etapa que contém o comando SCP (etapa 4).

Para usar o SCP para transferir um arquivo

1. Transfira um arquivo para sua instância usando o nome DNS público da instância. Por exemplo, se o nome do arquivo de chave privada for `key-pair-name`, o arquivo a transferir for `SampleFile.txt`, o nome do usuário for `instance-user-name` e o nome DNS público da instância for `my-instance-public-dns-name` ou o endereço IPv6 for `my-instance-IPv6-address`, use os comandos a seguir para copiar o arquivo para o diretório inicial `instance-user-name`.
   - (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
     ```
   - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, será possível transferir um arquivo usando o endereço IPv6 da instância. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@\[my-instance-IPv6-address\]:~
     ```

   Você verá uma resposta como a seguinte:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
3. Digite **yes**.

   Você verá uma resposta como a seguinte:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   Sending file modes: C0644 20 SampleFile.txt
   Sink: C0644 20 SampleFile.txt
   SampleFile.txt                                100%   20     0.0KB/s   00:00
   ```

   Se você receber o erro "bash: scp: command not found", deverá primeiro instalar scp na sua instância do Linux. Para alguns sistemas operacionais, isso está localizado no pacote `openssh-clients`. Para variantes do Amazon Linux, como a Amazon ECS otimizada por AMI, use o comando para instalar o scp:

   ```
   [ec2-user ~]$ sudo yum install -y openssh-clients
   ```
4. Para transferir arquivos na outra direção (de uma instância do Amazon EC2 para o computador local), basta inverter a ordem dos parâmetros do host. Por exemplo, para transferir o arquivo `SampleFile.txt` da instância do EC2 de volta ao diretório inicial no computador local como `SampleFile2.txt`, use um dos comandos a seguir no computador local.
   - (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

     ```
     scp -i /path/key-pair-name.pem instance-user-
     name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/
     SampleFile2.txt
     ```
   - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para transferir arquivos na outra direção usando o endereço IPv6 da instância, insira o comando a seguir.

     ```
     scp -i /path/key-pair-name.pem instance-user-name@
     \[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
     ```

Desinstalar o WSL

Para obter informações sobre como desinstalar o Subsistema Windows para Linux, consulte Como desinstalar o WSL Distribution?.

Conectar-se à instância do Linux com o EC2 Instance Connect

O Amazon EC2 Instance Connect fornece uma forma simples e segura de conectar a instâncias do Linux com o Secure Shell (SSH). Com o EC2 Instance Connect, você usa políticas do AWS Identity and Access Management (IAM) e principais para controlar o acesso de SSH às suas instâncias, eliminando a necessidade de compartilhar e gerenciar as chaves de SSH. Todas as solicitações de conexão usando o EC2 Instance Connect são registradas no AWS CloudTrail para que você possa auditar as solicitações de conexão.

É possível usar o EC2 Instance Connect para se conectar às suas instâncias usando o console do Amazon EC2 ou um cliente SSH da sua escolha.

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do Instance Connect envia por push e uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. A política do IAM anexada ao usuário autoriza o usuário a enviar por push a chave pública para os metadados da instância. O daemon SSH usa `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, que são configurados quando o Instance Connect é instalado, para procurar a chave pública dos metadados da instância para autenticação e conectar você à instância.

É possível usar EC2 Instance Connect para se conectar a instâncias que têm endereços IP públicos ou privados. Para ter mais informações, consulte Conectar-se usando EC2 Instance Connect.

Para obter uma postagem de blog que discute como melhorar a segurança de bastion hosts usando o EC2 Instance Connect, consulte Proteção dos seus bastion hosts com o Amazon EC2 Instance Connect.

> **Tip**
>
> O EC2 Instance Connect é uma das opções para se conectar a instâncias do Linux. Para obter outras opções, consulte Conecte-se à sua instância do Linux. Para se conectar a uma instância do Windows, consulte Conectar-se à sua instância do Windows do .

Conteúdo

- Tutorial: Concluir a configuração necessária para se conectar à sua instância usando o EC2 Instance Connect
- Pré-requisitos
- Conceder permissões do IAM para o EC2 Instance Connect
- Instalar o EC2 Instance Connect nas suas instâncias do EC2
- Conectar-se usando EC2 Instance Connect
- Desinstalar o EC2 Instance Connect

Tutorial: Concluir a configuração necessária para se conectar à sua instância usando o EC2 Instance Connect

Para se conectar à sua instância usando o EC2 Instance Connect no console do Amazon EC2, primeiro é necessário concluir a configuração de pré-requisito que permitirá que você se conecte com sucesso à sua instância. O objetivo deste tutorial é orientar você pelas tarefas de conclusão da configuração de pré-requisitos.

Visão geral do tutorial

Nesse tutorial, você deverá concluir as seguintes quatro tarefas:

- Tarefa 1: criar e anexar uma política do IAM para permitir que você use o EC2 Instance Connect

  Primeiro, você criará uma política do IAM que contenha as permissões do IAM que permitem que você envie uma chave pública para os metadados da instância. Você anexará essa política à sua identidade (usuário, grupo de usuários ou perfil) do IAM para que sua identidade do IAM receba essas permissões.
- Tarefa 2: criar um grupo de segurança que permita o tráfego do EC2 Instance Connect para sua instância

  Em seguida, você criará um grupo de segurança que permita o tráfego do EC2 Instance Connect para sua instância. Isso é necessário quando você usa o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância.
- Tarefa 3: iniciar sua instância

  Em seguida, você iniciará uma instância do EC2 usando uma AMI pré-instalada com o EC2 Instance Connect e adicionará o grupo de segurança que criou na etapa anterior.
- Tarefa 4: conectar à sua instância

Por fim, você usará o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância. Se você conseguir se conectar, poderá ter certeza de que a configuração de pré-requisito concluída nas Tarefas 1, 2 e 3 foi bem-sucedida.

Tarefa 1: criar e anexar uma política do IAM para permitir que você use o EC2 Instance Connect

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. É necessário ter uma política do IAM anexada à sua identidade do IAM (usuário, grupo de usuários ou função) para fornecer a permissão necessária para enviar por push a chave pública para os metadados da instância.

Objetivo da tarefa

Nessa tarefa, você criará a política do IAM que concede a permissão necessária para enviar por push a chave pública para a instância. A ação específica a ser permitida é `ec2-instance-connect:SendSSHPublicKey`. Você também deve permitir a ação `ec2:DescribeInstances` para poder visualizar e selecionar sua instância no console do Amazon EC2.

Depois de criar a política, você anexará a política à sua identidade do IAM (usuário, grupo de usuários ou perfil) para que sua identidade do IAM receba as permissões.

Você criará uma política configurada da seguinte forma:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

> **Important**
>
> A política do IAM criada neste tutorial é uma política altamente permissiva. Ela permite que você se conecte a qualquer instância usando qualquer nome de usuário da AMI. Estamos usando essa política altamente permissiva para manter o tutorial simples e focado nas configurações específicas que este tutorial está ensinando. No entanto, em um ambiente de produção, recomendamos que sua política do IAM seja configurada para fornecer permissões com privilégios mínimos. Para obter exemplos de políticas do IAM, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Etapas para criar e anexar a política do IAM

Use as etapas a seguir para criar e anexar a política do IAM. Para visualizar uma animação das etapas, consulte Visualizar uma animação: criar uma política do IAM e Visualizar uma animação: anexar uma política do IAM.

Para criar e anexar uma política do IAM que permita a você usar o EC2 Instance Connect para se conectar às suas instâncias

1. Crie primeiro a política do IAM
    a. Abra o console do IAM em https://console.aws.amazon.com/iam/.
    b. No painel de navegação, escolha Policies.
    c. Escolha Criar política.
    d. Na página Especificar permissão, faça o seguinte:
        i. Em Serviço, escolha EC2 Instance Connect.
        ii. Em Ações permitidas, no campo de pesquisa, comece a digitar **`send`** para mostrar as ações relevantes e selecione SendSSHPublicKey.
        iii. Em Recursos, escolha Todos. Para um ambiente de produção, recomendamos especificar a instância pelo ARN, mas, neste tutorial, você está permitindo todas as instâncias.
        iv. Escolha Add more permissions (Adicionar mais permissões).
        v. Em Serviço, escolha EC2.
        vi. Em Ações permitidas, no campo de pesquisa, comece a digitar **`describein`** para mostrar as ações relevantes e selecione DescribeInstances.

vii. Escolha Próximo.

e. Na página Revisar e criar, faça o seguinte:

i. Em Policy Name (Nome da política), digite um nome para a política.

ii. Escolha Criar política.

2. Em seguida, anexe a política à sua identidade

a. No console do IAM, no painel de navegação, escolha Policies (Políticas).

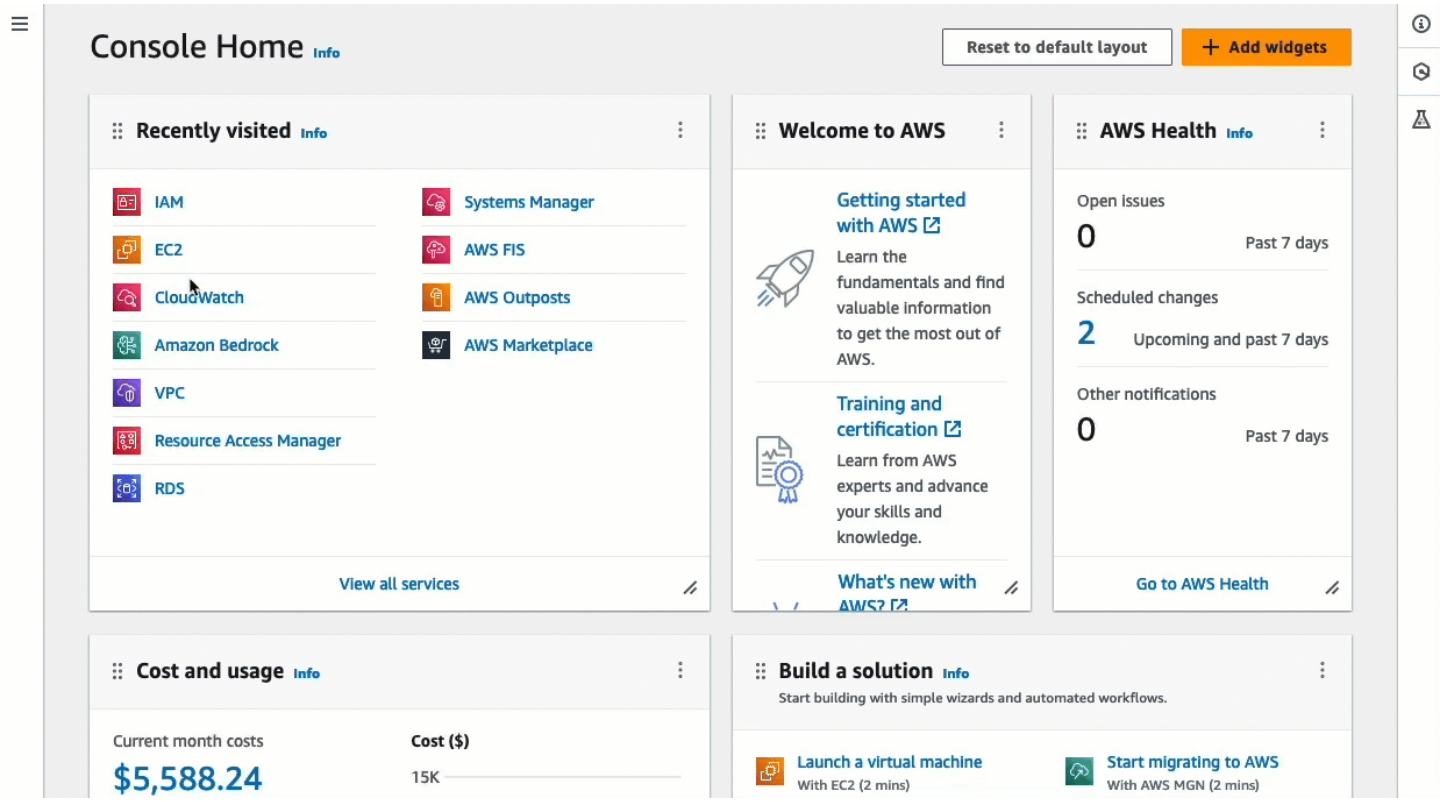
b. Na lista de políticas, selecione o botão de seleção ao lado do nome da política que você criou. Você pode usar a caixa de pesquisa para filtrar a lista de políticas.

c. Clique em Actions (Ações) e em Attach (Associar).

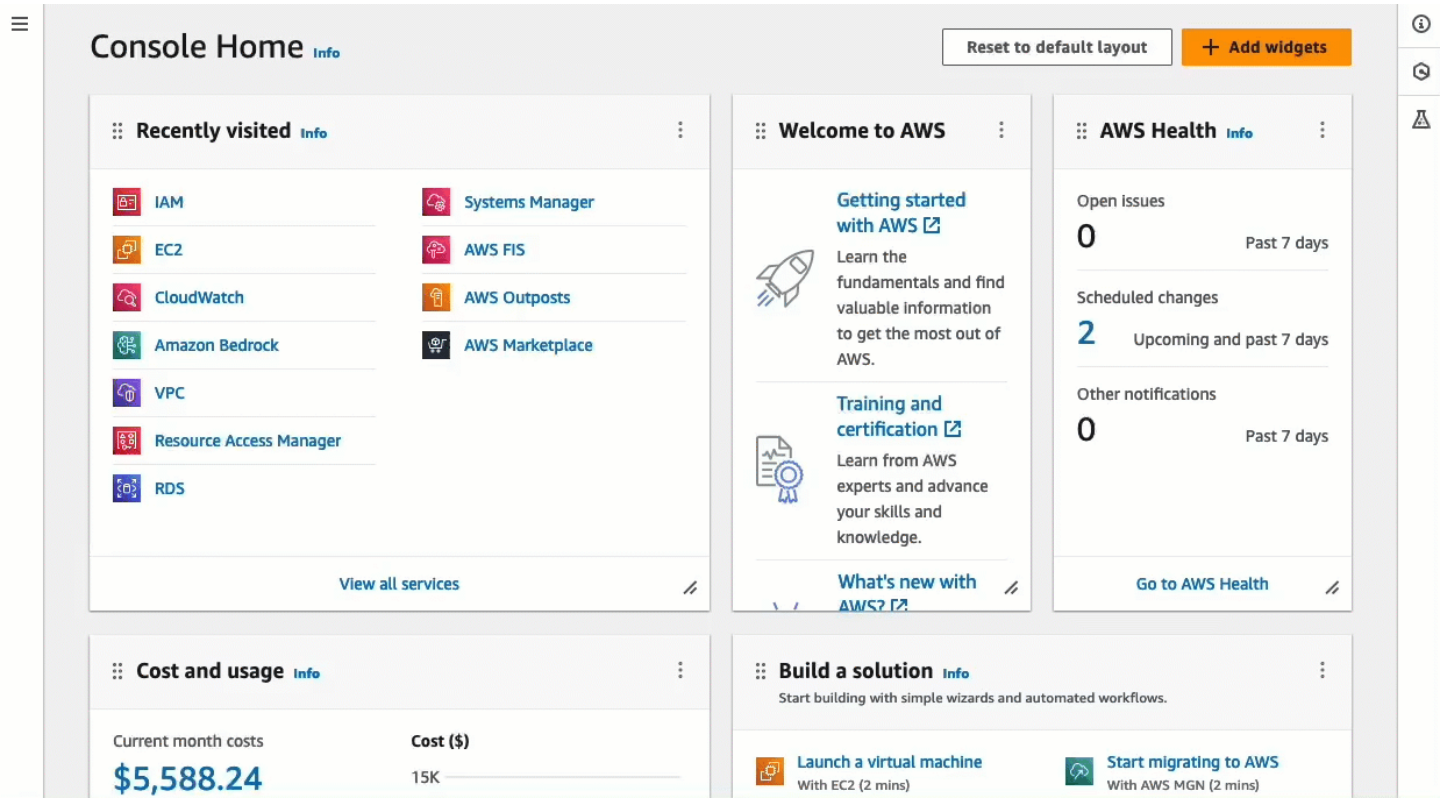
d. Em Entidades do IAM, marque a caixa de seleção ao lado da sua identidade (usuário, grupo de usuários ou perfil). É possível usar a caixa de pesquisa para filtrar a lista de identidades.

e. Escolha Anexar política.

Visualizar uma animação: criar uma política do IAM



Visualizar uma animação: anexar uma política do IAM



Tarefa 2: criar um grupo de segurança que permita o tráfego do EC2 Instance Connect para sua instância

Quando você usa o EC2 Instance Connect no console do Amazon EC2 para se conectar a uma instância, o tráfego que deve ser permitido para chegar à instância é o tráfego do serviço do EC2 Instance Connect. Isso é diferente de se conectar do seu computador local a uma instância; nesse caso, você deverá permitir o tráfego do seu computador local para sua instância. Para permitir o tráfego do EC2 Instance Connect, é necessário criar um grupo de segurança que permita tráfego SSH de entrada da faixa de endereços IP para o serviço do EC2 Instance Connect.

Os intervalos de endereços IP dos serviços da AWS estão disponíveis em https://ip-ranges.amazonaws.com/ip-ranges.json. Os intervalos de endereços IP do EC2 Instance Connect são identificados por `"service": "EC2_INSTANCE_CONNECT"`.

Objetivo da tarefa

Nessa tarefa, primeiro você encontrará o intervalo de endereços IP para `EC2_INSTANCE_CONNECT` na Região da AWS em que sua instância está localizada. Em seguida, você criará um grupo de segurança que permita na porta 22 tráfego SSH de entrada proveniente desse intervalo de endereços IP.

Etapas para criar os grupos de segurança

Use as etapas a seguir para criar um grupo de faturamento. Para visualizar uma animação das etapas, consulte Visualizar uma animação: obtenha o intervalo de endereços IP do EC2 Instance Connect para uma região específica e Visualizar uma animação: configurar um grupo de segurança.

Para criar um grupo de segurança que permita tráfego de entrada do serviço do EC2 Instance Connect para sua instância

1. Primeiro, obtenha o intervalo de endereços IP para o serviço do EC2 Instance Connect

   a. Abra o arquivo JSON dos intervalos de endereços IP da AWS em https://ip-ranges.amazonaws.com/ip-ranges.json.

   b. Escolha Dados brutos.

   c. Encontre o intervalo de endereços IP para `EC2_INSTANCE_CONNECT` para a Região da AWS em que sua instância está localizada. Você pode usar o campo de pesquisa do navegador para pesquisar o serviço `EC2_INSTANCE_CONNECT` e continuar pesquisando até encontrar a região na qual sua instância está localizada.

      Por exemplo, se sua instância estiver localizada na região Leste dos EUA (Norte da Virgínia) (`us-east-1`), o intervalo de endereços IP para `EC2_INSTANCE_CONNECT` nessa região será `18.206.107.24/29`.

      > **Note**
      >
      > Os intervalos de endereços IP são diferentes para cada Região da AWS.

   d. Copie o intervalo de endereços IP que aparece ao lado de `ip_prefix`. Você usará esse intervalo de endereços IP posteriormente neste procedimento.

   Para obter mais informações sobre como baixar o arquivo JSON de intervalos de endereços IP da AWS e filtrar por serviço, consulte Intervalos de endereços IP da AWS no Guia do usuário da Amazon VPC.

2. Em seguida, crie o grupo de segurança com uma regra de entrada para permitir o tráfego do intervalo de endereços IP copiados

   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

   b. No painel de navegação, selecione Grupos de segurança.

c. Escolha Create grupo de segurança (Criar grupo de segurança).

d. Em Basic details (Detalhes básicos), faça o seguinte:

   i. Em Nome do grupo de segurança, insira um nome que faça sentido para o grupo de segurança.

   ii. Em Descrição, insira uma descrição para o grupo de segurança.

e. Em Regras de entrada, faça o seguinte:

   i. Escolha Adicionar regra.

   ii. Para Tipo, escolha SSH.

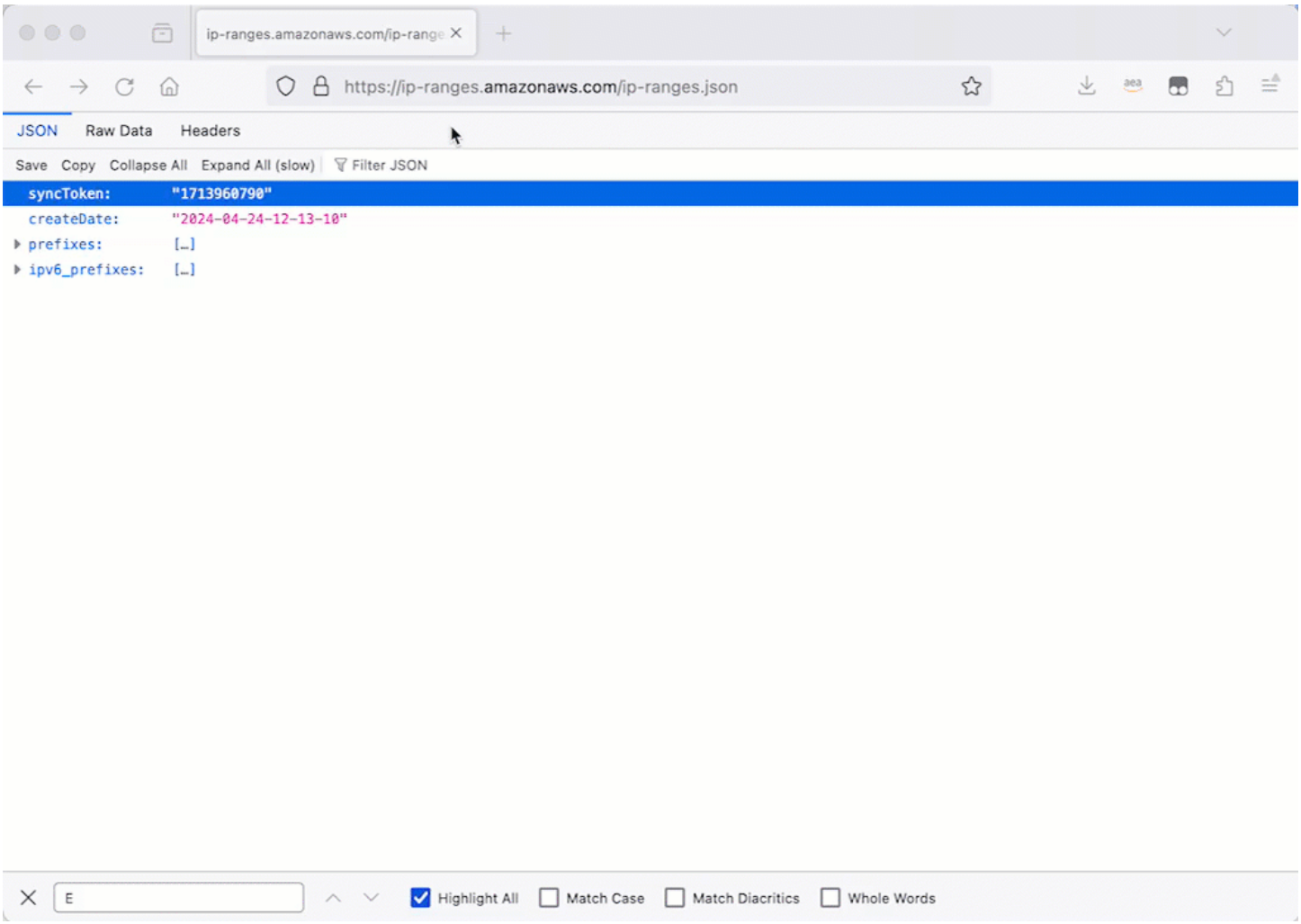
   iii. Em Origem, mantenha a opção Personalizada.

   iv. No campo ao lado de Origem, cole o intervalo de endereços IP do serviço EC2 Instance Connect que você copiou anteriormente neste procedimento.

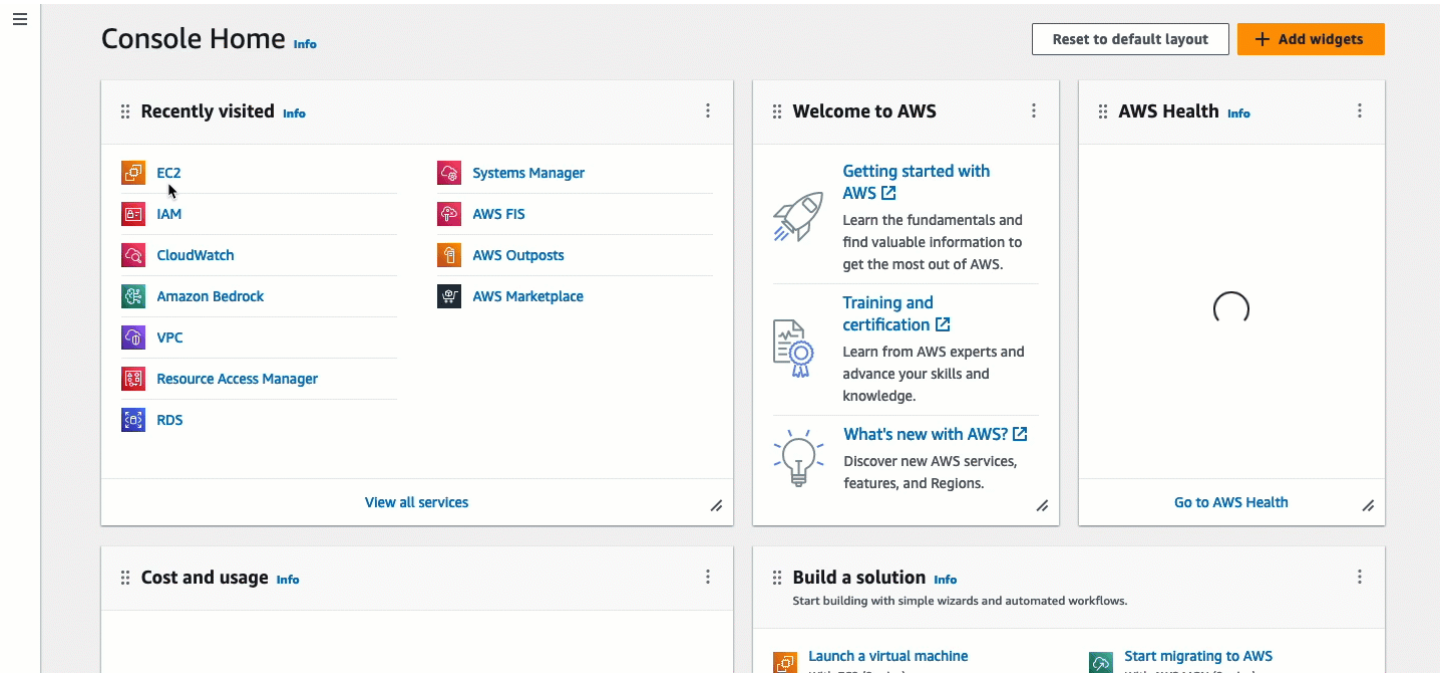
   Por exemplo, se sua instância estiver localizada na região Leste dos EUA (Norte da Virgínia) (`us-east-1`), cole o seguinte intervalo de endereços IP no campo: `18.206.107.24/29`

f. Escolha Create security group (Criar grupo de segurança).

Visualizar uma animação: obtenha o intervalo de endereços IP do EC2 Instance Connect para uma região específica



Visualizar uma animação: configurar um grupo de segurança



Tarefa 3: iniciar sua instância

Ao iniciar uma instância, especifique uma AMI que contenha as informações necessárias para iniciá-la. É possível optar por iniciar uma instância com ou sem o EC2 Instance Connect pré-instalado. Nessa tarefa, especificamos uma AMI que é fornecida pré-instalada com o EC2 Instance Connect.

Se você iniciar sua instância sem o EC2 Instance Connect pré-instalado e quiser usar o EC2 Instance Connect para se conectar à sua instância, precisará executar etapas adicionais de configuração. Essas etapas estão fora do escopo deste tutorial.

Objetivo da tarefa

Nessa tarefa, você iniciará uma instância com a AMI do Amazon Linux 2023, a qual é fornecida pré-instalada com o EC2 Instance Connect. Você também especificará o grupo de segurança que criou anteriormente para poder usar o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância. Como você usará o EC2 Instance Connect para se conectar à sua instância, que envia uma chave pública aos metadados da sua instância, não será necessário especificar uma chave SSH ao executar sua instância. No entanto, é preciso garantir que sua instância tenha um endereço IPv4 público, pois o uso do EC2 Instance Connect no console do Amazon EC2 permite a conexão somente com instâncias com endereços IPv4 públicos.

Etapas para iniciar sua instância

Use as etapas a seguir para iniciar sua instância. Para visualizar uma animação dessas etapas, consulte Visualizar uma animação: iniciar sua instância.

Para iniciar uma instância que pode usar o EC2 Instance Connect no console do Amazon EC2 para conexão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, a região da AWS atual será exibida (por exemplo, Irlanda). Selecione uma região na qual a instância será iniciada. Essa escolha é importante porque você criou um grupo de segurança que permite tráfego para uma região específica. Por isso, é necessário selecionar a mesma região na qual a instância será executada.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.
5. Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Início rápido. O Amazon Linux é selecionado por padrão. Em Imagem de máquina da Amazon (AMI), a opção AMI do Amazon Linux 2023 é selecionada por padrão. Mantenha a seleção padrão para essa tarefa.
6. Em Tipo de instância, para Tipo de instância, mantenha a seleção padrão ou escolha um tipo de instância diferente.
7. Em Par de chaves (login), em Nome do par de chaves, escolha Continuar sem um par de chaves (não recomendado). Quando você usa o EC2 Instance Connect para se conectar a uma instância, o EC2 Instance Connect envia um par de chaves para os metadados da instância, e é esse par de chaves que é usado para a conexão.
8. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Atribuir IP público automaticamente, mantenha a opçaõ Habilitar.

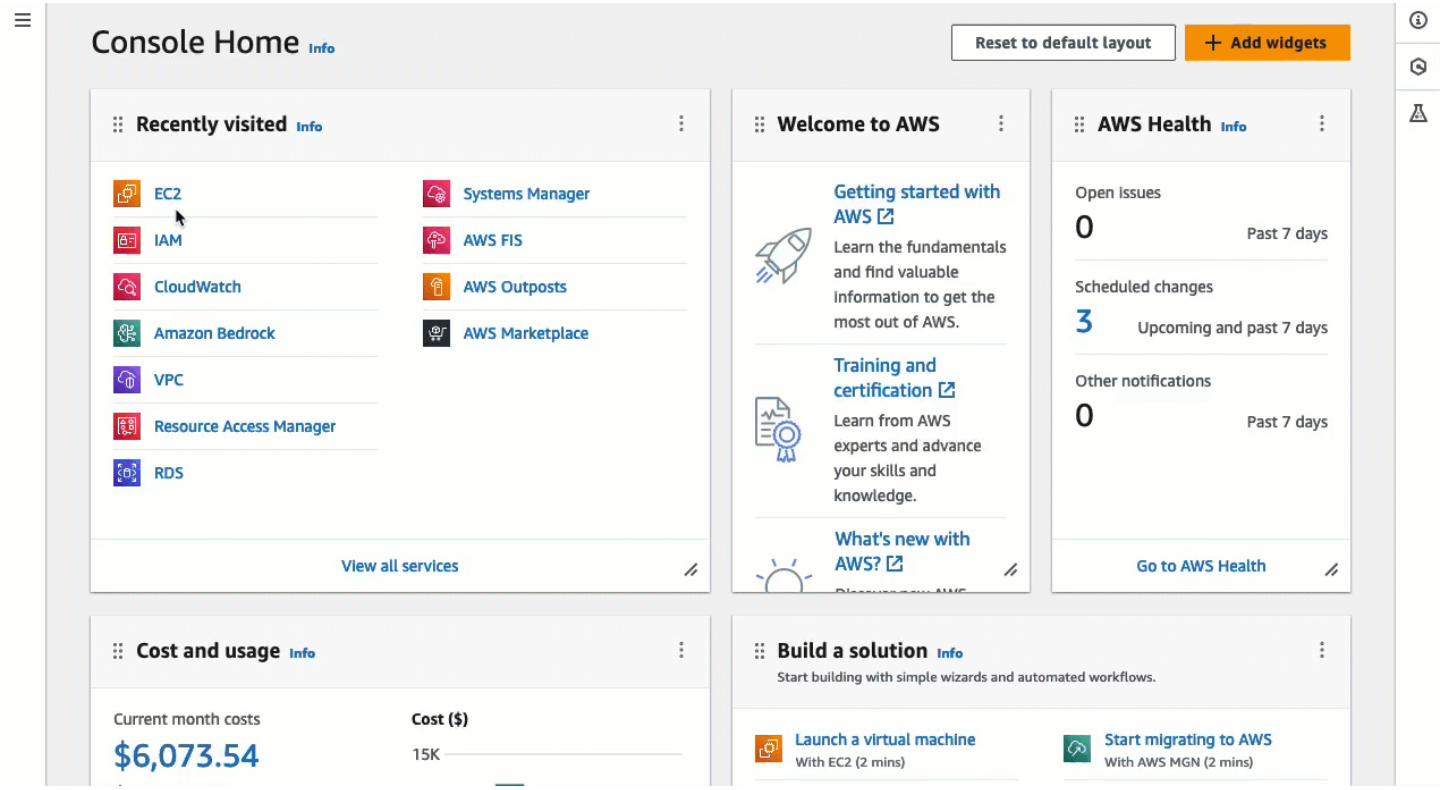
      > **Note**
      >
      > Para usar o EC2 Instance Connect no console do Amazon EC2 para conectar a uma instância, a instância deverá ter um endereço IPv4 público.

   b. Em Firewall (grupos de segurança), escolha Selecionar grupo de segurança existente.

   c. Em Grupos de segurança comuns, escolha o grupo de segurança criado anteriormente.

9. No painel Resumo painel, escolha Iniciar instância.

Visualizar uma animação: iniciar sua instância



Tarefa 4: conectar à sua instância

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. O daemon SSH usa `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` para procurar a chave pública nos metadados da instância para autenticação e conectar você à instância.

Objetivo da tarefa

Nessa tarefa, você se conectará à sua instância usando o EC2 Instance Connect no console do Amazon EC2. Se você concluiu os pré-requisitos das Tarefas 1, 2 e 3, a conexão deverá ser bem-sucedida.

Etapas para se conectar à sua instância

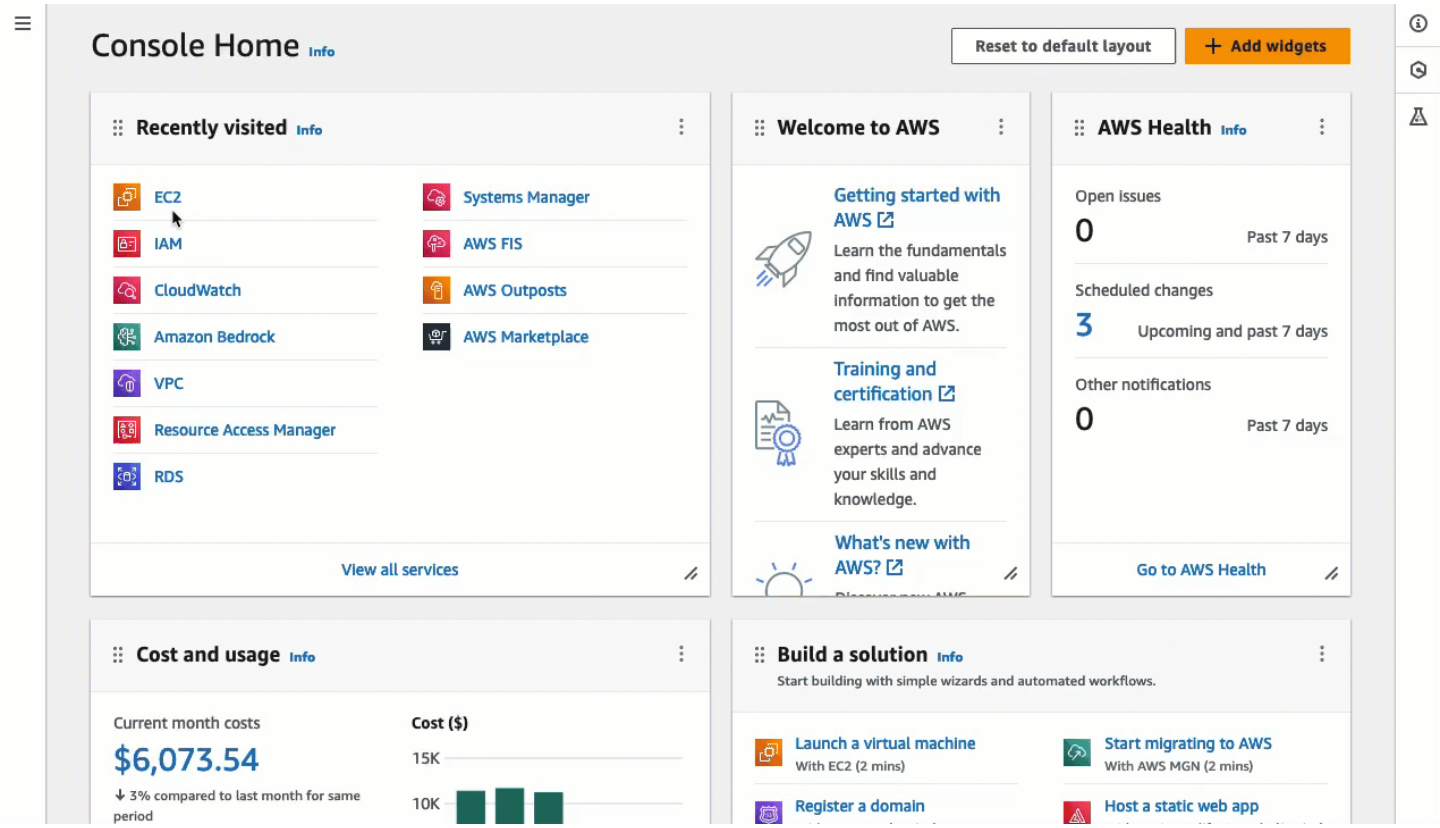
Use as etapas a seguir para se conectar à sua instância. Para visualizar uma animação dessas etapas, consulte Visualizar uma animação: conectar à sua instância.

Para conectar uma instância usando o EC2 Instance Connect no console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, a região da AWS atual será exibida (por exemplo, Irlanda). Selecione a região na qual a instância está localizada.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância e escolha Conectar.
5. Escolha a guia EC2 Instance Connect.
6. Em Tipo de conexão, escolha Conectar usando o EC2 Instance Connect.
7. Selecione Conectar.

   Uma janela de terminal abrirá no navegador e você estará conectado à sua instância.

Visualizar uma animação: conectar à sua instância



Pré-requisitos

Os seguintes pré-requisitos para instalar o EC2 Instance Connect e usar o EC2 Instance Connect para se conectar a uma instância são aplicáveis:

- Regiões da AWS
- Zonas Locais
- AMIs
- Instalação do EC2 Instance Connect
- Endereço IPv4
- Acesso à rede
- Regra do grupo de segurança
- Conceder permissões
- Configurações do computador local
- Nome de usuário

Regiões da AWS

Compatível em todas as Regiões da AWS, exceto Oeste do Canadá (Calgary).

Zonas Locais

Sem suporte.

AMIs

O EC2 Instance Connect é fornecido pré-instalado nas seguintes AMIs:

- AL2023
- Amazon Linux 2 2.0.20190618 ou posterior
- macOS Sonoma 14.2.1 ou posterior
- macOS Ventura 13.6.3 ou posterior
- macOS Monterey 12.7.2 ou posterior
- Ubuntu 20.04 ou posterior

O EC2 Instance Connect não é pré-instalado nas AMIs a seguir, mas você pode instalá-lo nas instâncias que são iniciadas usando as seguintes AMIs:

- Amazon Linux 2 anterior à versão 2.0.20190618
- CentOS Stream 8 e 9

- macOS Sonoma anterior à versão 14.2.1, Ventura anterior à versão 13.6.3 e Monterey anterior à versão 12.7.2
- Red Hat Enterprise Linux (RHEL) 8 e 9
- Ubuntu 16.04 ou 18.04

Instalação do EC2 Instance Connect

Para usar o EC2 Instance Connect para se conectar a uma instância, a instância deve ter o EC2 Instance Connect instalado. É possível iniciar a instância usando uma AMI que é fornecida pré-instalada com o EC2 Instance Connect ou instalar o EC2 Instance Connect em instâncias que são iniciadas com AMIs compatíveis. Para ver as AMIs compatíveis, consulte a seção anterior. Para obter as instruções de instalação, consulte Instalar o EC2 Instance Connect nas suas instâncias do EC2.

Endereço IPv4

A instância deve ter um endereço IPv4 (privado ou público). O EC2 Instance Connect não oferece suporte à conexão usando um endereço IPv6.

Acesso à rede

As instâncias podem ser configuradas para permitir que os usuários conectem-se à sua instância pela Internet ou por meio do endereço IP privado da instância. Dependendo de como seus usuários forem conectar-se à sua instância usando o EC2 Instance Connect, será necessário configurar o seguinte acesso à rede:

- Caso seus usuários forem conectar-se à sua instância pela Internet, ela deverá ter um endereço IP público e estar em uma sub-rede pública. Para obter mais informações, consulte Habilitar o acesso à Internet no Manual do usuário da Amazon VPC.
- Caso seus usuários forem conectar-se à sua instância por meio do endereço IP privado da instância, você deverá estabelecer uma conectividade de rede privada com sua VPC por meio do AWS Direct Connect, do AWS Site-to-Site VPN ou do emparelhamento da VPC, para que os usuários possam acessar o endereço IP privado da instância.

Se sua instância não tiver um endereço IPv4 público e você preferir não configurar o acesso à rede conforme descrito acima, considere o EC2 Instance Connect Endpoint como uma alternativa ao EC2 Instance Connect. O EC2 Instance Connect Endpoint permite que você conecte-se a uma instância via SSH ou RDP sem exigir que a instância tenha um endereço IPv4 público. Para ter mais informações, consulte Conectar-se à sua instância do Linux usando o console do Amazon EC2.

Regra do grupo de segurança

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada na porta 22 a partir do seu endereço IP ou da rede. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de inicialização de instâncias permite o tráfego SSH de entrada por padrão. Para ter mais informações, consulte Regras para se conectar a instâncias pelo computador.

O EC2 Instance Connect usa intervalos de endereços IP específicos para conexões de SSH baseadas em navegador com sua instância (quando os usuários usam o console do Amazon EC2 para se conectar a uma instância). Caso os usuários utilizem o console do Amazon EC2 para se conectar a uma instância, certifique-se de que o grupo de segurança associado à sua instância permita tráfego de SSH de entrada da faixa de endereços IP para `EC2_INSTANCE_CONNECT`. Para identificar o intervalo de endereços, faça download do arquivo JSON fornecido pela AWS e filtre para o subconjunto do EC2 Instance Connect, usando `EC2_INSTANCE_CONNECT` como valor do serviço. Esses intervalos de endereços IP diferem entre Regiões da AWS. Para obter mais informações sobre como baixar o arquivo JSON e filtrar por serviço, consulte Intervalos de endereços IP da AWS no Guia do usuário da Amazon VPC.

Conceder permissões

Você deve conceder as permissões necessárias a cada usuário do IAM que usará o EC2 Instance Connect para se conectar a uma instância. Para ter mais informações, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Configurações do computador local

Caso os usuários utilizem SSH para se conectar, eles devem garantir que o computador local tenha um cliente SSH.

É muito provável que o computador local do usuário tenha um cliente SSH instalado por padrão. É possível verificar se existe um cliente SSH digitando ssh na linha de comando. Se o computador local não reconhecer o comando, será preciso instalar um cliente SSH. Para obter informações sobre como instalar um cliente SSH no Linux ou macOS X, consulte http://www.openssh.com. Para obter informações sobre como instalar um cliente SSH no Windows 10, consulte OpenSSH no Windows.

Não haverá necessidade de instalar o cliente SSH no computador local se os usuários só usarem o console do Amazon EC2 para se conectar a uma instância.

Nome de usuário

Ao usar o EC2 Instance Connect para se conectar a uma instância, o nome de usuário deve atender aos seguintes pré-requisitos:

- Primeiro caractere: deve ser uma letra (`A-Z` ou `a-z`), um dígito (`0-9`) ou um sublinhado (`_`)
- Caracteres subsequentes: podem ser letras (`A-Z`, `a-z`), dígitos (`0-9`) ou os seguintes caracteres: `@ . _ -`
- Tamanho mínimo: 1 caractere
- Tamanho máximo: 31 caracteres

Conceder permissões do IAM para o EC2 Instance Connect

Para se conectar a uma instância usando o EC2 Instance Connect, é necessário criar uma política do IAM que conceda permissões aos usuários para as ações e condições a seguir:

- Ação `ec2-instance-connect:SendSSHPublicKey`: concede permissão para enviar por push a chave pública a uma instância.
- Condição `ec2:osuser`: especifica o nome do usuário do sistema operacional que pode enviar por push a chave pública a uma instância. Use o nome de usuário padrão da AMI que você usou para iniciar a instância. O nome de usuário padrão para o AL2023 e o Amazon Linux 2 é `ec2-user` e, para o Ubuntu, é `ubuntu`.
- Ação `ec2:DescribeInstances`: exigida ao usar o console do EC2, pois o wrapper chama essa ação. Os usuários talvez já tenham permissão para chamar essa ação a partir de outra política.

Considere restringir o acesso a instâncias do EC2 específicas. Caso contrário, todas as entidades principais do IAM com permissão para ação `ec2-instance-connect:SendSSHPublicKey` poderão conectar a todas as instâncias do EC2. É possível restringir o acesso especificando ARNs de recursos ou usando tags de recurso como chaves de condição.

Para obter mais informações, consulte Ações, recursos e chaves de condição para o Amazon EC2 Instance Connect.

Para obter informações sobre a criação de políticas do IAM, consulte Criação de políticas do IAM, no Manual do usuário do IAM.

Permitir que os usuários conectem-se a instâncias específicas

A política do IAM a seguir concede permissão para se conectar a instâncias específicas, identificadas por seus ARNs de recursos.

No exemplo de política do IAM a seguir, as ações e condições abaixo são especificadas:

- A ação `ec2-instance-connect:SendSSHPublicKey` concede aos usuários permissão para se conectar a duas instâncias, especificadas pelos ARNs do recurso. Para conceder aos usuários permissão para se conectar a todas as instâncias do EC2, substitua os ARNs do recurso pelo curinga `*`.
- A condição `ec2:osuser` concede permissão para se conectar às instâncias somente se o nome do *`ami-user`* for especificado durante a conexão.
- A ação `ec2:DescribeInstances` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias. Caso seus usuários utilizem somente um cliente SSH para se conectar às suas instâncias, é possível omitir `ec2:DescribeInstances`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": [
    "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
    "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
   ],
   "Condition": {
    "StringEquals": {
     "ec2:osuser": "ami-username"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
```

```
}
```

Permitir que os usuários conectem-se a instâncias com tags específicas

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões de acordo com tags que podem ser anexadas a usuários e a recursos da AWS. É possível usar tags de recurso para controlar o acesso a uma instância. Para obter mais informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte Controle do acesso aos recursos da AWS no Guia do usuário do IAM.

No exemplo de política do IAM a seguir, a ação `ec2-instance-connect:SendSSHPublicKey` concede aos usuários permissão para se conectar a qualquer instância (indicada pelo curinga `*` no ARN do recurso), desde que a instância tenha uma tag de recurso com key=`tag-key` e value=`tag-value`.

A ação `ec2:DescribeInstances` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias. Caso seus usuários utilizem somente um cliente SSH para se conectar às suas instâncias, é possível omitir `ec2:DescribeInstances`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": "arn:aws:ec2:region:account-id:instance/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/tag-key": "tag-value"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Instalar o EC2 Instance Connect nas suas instâncias do EC2

Para se conectar a uma instância usando o EC2 Instance Connect, a instância deve ter o EC2 Instance Connect instalado.

As seguintes AMIs são fornecidas pré-instaladas com o EC2 Instance Connect:

- AMI padrão do AL2023
- Amazon Linux 2 2.0.20190618 ou posterior
- macOS Sonoma 14.2.1 ou posterior
- macOS Ventura 13.6.3 ou posterior
- macOS Monterey 12.7.2 ou posterior
- Ubuntu 20.04 ou posterior

Se a instância foi iniciada usando uma das AMIs da lista anterior, essa tarefa poderá ser pulada.

> **Note**
>
> Se você definiu as configurações de `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` para a autenticação SSH, a instalação do EC2 Instance Connect não as atualizará. Consequentemente, não é possível usar o EC2 Instance Connect.

Pré-requisitos para a instalação EC2 Instance Connect

- Inicie a instância com uma das seguintes AMIs compatíveis:

  Amazon Linux 2 anterior à versão 2.0.20190618

  AMI mínima do AL2023 ou AMI otimizada para o Amazon ECS

  CentOS Stream 8 e 9

  macOS Sonoma anterior à versão 14.2.1, Ventura anterior à versão 13.6.3 e Monterey anterior à versão 12.7.2

  Red Hat Enterprise Linux (RHEL) 8 e 9

  Ubuntu 16.04 e 18.04

Se a instância tiver sido executada com uma versão posterior do Amazon Linux 2, macOS Sonoma, Ventura, Monterey ou do Ubuntu, ela virá com o EC2 Instance Connect pré-instalado e você poderá ignorar esse procedimento.

- Verifique os pré-requisitos gerais para o EC2 Instance Connect.

  Para ter mais informações, consulte Pré-requisitos.

- Verifique os pré-requisitos para se conectar à sua instância usando um cliente SSH em sua máquina local.

  Se sua máquina local for Linux ou macOS, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH.. Se sua máquina local for Windows, consulte Pré-requisitos.

  Para ter mais informações, consulte Pré-requisitos de conexão via SSH.

- Obtenha o ID da instância.

  É possível obter o ID da instância usando o console do Amazon EC2 (na coluna ID da instância). Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell).

- Instale um cliente SSH no computador local.

  É muito provável que seu computador local tenha um cliente SSH instalado por padrão. É possível verificar se existe um cliente SSH digitando ssh na linha de comando. Se o seu computador local não reconhecer o comando, será possível instalar um cliente SSH. Para obter informações sobre como instalar um cliente SSH no Linux ou macOS X, consulte http://www.openssh.com. Para obter informações sobre como instalar um cliente SSH no Windows 10, consulte OpenSSH no Windows.

- (Ubuntu) Instale a AWS CLI em sua instância.

  Para instalar o EC2 Instance Connect em uma instância do Ubuntu, use a AWS CLI na instância. Para obter informações sobre como instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Instalação do EC2 Instance Connect

Instalar o EC2 Instance Connect configura o daemon SSH na instância.

Use um dos procedimentos a seguir para instalar o EC2 Instance Connect, dependendo do sistema operacional da sua instância.

Amazon Linux 2

Para instalar o EC2 Instance Connect em uma instância aberta com Amazon Linux 2

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. Instale o pacote EC2 Instance Connect na sua instância.

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   Deverão estar visíveis três novos scripts na pasta `/opt/aws/bin/`:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

3. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

   ```
   [ec2-user ~]$ sudo less /etc/ssh/sshd_config
   ```

   O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância

- O `AuthorizedKeysCommandUser` define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

CentOS

Para instalar o EC2 Instance Connect em uma instância executada com o CentOS

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o CentOS, o nome de usuário padrão é `centos` ou `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. Se você usar um proxy HTTP ou HTTPS, defina o `http_proxy` ou as variáveis de ambiente `https_proxy` na sessão do shell atual.

   Se você não estiver usando um proxy, ignore esta etapa.

   - Para um servidor de proxy HTTP, execute os seguintes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Para um servidor de proxy HTTPS, execute os seguintes comandos:

     ```
     $ export http_proxy=https://hostname:port
     ```

```
$ export https_proxy=https://hostname:port
```

3. Instale o pacote do EC2 Instance Connect na sua instância executando os comandos a seguir.

   Os arquivos de configuração do EC2 Instance Connect para CentOS são fornecidos em um pacote do Red Hat Package Manager (RPM), com pacotes do RPM diferentes para CentOS 8 e CentOS 9 e para tipos de instância executados em Intel/AMD (x86_64) ou ARM (AArch64).

   Use o bloco de comando para a arquitetura do seu sistema operacional e de CPU.

   - CentOS 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM (AArch64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

   - CentOS 9

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

   - Para o CentOS 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
     ```

   - Para o CentOS 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- O `AuthorizedKeysCommandUser` define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

macOS

Para instalar o EC2 Instance Connect em uma instância executada com o macOS

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para instâncias macOS, o nome de usuário padrão é `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. Atualize o Homebrew usando o seguinte comando. A atualização listará o software que o Homebrew conhece. O pacote do EC2 Instance Connect é fornecido via Homebrew em instâncias do macOS. Para obter mais informações, consulte Atualizar o sistema operacional e o software em instâncias Mac.

```
[ec2-user ~]$ brew update
```

3. Instale o pacote EC2 Instance Connect na sua instância. Isso instalará o software e configurará o SSHD para usá-lo.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- O `AuthorizedKeysCommandUser` define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

RHEL

Para instalar o EC2 Instance Connect em uma instância executada com o Red Hat Enterprise Linux (RHEL)

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o RHEL, o nome de usuário padrão é `ec2-user` ou `root`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. Se você usar um proxy HTTP ou HTTPS, defina o `http_proxy` ou as variáveis de ambiente `https_proxy` na sessão do shell atual.

   Se você não estiver usando um proxy, ignore esta etapa.

   - Para um servidor de proxy HTTP, execute os seguintes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Para um servidor de proxy HTTPS, execute os seguintes comandos:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instale o pacote do EC2 Instance Connect na sua instância executando os comandos a seguir.

   Os arquivos de configuração do EC2 Instance Connect para RHEL são fornecidos em um pacote do Red Hat Package Manager (RPM), com pacotes do RPM diferentes para RHEL 8 e RHEL 9 e para tipos de instância executados em Intel/AMD (x86_64) ou ARM (AArch64).

   Use o bloco de comando para a arquitetura do seu sistema operacional e de CPU.

- RHEL 8

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
```

```
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

   - Para o RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
     connect.conf
     ```

   - Para o RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância

- O `AuthorizedKeysCommandUser` define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

Ubuntu

Para instalar o EC2 Instance Connect em uma instância aberta com Ubuntu 16.04 ou posterior

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância quando você a executou e use o nome de usuário padrão da AMI que você usou para iniciar sua instância. Para uma AMI Ubuntu, o nome de usuário é `ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. (Opcional) Garanta que sua instância tenha a AMI do Ubuntu mais recente.

   Execute os comandos a seguir para atualizar todos os pacotes na instância.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Instale o pacote EC2 Instance Connect na sua instância.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

Deverão estar visíveis três novos scripts na pasta `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Opcional) Verifique se o Instance Connect foi instalando com sucesso na sua instância.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- O `AuthorizedKeysCommandUser` define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

Para obter mais informações sobre o pacote do EC2 Instance Connect, consulte aws/aws-ec2-instance-connect-config no site do GitHub.

Conectar-se usando EC2 Instance Connect

As instruções a seguir explicam como se conectar à sua instância do Linux usando o EC2 Instance Connect.

Decida qual opção de conexão usar.A opção de conexão a ser usada depende de sua instância ter um endereço IPv4 público:

- Amazon EC2 console: para se conectar usando o console do Amazon EC2, a instância deve ter um endereço IPv4 público.
- Cliente SSH: se a instância não tiver um endereço IP público, será possível conectar-se à instância através de uma rede privada usando um cliente SSH. Por exemplo, é possível se conectar de dentro da mesma VPC ou por meio de uma conexão VPN, de um gateway de trânsito ou do AWS Direct Connect.

O EC2 Instance Connect não oferece suporte à conexão usando um endereço IPv6.

> **Tip**
>
> O EC2 Instance Connect é uma das opções para se conectar a instâncias do Linux. Para obter outras opções, consulte Conecte-se à sua instância do Linux. Para se conectar a uma instância do Windows, consulte Conectar-se à sua instância do Windows do .

Opções de conexão para o EC2 Instance Connect

- Conectar-se usando o console do Amazon EC2
- Conectar-se usando sua própria chave e cliente SSH
- Conectar-se usando o AWS CLI
- Solução de problemas

Conectar-se usando o console do Amazon EC2

É possível se conectar a uma instância usando o console do Amazon EC2 ao selecionar a instância no console e optar por se conectar usando o EC2 Instance Connect. O Instance Connect lida com as permissões e fornece uma conexão bem-sucedida.

Para se conectar usando o console do Amazon EC2, a instância deve ter um endereço IPv4 público. Antes de se conectar, certifique-se de revisar todos os pré-requisitos.

Como conectar-se à sua instância usando o cliente com base em navegador no console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar).
4. Escolha a guia EC2 Instance Connect.
5. Em Tipo de conexão, escolha Conectar usando o EC2 Instance Connect.
6. Em Nome de usuário, verifique o nome de usuário.
7. Escolha Conectar para abrir uma janela de terminal.

Conectar-se usando sua própria chave e cliente SSH

É possível usar sua própria chave SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do EC2 Instance Connect. Isso permite que você se beneficie da capacidade do Instance Connect de enviar por push uma chave pública para a instância. Esse método de conexão funciona para instâncias com endereços IP públicos e privados.

Requisitos

- Requisitos para pares de chaves
  - Tipos com suporte: RSA (OpenSSH e SSH2) e ED25519
  - Tamanhos com suporte: 2048 e 4096.
  - Para ter mais informações, consulte Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.
- Ao se conectar a uma instância que só tenha endereços IP privados, o computador local a partir do qual você está iniciando a sessão SSH deve ter conectividade com o endpoint do serviço EC2 Instance Connect (para enviar sua chave pública SSH para a instância), além de conectividade de rede para o endereço IP privado da instância para estabelecer a sessão SSH. O endpoint de serviço do EC2 Instance Connect é acessível pela Internet ou por meio de uma interface virtual pública do AWS Direct Connect. Para se conectar ao endereço IP privado da instância, é possível aproveitar serviços, como AWS Direct Connect, AWS Site-to-Site VPN ou emparelhamento de VPC.

Antes de se conectar, certifique-se de revisar todos os pré-requisitos.

Para se conectar à sua instância usando a própria chave e qualquer cliente SSH

1. (Opcional) Gerar chaves novas chaves SSH privadas e públicas

   É possível gerar novas chaves SSH públicas e privadas, `my_key` e `my_key.pub`, usando o comando a seguir:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Envie por push a chave pública do SSH para a instância

   Use o comando send-ssh-public-key para enviar por push a chave pública SSH para a instância. Se você executou sua instância usando o AL2023 ou o Amazon Linux 2, o nome de usuário padrão da AMI é `ec2-user`. Se você executou sua instância usando o Ubuntu, o nome de usuário padrão da AMI é `ubuntu`.

   O exemplo a seguir envia a chave pública para a instância especificada na zona de disponibilidade especificada, para autenticar `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Conecte-se à instância usando a chave privada

   Use o comando ssh para se conectar à instância usando a chave privada antes de a chave pública ser removida dos metadados da instância (você tem 60 segundos antes de ser removida). Especifique a chave privada que corresponde à chave pública, o nome de usuário padrão da AMI usado para iniciar sua instância e o nome DNS público da instância (se estiver se conectando por uma rede privada, especifique o nome DNS privado ou o endereço IP). Adicione a opção `IdentitiesOnly=yes` para garantir que apenas os arquivos na configuração ssh e a chave especificada sejam usados para a conexão.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Conectar-se usando o AWS CLI

Se você souber o ID da sua instância, poderá usar o comando ec2-instance-connect da AWS CLI para se conectar à sua instância usando um cliente SSH. Se você não especificar um tipo de conexão, o EC2 Instance Connect tentará conectar-se automaticamente ao endereço IPv4 público da sua instância. Se sua instância não tiver um endereço IPv4 público, o EC2 Instance Connect tentará conectar-se ao endereço IPv4 privado da sua instância por meio de um EC2 Instance Connect Endpoint. Se sua instância não tiver um endereço IPv4 privado ou se sua VPC não tiver um EC2 Instance Connect Endpoint, o EC2 Instance Connect tentará conectar-se ao endereço IPv6 da sua instância.

> **Important**
>
> Antes de se conectar com este método, certifique-se de ter configurado a AWS CLI, incluindo as credenciais que ela usa, e de estar usando a versão mais recente da AWS CLI. Para obter mais informações, consulte Instalação ou atualização da versão mais recente da AWS CLI e Configuração da AWS CLI no Guia do usuário da AWS Command Line Interface.

Tipos de conexão

`auto` (padrão)

A CLI tenta conectar-se usando os endereços IP da instância na seguinte ordem e com o tipo de conexão correspondente:

- IPv4 público: `direct`
- IPv4 privado: `eice`
- IPv6: `direct`

`direct`

A CLI tenta se conectar usando os endereços IP da instância na seguinte ordem (ela não se conecta por meio de um EC2 Instance Connect Endpoint):

- IPv4 público
- IPv6
- IPv4 privado

`eice`

A CLI sempre usa o endereço IPv4 privado da instância.

> **Note**
>
> No futuro, podemos mudar o comportamento do tipo de conexão `auto`. Para garantir que seu tipo de conexão desejado seja usado, recomendamos que você defina explicitamente `--connection-type` como `direct` ou `eice`.

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. A política do IAM anexada ao usuário autoriza o usuário a enviar por push a chave pública para os metadados da instância.

Para se conectar a uma instância usando o ID da instância

Se souber apenas o ID da instância e quiser permitir que o EC2 Instance Connect determine o tipo de conexão a ser usado ao se conectar à sua instância, use o comando da CLI ec2-instance-connect e especifique o parâmetro `ssh` e o ID da instância.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

> **Tip**
>
> Se receber um erro ao usar esse comando, verifique se está usando o AWS CLI versão 2. O parâmetro `ssh` apenas está disponível para o AWS CLI versão 2. Para obter mais informações, consulte Sobre o AWS CLI versão 2, no Guia do usuário do AWS Command Line Interface.

Para se conectar a uma instância usando o ID da instância e um EC2 Instance Connect Endpoint

Se você quiser conectar-se à sua instância por meio de um EC2 Instance Connect Endpoint, use o comando anterior e também especifique o parâmetro `--connection-type` com o valor `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Para se conectar a uma instância usando o ID da instância e seu próprio arquivo de chave privada

Se você quiser conectar-se à sua instância por meio de um EC2 Instance Connect Endpoint usando sua própria chave privada, especifique o ID da instância e o caminho para o arquivo da chave

privada. Não inclua *file://* no caminho. O exemplo a seguir falhará: *file: ///caminho/para/a/chave*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /path/to/key.pem
```

Solução de problemas

Se você receber um erro ao tentar se conectar à instância, consulte:

- Solução de problemas de conexão com a instância do Linux
- Como solucionar problemas de conexão à minha instância do EC2 usando o EC2 Instance Connect?

Desinstalar o EC2 Instance Connect

Para desabilitar o EC2 Instance Connect, conecte-se à sua instância e desinstale o pacote `ec2-instance-connect` que está instalado no SO. Se a configuração `sshd` corresponder ao que foi definido quando você instalou o EC2 Instance Connect, desinstalar o pacote `ec2-instance-connect` também removerá a configuração `sshd`. Se a configuração `sshd` tiver sido modificada após a instalação do EC2 Instance Connect, você deverá atualizá-la manualmente.

Amazon Linux

É possível desinstalar o EC2 Instance Connect no AL2023 e no Amazon Linux 2 2.0.20190618 ou posterior, em que o EC2 Instance Connect está pré-configurado.

Para desinstalar o EC2 Instance Connect em uma instância executada com o Amazon Linux 2

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH que você usou para sua instância ao executá-la e o nome de usuário padrão da AMI AL2023 ou Amazon Linux 2, que é `ec2-user`.

   Por exemplo. o comando ssh conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
   ```

2. Desinstale o pacote `ec2-instance-connect` usando o comando yum.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

Como desinstalar o EC2 Instance Connect em uma instância executada com uma AMI do Ubuntu

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH usado para sua instância ao iniciá-la e o nome de usuário padrão da AMI Ubuntu, que é `ubuntu`.

   Por exemplo. o comando ssh conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Desinstale o pacote `ec2-instance-connect` usando o comando apt-get.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

Conectar-se à sua instância do Windows do

É possível se conectar às instâncias do Amazon EC2 criadas da maioria das imagens de máquina da Amazon (AMIs) no Windows usando a Área de Trabalho Remota. O Remote Desktop usa o Remote Desktop Protocol (RDP) para se conectar e usar sua instância da mesma forma que você usa um computador que esteja na sua frente (computador local). Ele está disponível na maioria das edições do Windows e também para Mac OS.

A licença do sistema operacional (SO) Windows Server permite duas conexões remotas simultâneas para fins administrativos. A licença para Windows Server está incluída no preço da sua instância do Windows. Caso precise de mais de duas conexões remotas simultâneas, você deverá adquirir uma licença do Remote Desktop Services (RDS). Se você tentar uma terceira conexão, ocorrerá um erro.

> **Tip**
>
> Se precisar se conectar à instância para solucionar problemas de inicialização, configuração de rede e outros problemas para instâncias criadas no AWS Nitro System, use o Console de Série do EC2 para as instâncias do Amazon EC2.

Conteúdo

- Conexão com a instância do Windows usando um cliente RDP
- Conectar a uma instância do Windows usando o Fleet Manager
- Configurar suas contas
- Transferir arquivos para instâncias do Windows

Conexão com a instância do Windows usando um cliente RDP

A seção apresentada a seguir detalha os pré-requisitos e o processo para realizar a conexão com a instância usando o endereço IPv4 ou IPv6 com um cliente RDP.

Pré-requisitos

É necessário atender aos pré-requisitos apresentados a seguir para se conectar à instância do Windows usando um cliente RDP.

- Instalação de um cliente RDP
  - (Windows) O Windows inclui um cliente RDP por padrão. Para verificar, digite mstsc em uma janela de Prompt de Comando. Se o computador não reconhecer esse comando, consulte a página inicial do Windows e pesquise pelo download da aplicação do Desktop Remoto da Microsoft.
  - (macOS X) Faça o download da aplicação Microsoft Remote Desktop usando a Mac App Store.
  - (Linux) Use o Remmina.
- Encontrar a chave privada

  Obtenha o caminho totalmente qualificado para o local em seu computador do arquivo `.pem` para o par de chaves que você especificou quando executou a instância. Para ter mais informações, consulte the section called “Identifique a chave pública que foi especificada na inicialização”.

  Se você não conseguir encontrar seu arquivo de chave privada, consulte

Quando você se conecta a uma instância do Windows recém-iniciada, você descriptografa a senha da conta do administrador usando a chave privada para o par de chaves que você especificou quando iniciou a instância.

Se você perder a senha do Administrador e não tiver mais a chave privada, é preciso redefinir a senha ou criar uma nova instância. Para ter mais informações, consulte Redefinir uma senha de administrador do Windows perdida ou expirada. Para conhecer as etapas e redefinir a senha usando um documento do Systems Manager, consulte Redefinir senhas e chaves SSH nas instâncias do EC2 no Manual do usuário do AWS Systems Manager.

.

- Permitir tráfego RDP de entrada do endereço IP à instância

  Verifique se o grupo de segurança associado à instância permite tráfego RDP de entrada (`port 3389`) do endereço IP. O grupo de segurança padrão não permite o tráfego RDP de entrada. Para ter mais informações, consulte Regras para se conectar a instâncias pelo computador.

> **Tip**
>
> É possível criar um EC2 Instance Connect Endpoint para se conectar à instância do Windows usando o RDP sem a necessidade de usar um endereço IPv4 público.

Conexão com uma instância do Windows usando RDP e o endereço IPv4

Para se conectar a uma instância do Windows, é necessário recuperar a senha do administrador e usar essa senha ao se conectar à sua instância usando o desktop remoto. Após a execução da instância, leva alguns minutos para que a senha fique disponível.

O nome de usuário padrão correspondente à conta de administrador depende do idioma do sistema operacional (SO) contido na AMI. Para verificar o nome de usuário correto, identifique o idioma do sistema operacional da sua AMI e escolha o nome de usuário correspondente. Por exemplo, para um sistema operacional em inglês, o nome de usuário será `Administrator`, para um sistema operacional francês, será `Administrateur` e para um sistema operacional português, será `Administrador`. Se uma versão de idioma do sistema operacional não tiver um nome de usuário no mesmo idioma, escolha o nome de usuário `Administrator (Other)`. Para obter mais informações, consulte Localized Names for Administrator Account in Windows (Nomes localizados da conta de administrador no Windows) no Microsoft TechNet Wiki.

Se você associou sua instância a um domínio, poderá se conectar a sua instância usando credenciais de domínio definidas no AWS Directory Service. Na tela de login do Desktop Remoto, em vez de usar o nome do computador local e a senha gerada, use o nome de usuário totalmente qualificado para o administrador (por exemplo, **`corp.example.com\Admin`**) e a senha dessa conta.

Se você receber um erro ao tentar se conectar à instância, consulte the section called “O Remote Desktop não pode se conectar ao computador remoto”.

Para se conectar à sua instância do Windows usando um cliente RDP

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.
4. Na página Conectar à instância, escolha a guia Cliente RDP.
5. Em Nome de usuário, escolha o nome de usuário padrão para a conta do administrador. O nome de usuário escolhido deverá corresponder ao idioma do sistema operacional (SO) contido na AMI que você usou para executar a instância. Se não houver um nome de usuário no mesmo idioma do seu sistema operacional, escolha Administrador (Outro).
6. Escolha Obter senha.
7. Na página Obter senha do Windows, faça o seguinte:

   a. Escolha Fazer upload de arquivo de chave privada e localize o arquivo de chave privada (`.pem`) que especificou ao executar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.

   b. Escolha Descriptografar senha. A página Obter senha do Windows será fechada e a senha padrão do administrador para a instância será exibida em Senha, substituindo o link Obter senha exibido anteriormente.

   c. Copie e salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.
8. Escolha Download remote desktop file (Fazer download de arquivo do desktop remoto). Quando terminar o download do arquivo, escolha Cancel (Cancelar) para retornar à página Instances (Instâncias). Navegue até o diretório de downloads e abra o arquivo do RDP.
9. Você pode receber um aviso de que o editor da conexão remota é desconhecido. Escolha Connect (Conectar) para se conectar à sua instância.

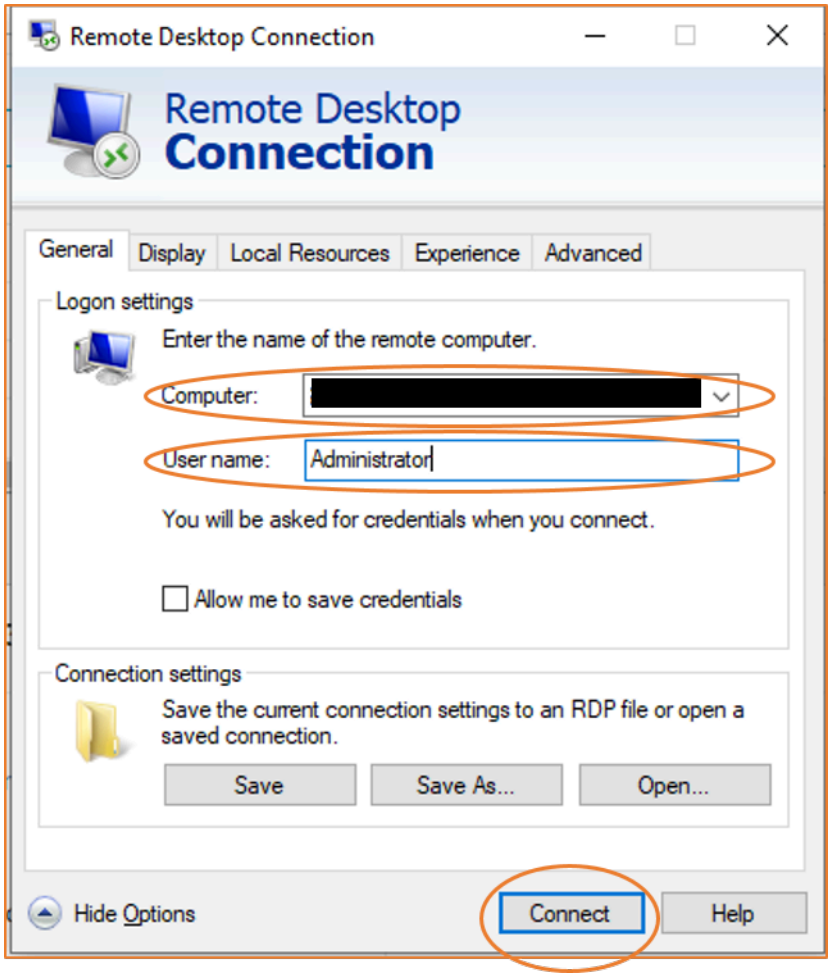
10. A conta de administrador é escolhida por padrão. Cole a senha que você copiou anteriormente e, em seguida, escolha OK.
11. Por causa da natureza de certificados autoassinados, talvez você receba um aviso indicando que não foi possível autenticar o certificado de segurança. Execute um destes procedimentos:
    - Se você confia no certificado, escolha Sim para realizar a conexão com a instância.
    - [Windows] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Visualizar certificado e, em seguida, escolha Impressão digital na guia Detalhes. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
    - [Mac OS X] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Mostrar certificado, expanda Detalhes e selecione Impressões digitais de SHA1. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.

Conexão com uma instância do Windows usando RDP e o endereço IPv6

Se você habilitou a VPC para IPv6 e atribuiu um endereço IPv6 à sua instância do Windows, poderá usar um cliente RDP para se conectar à sua instância usando seu endereço IPv6 (por exemplo, `2001:db8:1234:1a00:9691:9503:25ad:1761`) em vez de um endereço IPv4 público ou nome de host DNS público.

Para se conectar à sua instância do Windows usando seu endereço IPv6

1. Obtenha a senha inicial de administrador para sua instância, conforme descrito em Conexão com a instância do Windows usando um cliente RDP. Essa senha é necessária para se conectar à sua instância.
2. (Windows) Abra o cliente RDP em seu computador do Windows, escolha Mostrar opções e faça o seguinte:



- Em Computer (Computador), insira o endereço IPv6 da instância do Windows.
- Em User name (Nome do usuário), digite Administrator (Administrador).
- Selecione Conectar.
- Quando solicitado, digite a senha que você salvou anteriormente.

(macOS X) Abra o cliente RDP em seu computador e faça o seguinte:

- Escolha Novo.
- Em PC Name (Nome do PC), digite o endereço IPv6 da instância do Windows.
- Em User name (Nome do usuário), digite Administrator (Administrador).
- Feche a caixa de diálogo. Em My Desktops (Meus desktops), selecione a conexão e escolha Start (Iniciar).
- Quando solicitado, digite a senha que você salvou anteriormente.

3. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pôde ser autenticado. Se você confia no certificado, pode escolher Yes (Sim) ou Continue (Continuar). Caso contrário, é possível verificar a identidade do computador remoto, conforme descrito em Conexão com a instância do Windows usando um cliente RDP.

Conectar a uma instância do Windows usando o Fleet Manager

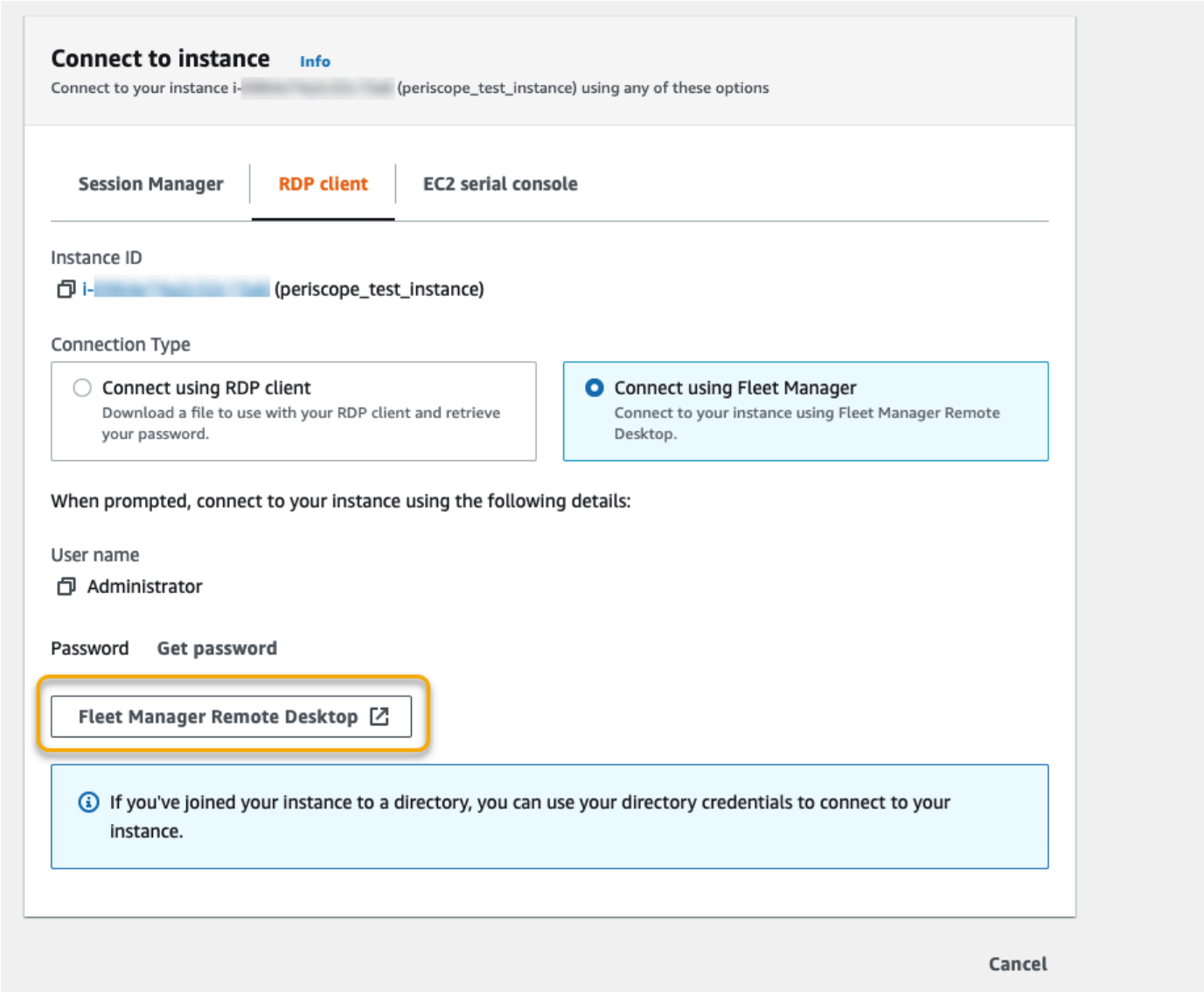
É possível usar o Fleet Manager, um recurso do AWS Systems Manager, para se conectar a instâncias do Windows usando o Remote Desktop Protocol (RDP) e exibir até quatro instâncias do Windows na mesma página no AWS Management Console. Você pode se conectar à primeira instância no Fleet Manager Remote Desktop diretamente da página Instâncias no console do Amazon EC2. Para obter mais informações sobre o Fleet Manager, consulte Conectar-se a um nó gerenciado usando o Remote Desktop no Guia do usuário doAWS Systems Manager.

Antes de tentar se conectar a uma instância usando o Fleet Manager, verifique se as etapas de configuração necessárias foram concluídas. Para obter mais informações, consulte Configurar o Fleet Manager.

> **Note**
>
> Não é necessário permitir especificamente o tráfego RDP de entrada do seu endereço IP se você usa o Fleet Manager para se conectar. O Fleet Manager trata disso para você.

Para se conectar a instâncias usando o RDP com o Fleet Manager (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.
4. Na página Connect to instance (Conectar a instância), escolha a opção Connect using Fleet Manager (Conectar usando o Fleet Manager) e, em seguida, escolha Fleet Manager Remote Desktop. Isso abre a página Fleet Manager Remote Desktop no console do AWS Systems Manager.



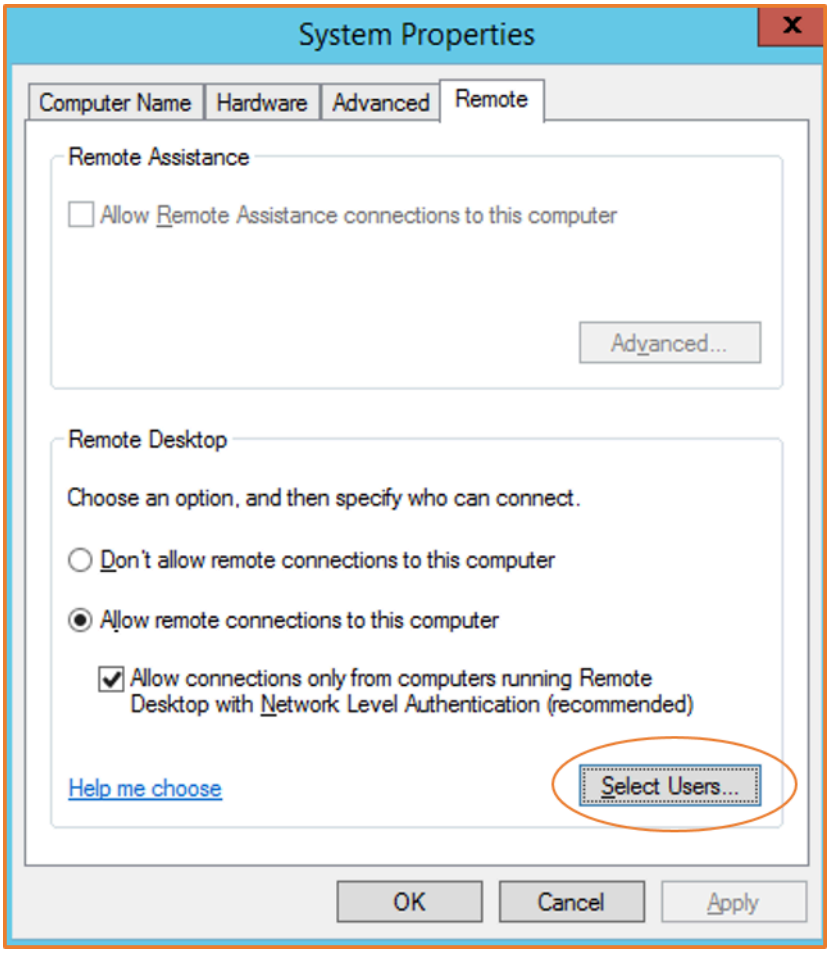
Para obter mais informações sobre como se conectar a instâncias do Windows via página Fleet Manager Remote Desktop, consulte Conectar via Remote Desktop no Guia do usuário doAWS Systems Manager.

Configurar suas contas

Após se conectar usando o RDP, recomendamos que você faça o seguinte:

- Altere a senha de administrador do valor padrão. É possível alterar a senha enquanto estiver conectado à instância, assim como faria em qualquer outro computador executando o Windows Server.

- Crie outro usuário com privilégios de administrador na instância. Essa é uma proteção no caso de você esquecer a senha de administrador ou ter um problema com a conta de administrador. O novo usuário deve ter permissão para acessar a instância remotamente. Abra System Properties (Propriedades do sistema clicando com o botão direito do mouse no ícone This PC (Este PC) no desktop do Windows ou no Explorador de Arquivos e selecione Properties (Propriedades). Escolha Remote settings (Configurações remotas) e escolha Select Users (Selecionar usuários) para adicionar o usuário ao grupo Remote Desktop Users (Usuários de Desktop Remoto).



Transferir arquivos para instâncias do Windows

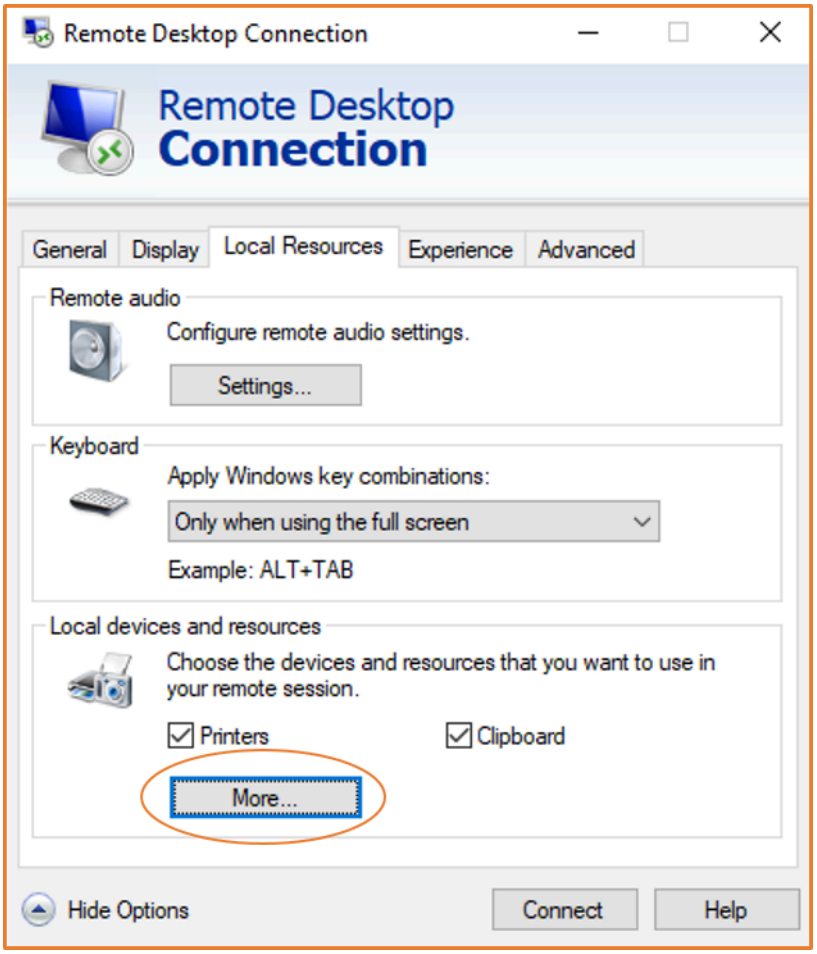
É possível trabalhar com sua instância Windows da mesma forma que trabalharia com qualquer servidor Windows. Por exemplo, é possível transferir arquivos entre uma instância do Windows e o computador local usando o recurso de compartilhamento de arquivos local do software Microsoft Remote Desktop Connection (RDP). É possível acessar arquivos locais em unidades de disco rígido, unidades de DVD, unidades de mídia portáteis e unidades de rede mapeadas.

Para acessar arquivos locais das instâncias do Windows, é necessário habilitar o recurso de compartilhamento de arquivos local mapeando a unidade de sessão remota para a unidade local. As etapas são um pouco diferentes, dependendo se o sistema operacional do computador local for Windows ou macOS X.

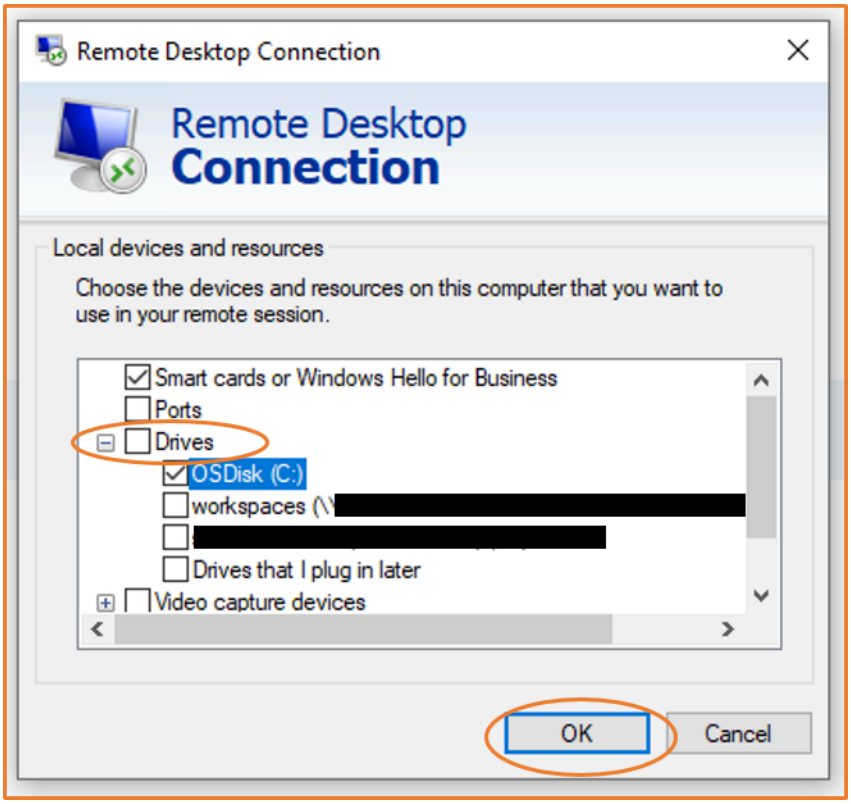
Windows

Para mapear a unidade de sessão remota para sua unidade local em seu computador Windows local

1. Abra o cliente de Conexão de Desktop Remoto.
2. Selecione Exibir opções.
3. Adicione o nome do host da instância ao campo Computer(Computador) e nome de usuário ao campo User name (Nome de usuário) da seguinte forma:
   a. Em Connection settings (Configurações de conexão), escolha Open... (Aberto) e busque o arquivo de atalho RDP baixado do console do Amazon EC2. O arquivo contém o nome do host DNS IPv4 público que identifica a instância e o nome de usuário do Administrador.
   b. Selecione o arquivo selecione Open (Abrir). Os campos Computer (Computador) e User name (Nome de usuário) são preenchidos com os valores do arquivo de atalho RDP.
   c. Escolha Salvar.
4. Selecione a guia Local Resources (Recursos locais).
5. Em Local Devices and resources (Dispositivos e recursos locais), escolha More... (Mais...).



6. Abra Drives (Unidades) e selecione a unidade local à qual mapear sua instância do Windows.
7. Escolha OK.

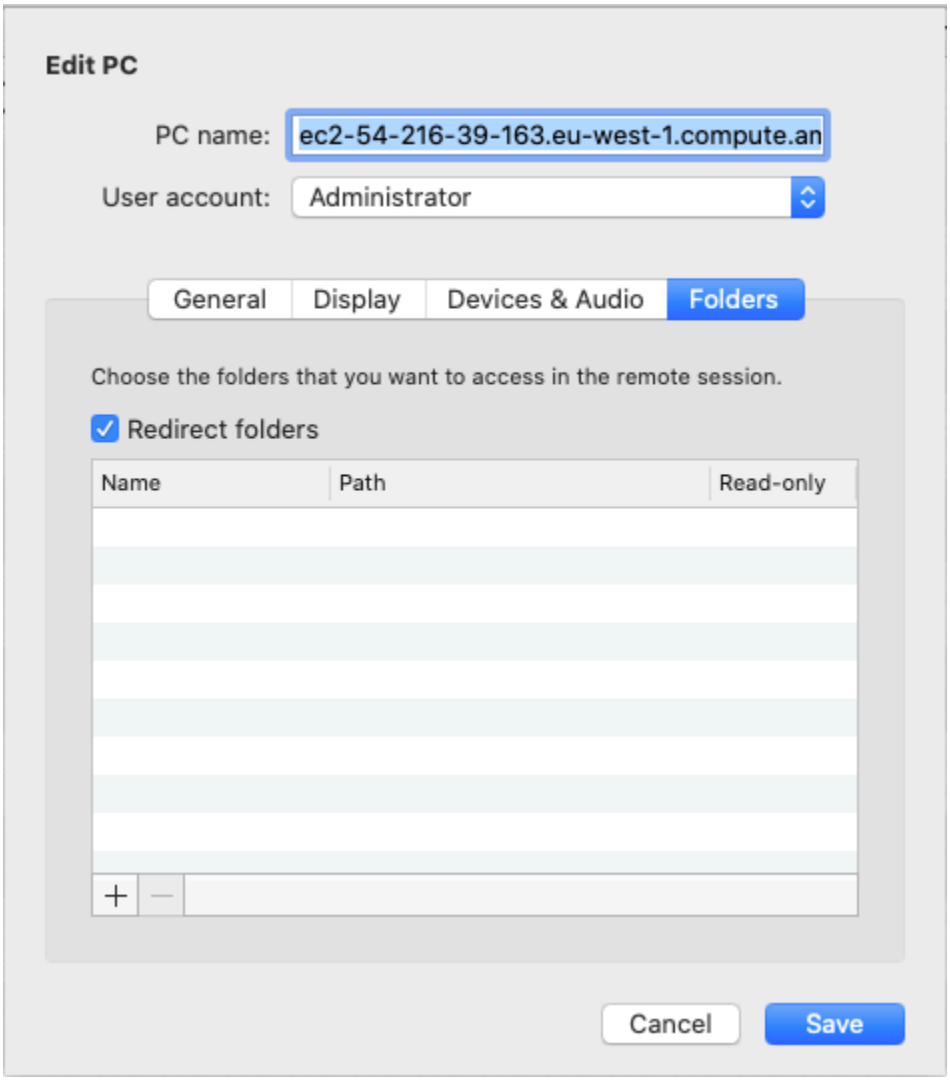


8. Selecione Connect (Conectar) para se conectar à sua instância do Windows.

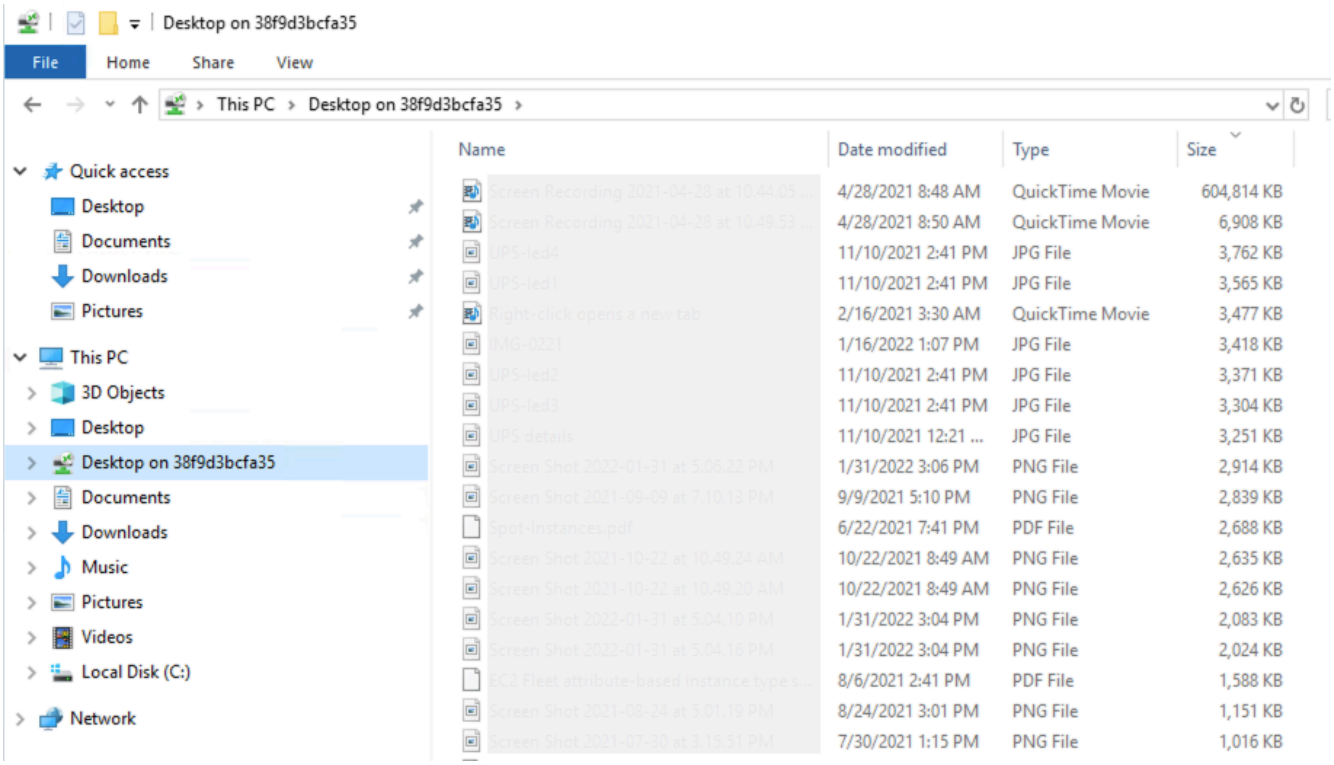
macOS X

Para mapear a unidade de sessão remota à pasta local em seu computador macOS X local

1. Abra o cliente de Conexão de Desktop Remoto.
2. Navegue até o arquivo RDP que você baixou do console do Amazon EC2 (ao se conectar inicialmente à instância) e arraste para o cliente Conexão de desktop remoto.
3. Clique com o botão direito do mouse no arquivo RDP e escolha Edit (Editar).
4. Selecione a guia Folders (Pastas) e a caixa de seleção Redirect folders (Pastas de redirecionamento).



5. Selecione o ícone + no canto inferior esquerdo, navegue até a pasta a ser mapeada e escolha Open (Abrir). Repita esta etapa para cada pasta a ser mapeada.
6. Escolha Salvar.
7. Selecione Connect (Conectar) para se conectar à sua instância do Windows. Você deverá inserir a senha.
8. Na instância, no Explorador de arquivos, expanda This PC (Este computador) e encontre a pasta compartilhada em que é possível acessar seus arquivos locais. Na captura de tela seguinte, a pasta Desktop no computador local foi mapeada para a unidade de sessão remota na instância.



Para obter mais informações sobre como disponibilizar dispositivos locais para uma sessão remota em um computador Mac, consulte Introdução ao cliente no Mac.

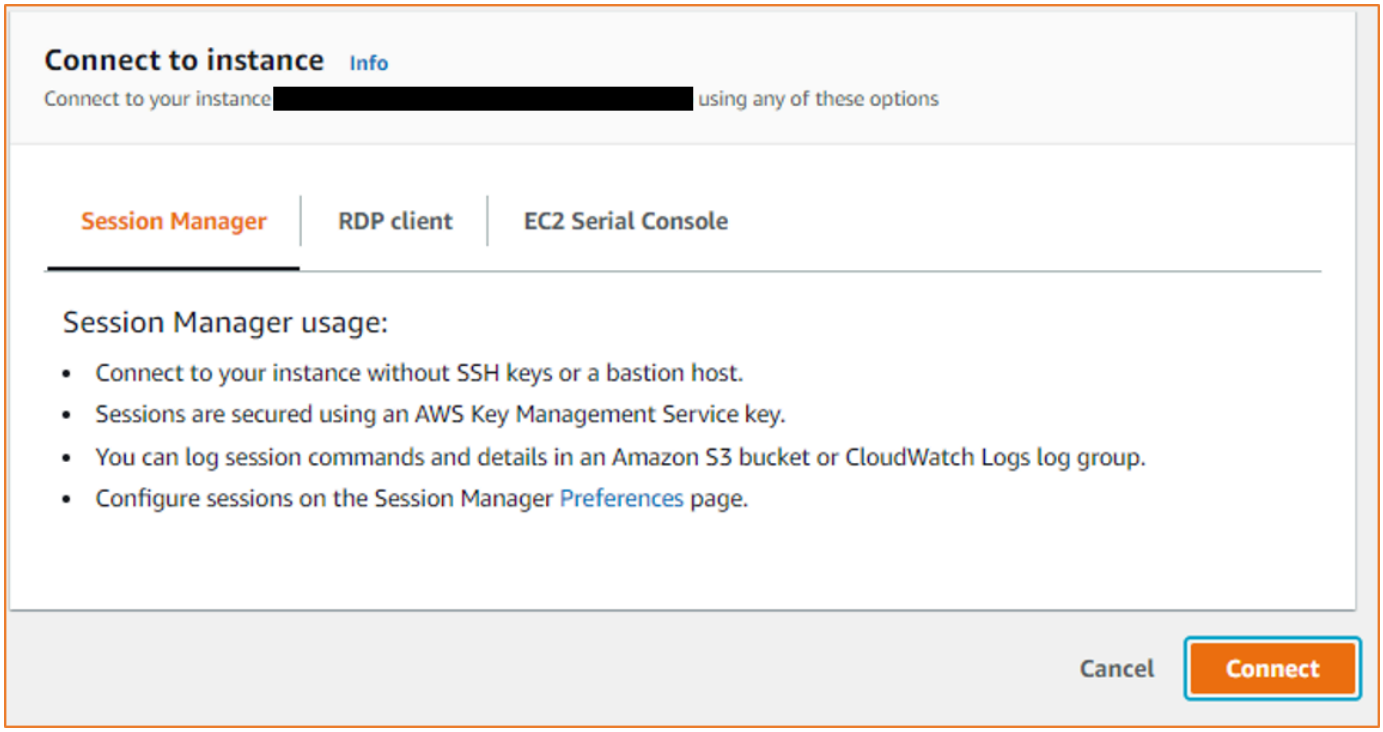
Conectar-se usando o Gerenciador de sessões

O Session Manager é um recurso totalmente gerenciado do AWS Systems Manager para gerenciar suas instâncias do Amazon EC2 por meio de um shell interativo baseado no navegador com um clique ou por meio da AWS CLI. É possível usar o Gerenciador de sessões para iniciar uma sessão com uma instância na sua conta. Depois que a sessão for iniciada, você poderá executar comandos interativos na instância como faria para qualquer outro tipo de conexão. Para obter mais informações sobre o Gerenciador de sessões, consulte Gerenciador de sessões do AWS Systems Manager no Guia do usuário do AWS Systems Manager.

Antes de tentar se conectar a uma instância usando o Gerenciador de sessões, verifique se as etapas de configuração necessárias foram concluídas. Para mais informações, consulte Configurar o Session Manager.

Para se conectar a uma instância do Amazon EC2 usando o Gerenciador de Sessões no console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar).
4. Em Connection method (Método de conexão), escolha Session Manager (Gerenciador de sessões).
5. Selecione Conectar.



> **Tip**
>
> Se você receber um erro informando que não você não tem autorização para executar uma ou mais ações do Systems Manager (`ssm:command-name`), será necessário atualizar suas políticas para permitir que inicie sessões pelo console do Amazon EC2. Para obter mais informações e instruções, consulte Início rápido de políticas padrão do IAM para o gerenciador de sessões no Guia do usuário doAWS Systems Manager.

Conectar-se a suas instâncias usando o EC2 Instance Connect Endpoint

O EC2 Instance Connect Endpoint permite a você se conectar com segurança a uma instância da Internet sem usar um bastion host ou exigir que sua nuvem privada virtual (VPC) tenha conectividade direta com a Internet.

Benefícios

- É possível estabelecer conexão com suas instâncias sem precisar que a instância tenha um endereço IPv4 público. A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.
- Você pode se conectar às suas instâncias pela Internet sem exigir que sua VPC tenha conectividade direta via gateway da Internet.
- Você pode controlar o acesso à criação e ao uso dos endpoints do EC2 Instance Connect para se conectar a instâncias usando políticas e permissões do IAM.
- Todas as tentativas de conexão com suas instâncias, tanto bem quanto malsucedidas, são registradas em log no CloudTrail.

Definição de preço

Não há custo adicional para usar endpoints do EC2 Instance Connect. Se você usar um EC2 Instance Connect Endpoint para se conectar a uma instância em uma zona de disponibilidade diferente, haverá uma cobrança adicional pela transferência de dados entre zonas de disponibilidade.

Conteúdo

- Como funcionam
- Considerações
- Conceder permissões para usar o EC2 Instance Connect Endpoint
- Grupos de segurança para o EC2 Instance Connect Endpoint
- Criar um EC2 Instance Connect Endpoint
- Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint
- Registro em log de conexões estabelecidas através do EC2 Instance Connect Endpoint
- Excluir um EC2 Instance Connect Endpoint

- Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint
- Cotas para EC2 Instance Connect Endpoint

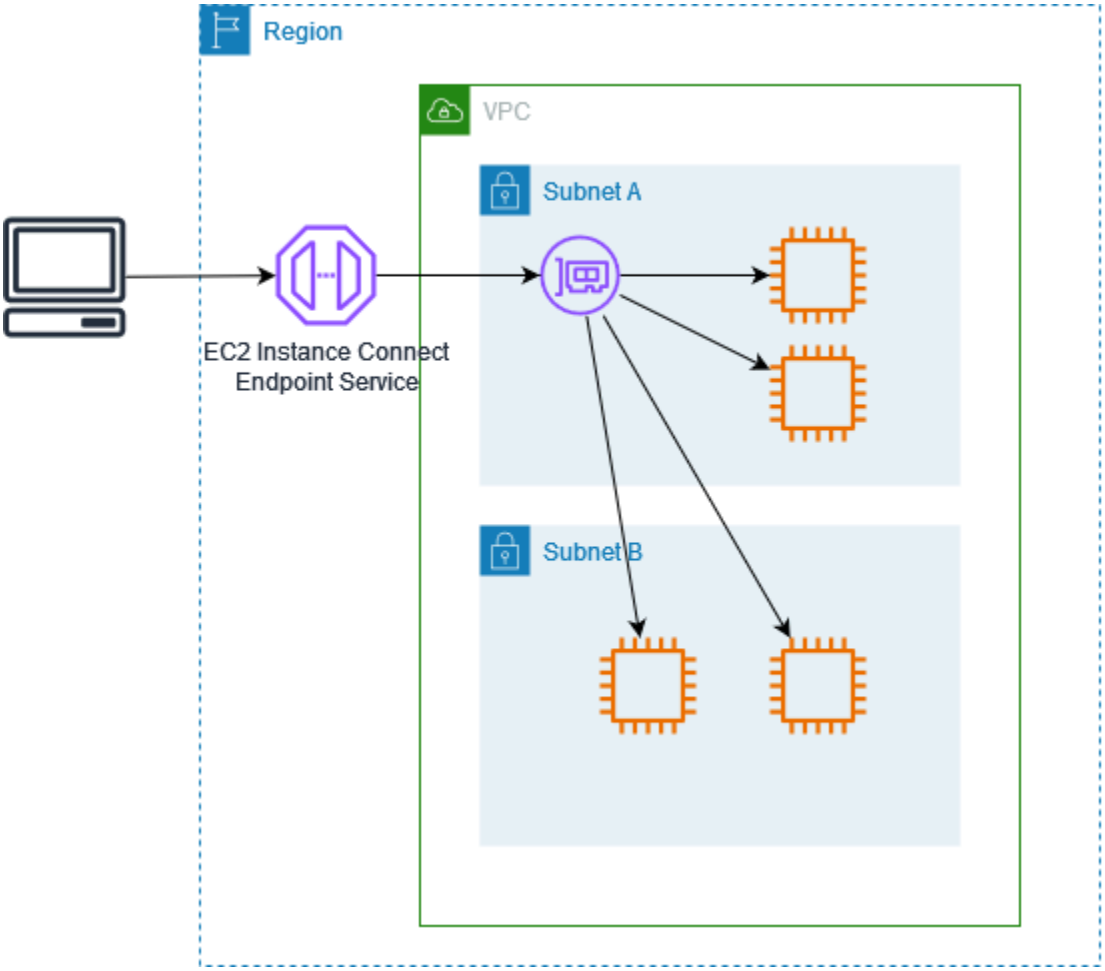
Como funcionam

O EC2 Instance Connect Endpoint é um proxy TCP com reconhecimento de identidade. O serviço EC2 Instance Connect Endpoint estabelece um túnel privado do seu computador até o endpoint usando as credenciais da sua entidade do IAM. O tráfego é autenticado e autorizado antes de chegar à sua VPC.

É possível configurar regras adicionais de grupo de segurança para restringir o tráfego de entrada para suas instâncias. Por exemplo, é possível usar regras de entrada para permitir nas portas de gerenciamento tráfego somente do EC2 Instance Connect Endpoint.

Também é possível configurar regras da tabela de rotas para permitir que o endpoint se conecte a qualquer instância em qualquer sub-rede da VPC.

O diagrama a seguir mostra como um usuário pode se conectar às suas instâncias via Internet usando um EC2 Instance Connect Endpoint. Primeiro, crie um EC2 Instance Connect Endpoint na sub-rede A. Criamos então uma interface de rede para o endpoint na sub-rede, o qual atua como ponto de entrada para o tráfego destinado às suas instâncias na VPC. Se a tabela de rotas da sub-rede B permitir o tráfego da sub-rede A, você poderá usar o endpoint para alcançar instâncias na sub-rede B.



Considerações

Antes de começar, considere o seguinte:

- O EC2 Instance Connect Endpoint foi projetado especificamente para casos de uso de tráfego de gerenciamento, e não para transferências de dados de alto volume. A utilização de transferências de dados de alto volume é controlada.
- A instância deve ter um endereço IPv4 (privado ou público). O EC2 Instance Connect Endpoint não oferece suporte a conexões com instâncias que utilizam endereços IPv6.
- (Instâncias do Linux) Caso use o próprio par de chaves, você poderá usar qualquer AMI do Linux. Caso contrário, a instância deverá ter o EC2 Instance Connect instalado. Para obter informações sobre quais AMIs incluem o EC2 Instance Connect e como instalá-lo em outras AMIs compatíveis, consulte Instalar o EC2 Instance Connect.
- Você pode atribuir um grupo de segurança a um EC2 Instance Connect Endpoint ao criá-lo. Caso contrário, o grupo de segurança padrão será usado para a VPC. O grupo de segurança de um EC2

Instance Connect Endpoint deve permitir tráfego de saída para as instâncias de destino. Para ter mais informações, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.

- É possível configurar um EC2 Instance Connect Endpoint para preservar os endereços IP de origem dos clientes ao rotear solicitações para as instâncias. Caso contrário, o endereço IP da interface de rede se tornará o endereço IP do cliente para todo o tráfego de entrada.
  - Se você ativar a preservação de IP do cliente, os grupos de segurança das instâncias deverão permitir o tráfego dos clientes. Além disso, as instâncias deverão estar na mesma VPC do EC2 Instance Connect Endpoint.
  - Se você desativar a preservação de IP do cliente, os grupos de segurança das instâncias deverão permitir o tráfego da VPC. Esse é o padrão.
  - Os seguintes tipos de instância não oferecem suporte à preservação do IP do cliente: C1, CG1, CG2, G1, HI1, M1, M2, M3 e T1. Se você ativar a preservação de IP do cliente e tentar se conectar a uma instância com um desses tipos de instância usando o EC2 Instance Connect Endpoint, a conexão falhará.
  - Não há suporte à preservação de IP do cliente quando o tráfego for roteado por meio de um gateway de trânsito.
- Ao criar um EC2 Instance Connect Endpoint, uma função vinculada ao serviço é criada automaticamente para o serviço Amazon EC2 no AWS Identity and Access Management (IAM). O Amazon EC2 usa o perfil vinculado ao serviço para provisionar interfaces de rede em sua conta, que são exigidas ao criar EC2 Instance Connect Endpoints. Para ter mais informações, consulte Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint.
- Cada EC2 Instance Connect Endpoint pode acomodar até 20 conexões simultâneas.
- A duração máxima de uma conexão TCP estabelecida é 1 hora (3.600 segundos). É possível especificar a duração máxima permitida em uma política do IAM, que pode ser de até 3.600 segundos. Para ter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.
- Não há suporte ao EC2 Instance Connect Endpoint na região Oeste do Canadá (Calgary).

Conceder permissões para usar o EC2 Instance Connect Endpoint

Por padrão, as entidades do IAM não têm permissão para criar, descrever ou modificar os EC2 Instance Connect Endpoints. Um administrador do IAM deve criar políticas do IAM que concedam as permissões necessárias para executar ações específicas nos recursos necessários.

Para obter informações sobre a criação de políticas do IAM, consulte Criação de políticas do IAM, no Manual do usuário do IAM.

Os exemplos de políticas a seguir mostram como é possível controlar as permissões que os usuários têm sobre os EC2 Instance Connect Endpoints.

Exemplos

- Permissões para criar, descrever e excluir EC2 Instance Connect Endpoints
- Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias
- Permissões para conectar somente de um intervalo de endereços IP específico

Permissões para criar, descrever e excluir EC2 Instance Connect Endpoints

Para criar um EC2 Instance Connect Endpoint, os usuários precisam de permissões para as seguintes ações:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Para descrever e excluir EC2 Instance Connect Endpoints, os usuários precisam de permissões para as seguintes ações:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

É possível criar uma política que conceda permissão para criar, descrever e excluir EC2 Instance Connect Endpoints em todas as sub-redes. Como alternativa, é possível restringir ações para sub-redes especificadas somente especificando os ARNs da sub-rede como o `Resource` permitido ou usando a chave de condição `ec2:SubnetID`. Você também pode usar a chave de condição `aws:ResourceTag` para permitir ou negar explicitamente a criação de endpoints com determinadas tags. Para obter mais informações, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

Exemplo de política do IAM

No exemplo de política do IAM a seguir, a seção `Resource` concede permissão para criar e excluir endpoints em todas as sub-redes, especificadas pelo asterisco (`*`). As ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "GrantAllActionsInAllSubnets",
            "Action": [
                "ec2:CreateInstanceConnectEndpoint",
                "ec2:DeleteInstanceConnectEndpoint",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:subnet/*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:::security-group/*"
        },
        {
            "Sid": "DescribeInstanceConnectEndpoints",
            "Action": [
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias

A ação `ec2-instance-connect:OpenTunnel` concede permissão para estabelecer uma conexão TCP com uma instância para se conectar via EC2 Instance Connect Endpoint. É possível especificar o EC2 Instance Connect Endpoint a ser usado. Como alternativa, um `Resource` com um asterisco

(*) permite que os usuários usem qualquer EC2 Instance Connect Endpoint disponível. Você também pode restringir o acesso às instâncias com base na presença ou ausência de tags de recurso como chaves de condição.

Condições

- `ec2-instance-connect:remotePort`: a porta na instância que pode ser usada para estabelecer uma conexão TCP. Quando essa chave de condição é usada, tentar conectar-se a uma instância em qualquer outra porta que não seja a especificada na política resultará em falha.
- `ec2-instance-connect:privateIpAddress`: o endereço IP privado de destino associado à instância com a qual você deseja estabelecer uma conexão TCP. É possível especificar um único endereço IP, como `10.0.0.1/32`, ou um intervalo de IPs por meio de CIDRs, como `10.0.1.0/28`. Quando essa chave de condição é usada, tentar conectar-se a uma instância com um endereço IP privado diferente ou fora do intervalo CIDR resultará em falha.
- `ec2-instance-connect:maxTunnelDuration`: a duração máxima de uma conexão TCP estabelecida. A unidade é em segundos, e a duração varia de um mínimo de 1 segundo a um máximo de 3.600 segundos (uma hora). Se a condição não for especificada, a duração padrão será definida como 3.600 segundos (uma hora). A tentativa de conectar-se a uma instância por mais tempo do que a duração especificada na política do IAM ou por mais tempo do que o máximo padrão resultará em falha. A conexão é desconectada após a duração especificada.

  Se `maxTunnelDuration` for especificado na política do IAM e o valor especificado for inferior a 3.600 segundos (o padrão), você deverá especificar `--max-tunnel-duration` no comando ao conectar-se a uma instância. Para obter informações sobre como conectar-se a uma instância, consulte Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint.

Também é possível conceder a um usuário acesso para estabelecer conexões com instâncias com base na presença de tags de recursos no EC2 Instance Connect Endpoint. Para obter mais informações, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

Para instâncias do Linux, a ação `ec2-instance-connect:SendSSHPublicKey` concede permissão para enviar a chave pública para uma instância. A condição `ec2:osuser` especifica o nome do usuário do SO (sistema operacional) que pode enviar a chave pública para uma instância. Use o nome de usuário padrão da AMI que você usou para iniciar a instância. Para ter mais informações, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Exemplo de política do IAM

Os exemplos de políticas do IAM apresentados a seguir permitem que uma entidade principal do IAM se conecte a uma instância usando somente o endpoint de conexão da instância do EC2 especificado, que é identificado pelo ID `eice-123456789abcdef` do endpoint especificado. A conexão será estabelecida com êxito somente se todas as condições forem atendidas.

> **Note**
>
> As ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

Linux

Este exemplo avalia se a conexão com a instância foi estabelecida na porta 22 (SSH), se o endereço IP privado da instância está dentro do intervalo de `10.0.1.0/31` (que compreende `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` é menor ou igual a `3600` segundos. A conexão será desconectada após `3600` segundos (1 hora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Este exemplo avalia se a conexão com a instância foi estabelecida na porta 3389 (RDP), se o endereço IP privado da instância está dentro do intervalo de `10.0.1.0/31` (que compreende `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` é menor ou igual a `3600` segundos. A conexão será desconectada após `3600` segundos (1 hora).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
```

```
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Permissões para conectar somente de um intervalo de endereços IP específico

O exemplo de política do IAM a seguir permite que uma entidade principal do IAM conecte-se a uma instância, desde que esteja se conectando a partir de um endereço IP dentro do intervalo de endereços IP especificado na política. Se a entidade principal do IAM chamar `OpenTunnel` desde um endereço IP que não esteja dentro de `192.0.2.0/24` (o exemplo de intervalo de endereços IP nesta política), a resposta será `Access Denied`. Para obter mais informações, consulte`aws:SourceIp` no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
```

```
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Grupos de segurança para o EC2 Instance Connect Endpoint

Um grupo de segurança controla o tráfego que tem permissão para acessar e sair dos recursos aos quais está associado. Por exemplo, negamos tráfego de e para uma instância do Amazon EC2, a menos que seja especificamente permitido pelos grupos de segurança associados à instância.

Os exemplos a seguir mostram como configurar as regras do grupo de segurança para o EC2 Instance Connect Endpoint e as instâncias de destino.

Exemplos

- Regras de grupo de segurança para o EC2 Instance Connect Endpoint
- Regras do grupo de segurança da instância de destino

Regras de grupo de segurança para o EC2 Instance Connect Endpoint

As regras de grupo de segurança para um EC2 Instance Connect Endpoint devem permitir que o tráfego de saída para as instâncias de destino deixem o endpoint. Você pode especificar o grupo de segurança da instância ou o intervalo de endereços IPv4 da VPC como o destino.

O tráfego para o endpoint é proveniente do EC2 Instance Connect Endpoint Service e é permitido independentemente das regras de entrada do grupo de segurança do endpoint. Para controlar quem

pode usar o endpoint do EC2 Instance Connect para se conectar a uma instância, use uma política do IAM. Para ter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.

Exemplo de regra de saída: referência a grupos de segurança

O exemplo a seguir usa referência a grupos de segurança, o que significa que o destino é um grupo de segurança associado às instâncias de destino. Essa regra permite tráfego de saída do endpoint para todas as instâncias que usam esse grupo de segurança.

Protocolo	Destination (Destino)	Intervalo de portas	Comentário
TCP	*ID do grupo de segurança da instância*	22	Permite tráfego SSH de saída para todas as instâncias associadas ao grupo de segurança da instância

Exemplo de regra de saída: intervalo de endereços IPv4

O exemplo a seguir permite tráfego de saída para o intervalo de endereços IPv4 especificado. Os endereços IPv4 de uma instância são atribuídos a partir de sua sub-rede para que você possa usar o intervalo de endereços IPv4 da VPC.

Protocolo	Destination (Destino)	Intervalo de portas	Comentário
TCP	*CIDR IPv4 da VPC*	22	Permite tráfego SSH de saída para a VPC

Regras do grupo de segurança da instância de destino

As regras do grupo de segurança para instâncias de destino devem permitir o tráfego de entrada do EC2 Instance Connect Endpoint. É possível especificar o grupo de segurança do endpoint ou um intervalo de endereços IPv4 como origem. Se você especificar um intervalo de endereços IPv4, a origem dependerá se a preservação do IP do cliente está desativada ou ativada. Para ter mais informações, consulte Considerações.

Como os grupos de segurança são stateful, o tráfego de resposta tem permissão para sair da VPC, independentemente das regras de saída do grupo de segurança da instância.

Exemplo de regra de entrada: referência a grupos de segurança

O exemplo a seguir usa referência a grupos de segurança, o que significa que a origem é o grupo de segurança associado ao endpoint. Essa regra permite tráfego SSH de entrada do endpoint para todas as instâncias que usam esse grupo de segurança, independentemente de a preservação do IP do cliente estar ativada ou desativada. Se não houver outras regras do grupo de segurança de entrada para SSH, as instâncias aceitarão tráfego SSH somente do endpoint.

Protocolo	Origem	Intervalo de portas	Comentário
TCP	*ID do grupo de segurança do endpoint*	22	Permite tráfego SSH de entrada dos recursos associados ao grupo de segurança do endpoint

Exemplo de regra de entrada: preservação do IP do cliente desativada

O exemplo a seguir permite tráfego SSH de entrada do intervalo de endereços IPv4 especificado. Como a preservação do IP do cliente está desativada, o endereço IPv4 de origem é o endereço da interface de rede do endpoint. O endereço da interface de rede do endpoint é atribuído a partir de sua sub-rede, então você pode usar o intervalo de endereços IPv4 da VPC para permitir conexões com todas as instâncias na VPC.

Protocolo	Origem	Intervalo de portas	Comentário
TCP	*CIDR IPv4 da VPC*	22	Permitir tráfego de entrada SSH da VPC

Exemplo de regra de entrada: preservação do IP do cliente ativada

O exemplo a seguir permite tráfego SSH de entrada do intervalo de endereços IPv4 especificado. Como a preservação do IP do cliente está ativada, o endereço IPv4 de origem é o endereço do cliente.

Protocolo	Origem	Intervalo de portas	Comentário
TCP	*Intervalo de endereços IPv4 públicos*	22	Permite tráfego de entrada do intervalo de endereços IPv4 do cliente especificado.

Criar um EC2 Instance Connect Endpoint

É possível criar um EC2 Instance Connect Endpoint para permitir uma conexão segura com suas instâncias.

Você não pode modificar um EC2 Instance Connect Endpoint depois de criá-lo. Em vez disso, será necessário excluir o EC2 Instance Connect Endpoint e criar um novo com as configurações necessárias.

Pré-requisitos

É necessário ter as permissões do IAM exigidas para criar um EC2 Instance Connect Endpoint. Para ter mais informações, consulte Permissões para criar, descrever e excluir EC2 Instance Connect Endpoints.

Sub-redes compartilhadas

Você pode criar um endpoint de conexão de instância do EC2 em uma sub-rede que é compartilhada com você. Você não pode criar um endpoint de conexão de instância do EC2 que o proprietário da VCP criou em uma sub-rede que é compartilhada com você.

Criar um endpoint usando o console

Use o procedimento a seguir para criar um EC2 Instance Connect Endpoint.

Para criar um EC2 Instance Connect Endpoint

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Endpoints.
3. Escolha Criar endpoint e, em seguida, especifique as configurações do endpoint:

a. (Opcional) Em Tag de nome, insira um nome para o endpoint.
b. Em Categoria de serviço, escolha Endpoint do EC2 Instance Connect.
c. Em VPC, escolha a VPC que contém as instâncias de destino.
d. (Opcional) Para preservar os endereços IP do cliente, expanda Configurações adicionais e marque a caixa de seleção. Caso contrário, o padrão é usar a interface de rede do endpoint como endereço IP do cliente.
e. (Opcional) Em Grupos de segurança, selecione o grupo de segurança a ser associado ao endpoint. Caso contrário, o grupo de segurança padrão da VPC será usado. Para ter mais informações, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.
f. Em Sub-rede, selecione a sub-rede na qual o endpoint será criado.
g. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.

4. Revise suas configurações e escolha Criar endpoint.

   O estado inicial do endpoint é Pendente. Antes de conectar-se a uma instância usando esse endpoint, aguarde até que o status do endpoint seja Disponível. Isso pode levar alguns minutos.

5. Para se conectar a uma instância usando seu endpoint, consulte Conectar a uma instância.

Criar o endpoint usando a AWS CLI

Use o comando create-instance-connect-endpoint para criar um EC2 Instance Connect Endpoint.

Pré-requisitos

Instale a AWS CLI versão 2 e configure-a usando suas credenciais. Para obter mais informações, consulte Instalar ou atualizar para a versão mais recente da AWS CLI e Configurar a AWS CLI no Guia do usuário da AWS Command Line Interface. Como alternativa, abra AWS CloudShell e execute os comandos da AWS CLI em seu shell pré-autenticado.

Para criar o endpoint

Use o comando a seguir para criar uma interface de rede de endpoint para seu EC2 Instance Connect Endpoint na sub-rede especificada.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

O seguinte é um exemplo de saída.

```
 {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": []
}
```

Para monitorar o status da criação

O valor inicial do campo `State` é `create-in-progress`. Antes de se conectar a uma instância usando esse endpoint, aguarde até que o status seja `create-complete`. Use o comando describe-instance-connect-endpoints para monitorar o status do EC2 Instance Connect Endpoint. O parâmetro --query filtra os resultados para o campo `State`.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

O seguinte é um exemplo de saída.

```
create-complete
```

Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint

É possível usar o EC2 Instance Connect Endpoint para se conectar a uma instância do Amazon EC2 compatível com SSH ou RDP.

Conteúdos

- Pré-requisitos
- Solução de problemas

Pré-requisitos

- É necessário ter a permissão do IAM exigida para criar um EC2 Instance Connect Endpoint. Para ter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.
- O EC2 Instance Connect Endpoint deve estar no estado Disponível (console) ou `create-complete` (AWS CLI). Caso não tenha um EC2 Instance Connect Endpoint para sua VPC, você poderá criar um. Para ter mais informações, consulte Criar um EC2 Instance Connect Endpoint.
- (Instâncias do Linux) Para usar o console do EC2 para se conectar à instância ou para usar a CLI para se conectar e fazer com que o EC2 Instance Connect lide com a chave temporária, a instância deve ter o EC2 Instance Connect instalado. Para ter mais informações, consulte Instalar o EC2 Instance Connect.
- Certifique-se de que o grupo de segurança da instância permita tráfego SSH de entrada do grupo de segurança do EC2 Instance Connect Endpoint. Para ter mais informações, consulte Regras do grupo de segurança da instância de destino.

Conectar-se à sua instância do Linux usando o console do Amazon EC2

Você pode se conectar a uma instância usando o console do Amazon EC2 conforme descrito a seguir.

Como se conectar à sua instância usando o cliente com base em navegador

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.

4. Escolha a guia EC2 Instance Connect.
5. Em Tipo de conexão, escolha Conectar-se usando o EC2 Instance Connect Endpoint.
6. Em EC2 Instance Connect Endpoint, escolha o ID do EC2 Instance Connect Endpoint.
7. Em Nome de usuário, se a AMI que você usou para iniciar a instância usar um nome de usuário diferente de `ec2-user`, insira o nome de usuário correto.
8. Em Duração máxima do túnel (segundos), insira a duração máxima permitida para a conexão de SSH.

   A duração deve estar em conformidade com qualquer condição `maxTunnelDuration` especificada na política do IAM. Caso não tenha acesso à política do IAM, entre em contato com seu administrador.
9. Selecione Conectar. Isso abrirá uma janela de terminal para sua instância.

Conectar-se à instância do Linux usando SSH

É possível usar o SSH para se conectar à sua instância de Linux e usar o comando `open-tunnel` para estabelecer um túnel privado. É possível usar `open-tunnel` no modo de conexão única ou de conexão múltipla.

Para obter mais informações sobre o uso da AWS CLI para se conectar à sua instância utilizando SSH, consulte Conectar-se usando o AWS CLI.

Os exemplos a seguir usam OpenSSH. É possível usar qualquer outro cliente SSH que ofereça suporte a um modo proxy.

Conexão única

Para permitir somente uma única conexão com uma instância usando SSH e o comando **`open-tunnel`**

Use o `ssh` o comando open-tunnel da AWS CLI da seguinte forma. O comando de proxy `-o` inclui o comando `open-tunnel` que cria o túnel privado para a instância.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-0123456789example'
```

Em:

- `-i`: especifique o par de chaves usado para iniciar a instância.
- *`ec2-user`*`@`*`i-0123456789example`*: especifique o nome do usuário da AMI que foi usada para iniciar a instância e o ID da instância.
- `--instance-id`: especifique o ID da instância à qual se conectar. Como alternativa, especifique `%h`, que extrai o ID da instância do usuário.

Conexão múltipla

Para permitir várias conexões a uma instância, primeiro execute o comando open-tunnel da AWS CLI para começar a escutar novas conexões de TCP, e depois use o `ssh` para criar uma nova conexão de TCP e um túnel privado para sua instância.

Para permitir várias conexões com sua instância usando SSH e o comando **`open-tunnel`**

1. Execute o comando a seguir para começar a escutar novas conexões de TCP na porta especificada em sua máquina local.

```
aws ec2-instance-connect open-tunnel \
    --instance-id i-0123456789example \
    --local-port 8888
```

   Saída esperada

```
Listening for connections on port 8888.
```

2. Em uma nova janela de terminal, execute o comando `ssh` a seguir para criar uma nova conexão de TCP e um túnel privado para sua instância.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

   Saída esperada: na primeira janela do terminal, você verá o seguinte:

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

   Também será possível ver o seguinte:

```
[1] Closing tcp connection.
```

Conectar-se à sua instância do Linux usando a AWS CLI

Se você souber apenas o ID da sua instância, poderá usar o comando ec2-instance-connect da AWS CLI para se conectar à sua instância usando um cliente SSH. Para obter mais informações sobre como usar o comando ec2-instance-connect, consulte Conectar-se usando o AWS CLI.

Pré-requisitos

Instale a AWS CLI versão 2 e configure-a usando suas credenciais. Para obter mais informações, consulte Instalar ou atualizar para a versão mais recente da AWS CLI e Configurar a AWS CLI no Guia do usuário da AWS Command Line Interface. Como alternativa, abra AWS CloudShell e execute os comandos da AWS CLI em seu shell pré-autenticado.

Para se conectar a uma instância usando o ID da instância e um EC2 Instance Connect Endpoint

Se você souber apenas o ID da instância, use o comando ec2-instance-connect da CLI e especifique o comando `ssh`, o ID da instância e o parâmetro `--connection-type` com o valor `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

> **Tip**
>
> Se receber um erro ao usar esse comando, verifique se está usando o AWS CLI versão 2. O parâmetro `ssh` apenas está disponível para o AWS CLI versão 2. Para obter mais informações, consulte Sobre o AWS CLI versão 2, no Guia do usuário do AWS Command Line Interface.

Conectar a sua instância Windows usando o EC2 Instance Connect Endpoint

É possível usar o Remote Desktop Protocol (RDP) no EC2 Instance Connect Endpoint para se conectar a uma instância do Windows sem um endereço IPv4 público ou nome de DNS público.

Para se conectar à sua instância do Windows usando um cliente RDP

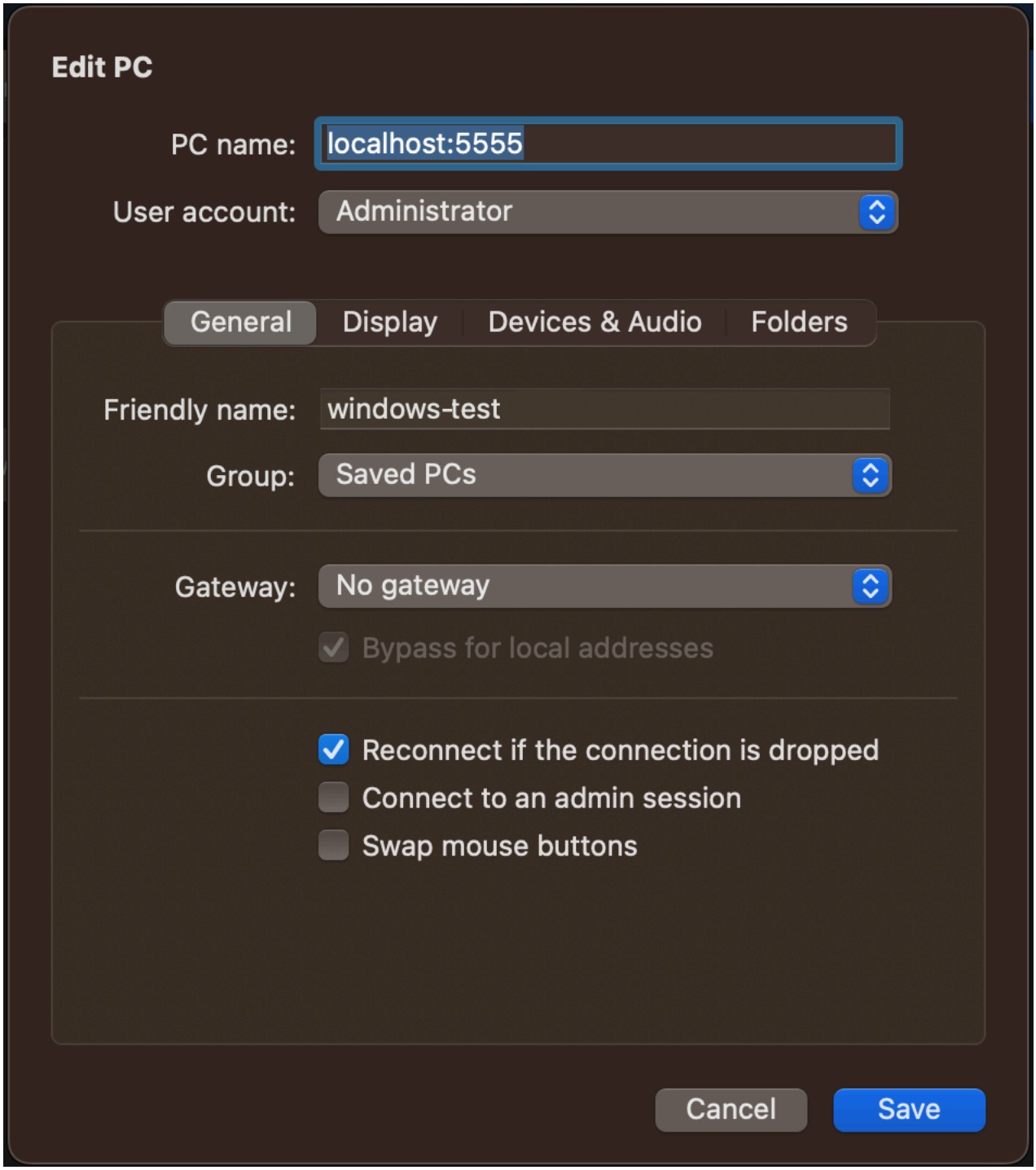
1. Conclua as etapas 1 a 8 em Conectar-se à sua instância baseada no Windows usando RDP. Após fazer o download do arquivo da área de trabalho RDP na Etapa 8, você receberá uma mensagem Não foi possível se conectar, o que é esperado porque a instância não tem um endereço IP público.

2. Execute o comando a seguir para estabelecer um túnel privado para a VPC na qual a instância está localizada. A `--remote-port` deve ser `3389`, pois o RDP usa a porta 3389 por padrão.

```
aws ec2-instance-connect open-tunnel \
    --instance-id i-0123456789example \
    --remote-port 3389 \
    --local-port any-port
```

3. Na sua pasta Downloads, localize o arquivo de área de trabalho de RDP que você baixou e arraste-o para a janela do cliente RDP.
4. Clique com o botão direito do mouse no arquivo de área de trabalho de RDP e escolha Editar.
5. Na janela Editar computador, para Nome do computador (a instância à qual se conectar), insira `localhost:`*`local-port`*, em que *`local-port`* usa o mesmo valor especificado na Etapa 2, e, em seguida, escolha Salvar.

   Observe que a captura de tela a seguir da janela Editar PC é do Microsoft Remote Desktop em um Mac. Se você estiver usando um cliente Windows, a janela pode ser diferente.



6. No cliente RDP, clique com o botão direito do mouse no PC (que você acabou de configurar) e escolha Conectar para se conectar à sua instância.
7. No prompt, insira a senha descriptografada da conta do administrador.

Solução de problemas

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas que podem ser encontrados ao usar o EC2 Instance Connect Endpoint para se conectar a uma instância.

Não é possível conectar-se à sua instância

A seguir estão motivos comuns pelos quais você pode não conseguir se conectar à sua instância.

- Grupos de segurança: verifique os grupos de segurança atribuídos ao EC2 Instance Connect Endpoint e à sua instância. Para obter mais informações sobre as regras necessárias de grupo de segurança, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.
- Estado da instância:^verifique se a instância está no estado `running`.
- Par de chaves: se o comando que você está usando para se conectar exigir uma chave privada, verifique se sua instância tem uma chave pública e se você tem a chave privada correspondente.
- Permissões do IAM: verifique se você tem as permissões do IAM necessárias. Para ter mais informações, consulte Conceder permissões para usar o EC2 Instance Connect Endpoint.

Para obter mais dicas de solução de problemas para instâncias do Linux, consulte Solução de problemas de conexão com a instância do Linux. Para obter dicas de solução de problemas para instâncias do Windows, consulte the section called “Conectar-se à sua instância do Windows do ”.

ErrorCode: AccessDeniedException

Se você receber um erro `AccessDeniedException` e a condição `maxTunnelDuration` estiver especificada na política do IAM, certifique-se de especificar o parâmetro `--max-tunnel-duration` ao conectar-se a uma instância. Para obter mais informações sobre esse parâmetro, consulte open-tunnel na Referência de comandos da AWS CLI.

Registro em log de conexões estabelecidas através do EC2 Instance Connect Endpoint

É possível registrar em log operações de recursos e auditar conexões estabelecidas através do EC2 Instance Connect Endpoint com logs do AWS CloudTrail.

Para obter mais informações sobre o uso do AWS CloudTrail com o Amazon EC2, consulte Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail.

Registro em log de chamadas da API do EC2 Instance Connect Endpoint com o AWS CloudTrail

As operações de recursos do EC2 Instance Connect Endpoint são registradas em log no CloudTrail como eventos de gerenciamento. Quando as seguintes chamadas de API são executadas, a atividade é registrada como um evento do CloudTrail no Histórico de eventos:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

É possível visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos CloudTrail no Guia do usuário do AWS CloudTrail.

Use o AWS CloudTrail para auditar usuários que se conectam a uma instância usando o EC2 Instance Connect Endpoint

As tentativas de conexão a instâncias por meio do EC2 Instance Connect Endpoint são registradas em log no CloudTrail no Histórico de eventos. Quando uma conexão a uma instância é iniciada por meio de um EC2 Instance Connect Endpoint, a conexão é registrada em log como um evento de gerenciamento do CloudTrail com `eventName` de `OpenTunnel`.

É possível criar regras do Amazon EventBridge que direcionem o evento do CloudTrail para um destino. Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Veja a seguir o exemplo de um evento de gerenciamento `OpenTunnel` que foi registrado em log no CloudTrail.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name"
    },
    "eventTime": "2023-04-11T23:50:40Z",
```

```
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Excluir um EC2 Instance Connect Endpoint

Quando não precisar mais de um EC2 Instance Connect Endpoint, você poderá excluí-lo.

É necessário ter as permissões do IAM exigidas para criar um EC2 Instance Connect Endpoint. Para ter mais informações, consulte Permissões para criar, descrever e excluir EC2 Instance Connect Endpoints.

Quando um EC2 Instance Connect Endpoint é excluído via console, ele entra no estado Excluindo. Se a exclusão for bem-sucedida, o endpoint excluído não aparecerá mais. Se exclusão falhar, o estado será `delete-failed` e o campo Mensagem de status fornecerá o motivo da falha.

Quando um EC2 Instance Connect Endpoint é excluído via AWS CLI, ele entra no estado `delete-in-progress`. Se a exclusão for bem-sucedida, ela entrará no estado `delete-complete`. Se exclusão falhar, o estado será `delete-failed` e `StateMessage` fornecerá o motivo da falha.

Console

Para excluir um EC2 Instance Connect Endpoint

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Endpoints.
3. Selecione o endpoint.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Excluir.

AWS CLI

Para excluir um EC2 Instance Connect Endpoint

Use o comando delete-instance-connect-endpoint da AWS CLI e especifique o ID do EC2 Instance Connect Endpoint a ser excluído.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

O seguinte é um exemplo de saída.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O Amazon EC2 usa perfis vinculados ao serviço do AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo especial de perfil do IAM vinculado diretamente ao Amazon EC2. Os perfis vinculados ao serviço são predefinidos pelo Amazon EC2 e incluem todas as permissões necessárias para que o Amazon EC2 possa chamar outros Serviços da AWS em seu nome. Para obter mais informações, consulte Usar perfis vinculados ao serviço no Guia do usuário do IAM.

Permissões de perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O Amazon EC2 usa o AWSServiceRoleForEC2InstanceConnect para gerenciar as interfaces de rede em sua conta que são exigidas pelo EC2 Instance Connect Endpoint.

O perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect confia nos seguintes serviços para assumir o perfil:

- `ec2-instance-connect.amazonaws.com`

O perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect usa a política gerenciada Ec2InstanceConnectEndpoint. Para visualizar as permissões para esta política, consulte Ec2InstanceConnectEndpoint na Referência de políticas gerenciadas da AWS.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do Usuário do IAM.

Criar um perfil vinculado ao serviço para um EC2 Instance Connect Endpoint

Você não precisa criar manualmente o perfil vinculado ao serviço. Quando você cria um EC2 Instance Connect Endpoint, o Amazon EC2 cria o perfil vinculado ao serviço por você.

Editar um perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O EC2 Instance Connect Endpoint não permite editar o perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect.

Excluir um perfil vinculado ao serviço para um EC2 Instance Connect Endpoint

Se você não precisar mais usar o EC2 Instance Connect Endpoint, é recomendável excluir o perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect.

Antes de excluir o perfil vinculado ao serviço, é necessário excluir todos os recursos do EC2 Instance Connect Endpoint.

Para excluir a função vinculada ao serviço, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Cotas para EC2 Instance Connect Endpoint

Sua Conta da AWS tem cotas padrão para cada serviço da AWS, que anteriormente eram chamadas de limites. A menos que especificado de outra forma, cada cota é específica da região .

Sua Conta da AWS tem as seguintes cotas relacionadas ao EC2 Instance Connect Endpoint.

Descrição	Quota
Número máximo de endpoints do EC2 Instance Connect por Conta da AWS Região da AWS	5
Número máximo de endpoints do EC2 Instance Connect por VPC	1
Número máximo de endpoints do EC2 Instance Connect por sub-rede	1
Número máximo de conexões simultâneas por endpoint do Instance Connect do EC2	20

Conectar sua instância do EC2 a um recurso da AWS

Depois de iniciar uma instância, é possível conectá-la a um ou mais recursos da AWS.

Esta seção descreve como conectar automaticamente uma instância do Amazon EC2 a um banco de dados do Amazon RDS.

Conectar automaticamente uma instância do EC2 e um banco de dados do RDS

É possível usar a funcionalidade de conexão automática no console do Amazon EC2 para conectar rapidamente uma ou mais instâncias do EC2 a um banco de dados do RDS para permitir o tráfego entre elas.

Para ter mais informações, consulte Como a conexão é configurada automaticamente. Para ver um passo a passo com outras formas de conectar uma instância do EC2 e um banco de dados do RDS, consulte Tutorial: conectar uma instância do Amazon EC2 a um banco de dados do Amazon RDS.

Tópicos

- Custos
- Pré-requisitos
- Conectar automaticamente uma instância e um banco de dados
- Como a conexão é configurada automaticamente

Custos

Embora não haja cobrança para conectar automaticamente sua instância do EC2 a um banco de dados do RDS, você paga pelos serviços subjacentes. Taxas de transferência de dados serão aplicadas se sua instância do EC2 e o banco de dados do RDS estiverem em zonas de disponibilidade diferentes. Para obter informações, consulte a seção Transferência de dados na página Preço sob demanda do Amazon EC2.

Pré-requisitos

Antes de conectar automaticamente uma instância do EC2 a um banco de dados do RDS, verifique:

- As instâncias do EC2 devem estar no estado Running (Em execução). Não será possível conectar uma instância do EC2 se ela estiver em outro estado.
- As instâncias do EC2 e o banco de dados do RDS precisam estar na mesma nuvem privada virtual (VPC). Não há suporte para o recurso de conexão automática se a instância do EC2 e o banco de dados do RDS estiverem em VPCs diferentes.

Conectar automaticamente uma instância e um banco de dados

É possível conectar automaticamente uma instância do EC2 a um banco de dados do RDS logo após iniciar sua instância ou posteriormente.

Conectar automaticamente logo após a execução

Use as seguintes etapas para conectar automaticamente uma instância do EC2 a um banco de dados do RDS logo após a inicialização da instância do EC2.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS.

Para conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS usando o console do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do console, selecione Launch instances (Iniciar instâncias) e siga as etapas para iniciar uma instância.
3. Na página de confirmação de inicialização da instância, escolha Connect an RDS database (Conectar um banco de dados do RDS).
4. Na caixa de diálogo Connect RDS Database (Conectar banco de dados do RDS), faça o seguinte:

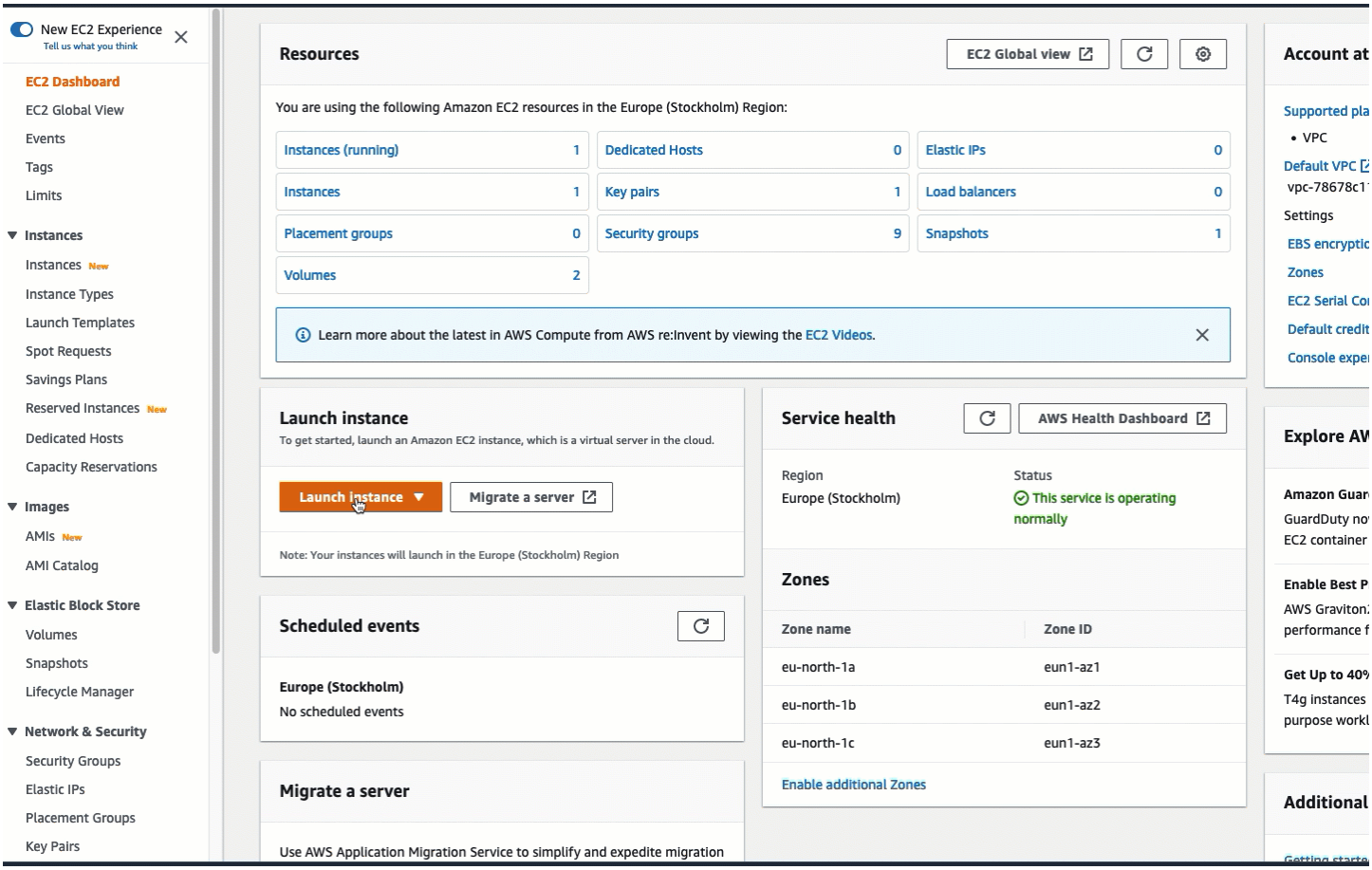
   a. Em Database role (Perfil de banco de dados), escolha Cluster ou Instance (Instância).

   b. Em RDS database (Banco de dados do RDS), selecione um banco de dados ao qual se conectar.

   > **Note**
   >
   > As instâncias do EC2 e o banco de dados do RDS devem estar na mesma VPC para se conectarem um ao outro.

   c. Selecione Conectar.

Visualizar uma animação: conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS



Conectar automaticamente uma instância existente

Use as seguintes etapas para conectar automaticamente uma instância do EC2 existente a um banco de dados do RDS.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: conectar automaticamente uma instância do EC2 existente a um banco de dados do RDS.

Para conectar automaticamente uma instância do EC2 existente a um banco de dados do RDS usando o console do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma ou mais instâncias do EC2 para se conectar a um banco de dados do RDS e escolha Actions (Ações), Networking (Redes), Connect RDS database (Conectar banco de dados do RDS).

Se Connect RDS database (Conectar banco de dados do RDS) não estiver disponível, verifique se as instâncias do EC2 estão no estado Running (Em execução) e se estão na mesma VPC.

4. Na caixa de diálogo Connect RDS Database (Conectar banco de dados do RDS), faça o seguinte:

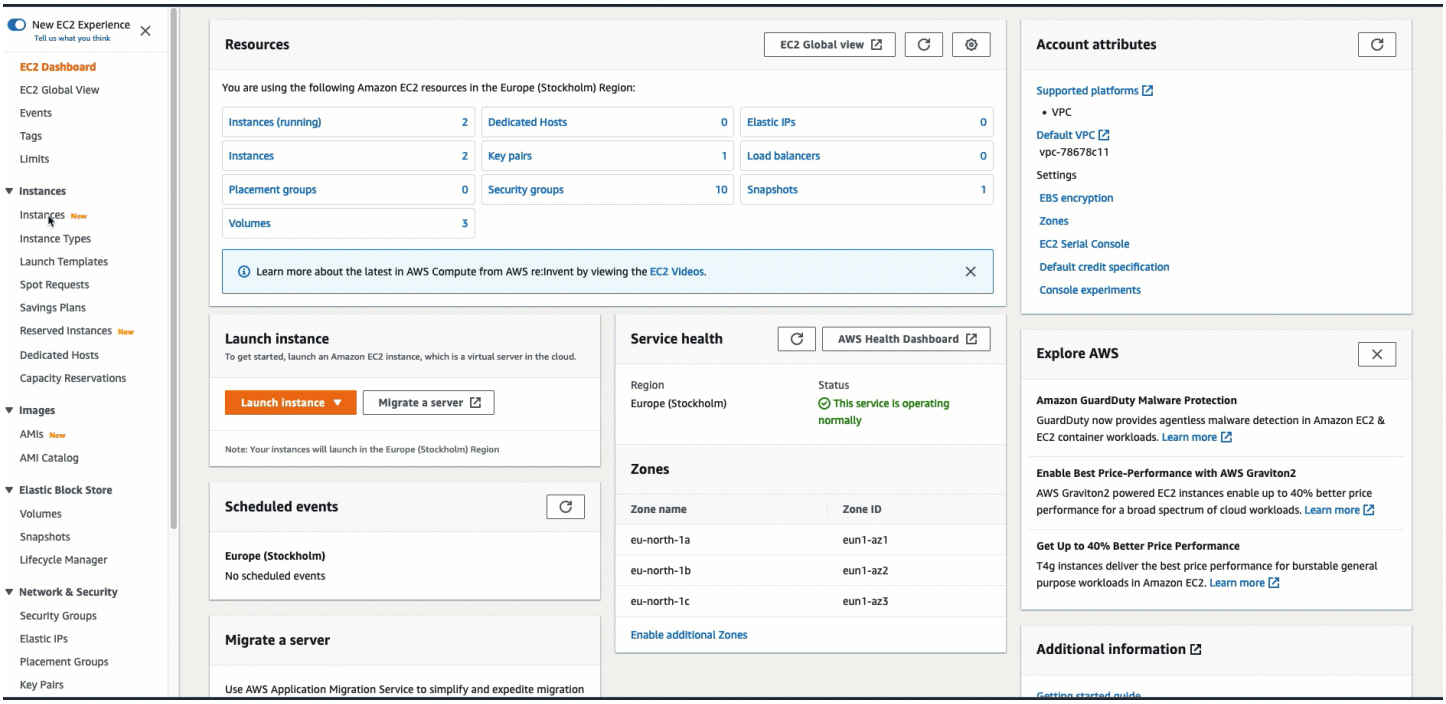
   a. Em Database role (Perfil de banco de dados), escolha Cluster ou Instance (Instância).

   b. Em RDS database (Banco de dados do RDS), selecione um banco de dados ao qual se conectar.

   > **Note**
   >
   > As instâncias do EC2 e o banco de dados do RDS devem estar na mesma VPC para se conectarem um ao outro.

   c. Selecione Conectar.

Visualizar uma animação: conectar automaticamente uma instância do EC2 existente a um banco de dados do RDS



Para obter informações sobre como usar o console do Amazon RDS para conectar automaticamente uma instância do EC2 a um banco de dados do RDS, consulte Configurar a conectividade automática de rede com uma instância do EC2 no Guia do usuário do Amazon RDS.

Como a conexão é configurada automaticamente

Quando se utiliza o console do EC2 para configurar automaticamente a conexão entre uma instância do EC2 e um banco de dados do RDS para permitir o tráfego entre eles, a conexão é configurada por grupos de segurança.

Os grupos de segurança são criados automaticamente e adicionados à instância do EC2 e ao banco de dados do RDS, da seguinte forma:

- O Amazon EC2 cria um grupo de segurança chamado ec2-rds-*x* e o adiciona à instância do EC2. Ele tem uma regra de saída que permite o tráfego para o banco de dados especificando rds-ec2-*x* (o grupo de segurança do banco de dados) como destino.
- O Amazon RDS cria um grupo de segurança chamado rds-ec2-*x* e o adiciona ao banco de dados. Ela tem uma regra de entrada que permite o tráfego da instância do EC2 especificando ec2-rds-*x* (o grupo de segurança da instância do EC2) como origem.

Os grupos de segurança referenciam uns aos outros como destino e origem e permitem somente tráfego na porta do banco de dados. É possível reutilizar esses grupos de segurança de modo que qualquer banco de dados que tenha o grupo de segurança rds-ec2-*x* possa se comunicar com qualquer instância do EC2 que tenha o grupo de segurança ec2-rds-*x*.

O nome dos grupos de segurança segue um padrão. Para os grupos de segurança criados pelo Amazon EC2, o padrão é ec2-rds-*x*; para os grupos de segurança criados pelo Amazon RDS, o padrão é rds-ec2-*x*. *x* é um número, que aumenta em 1 toda vez que um novo grupo de segurança é criado automaticamente.

Tutorial: conectar uma instância do Amazon EC2 a um banco de dados do Amazon RDS

Objetivo do tutorial

O objetivo deste tutorial é aprender a configurar a conexão entre uma instância do Amazon EC2 e um banco de dados do Amazon RDS usando o AWS Management Console.

Há diferentes opções para configurar a conexão. Neste tutorial, vamos explorar estas três opções:

- Opção 1: conectar automaticamente a instância do EC2 ao banco de dados do RDS usando o console do EC2

  Use o recurso de conexão automática do console do EC2 para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS.

- Opção 2: conectar automaticamente a instância do EC2 ao banco de dados do RDS usando o console do RDS

  Use o recurso de conexão automática do console do RDS para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS.

- Opção 3: conectar manualmente a instância do EC2 ao banco de dados do RDS imitando o recurso de conexão automática

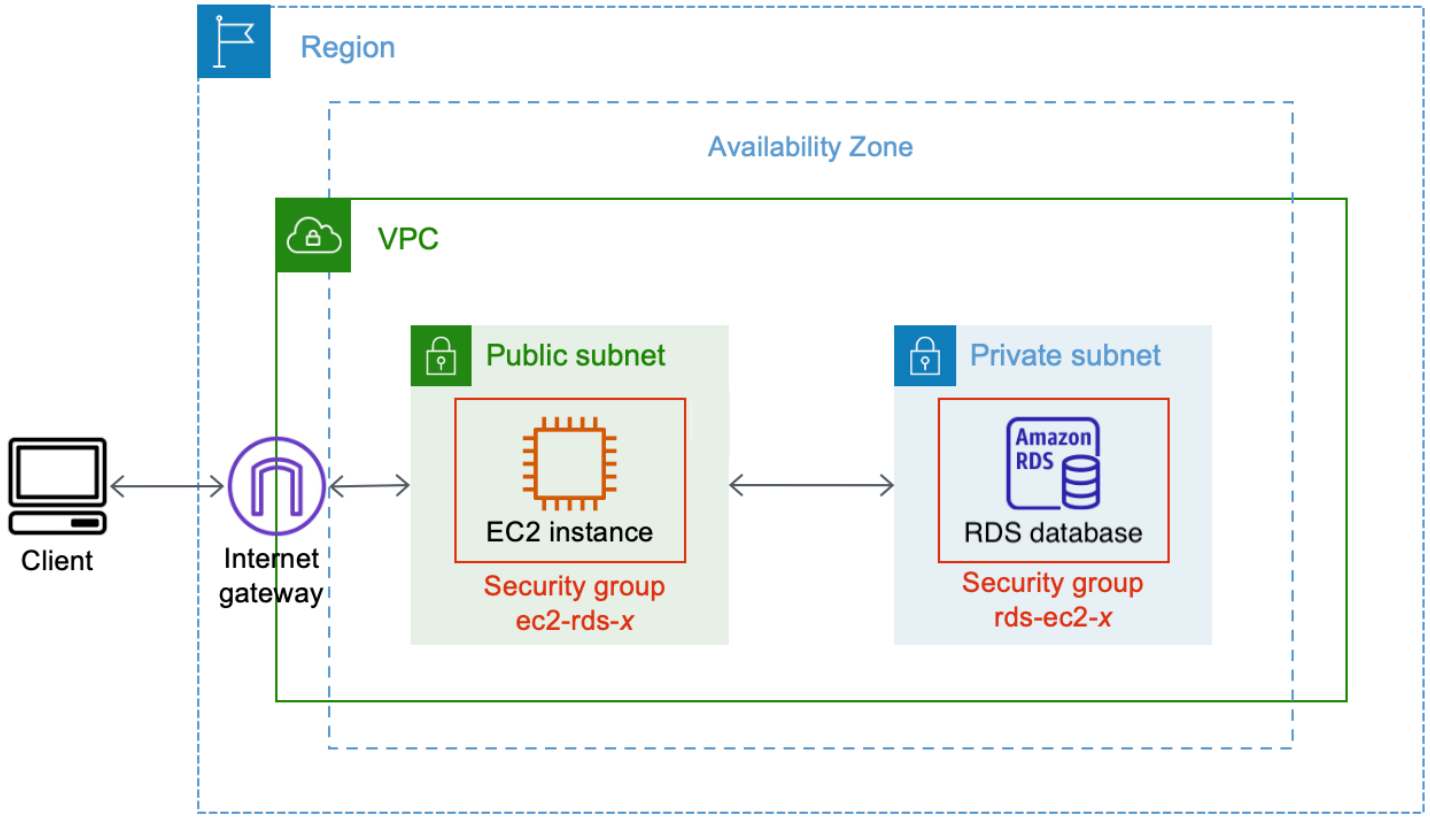
  Configure a conexão entre a instância do EC2 e o banco de dados do RDS configurando e atribuindo manualmente os grupos de segurança para reproduzir a configuração criada automaticamente pelo recurso de conexão automática na opção 1 e na opção 2.

Contexto

Como contexto do motivo para configurar uma conexão entre a instância do EC2 e um banco de dados do RDS, vamos considerar o seguinte cenário: seu site apresenta um formulário para os usuários preencherem. É necessário captar os dados do formulário em um banco de dados. Você pode hospedar o site em uma instância do EC2 que foi configurada como servidor Web e captar os dados do formulário em um banco de dados do RDS. A instância do EC2 e o banco de dados do RDS precisam estar conectados entre si para que os dados do formulário possam sair da instância do EC2 para o banco de dados do RDS. Este tutorial explica como configurar a conexão. Este é apenas um exemplo de um caso de uso para conectar uma instância do EC2 e um banco de dados do RDS.

Arquitetura

O diagrama a seguir mostra os recursos criados e a configuração arquitetônica resultante da conclusão de todas as etapas deste tutorial.



O diagrama ilustra os seguintes recursos que você criará:

- Você criará uma instância do EC2 e um banco de dados do RDS na mesma Região da AWS, VPC e zona de disponibilidade.
- Você criará a instância do EC2 em uma sub-rede pública.
- Você criará o banco de dados do RDS em uma sub-rede privada.

  Ao usar o console do RDS para criar o banco de dados do RDS e conectar automaticamente a instância do EC2, a VPC, o grupo de sub-redes de banco de dados e as configurações de acesso público para o banco de dados são selecionados automaticamente. O banco de dados do RDS é criado automaticamente em uma sub-rede privada na mesma VPC da instância do EC2.
- Os usuários da Internet podem se conectar à instância do EC2 usando SSH ou HTTP/HTTPS por um gateway da Internet.
- Os usuários da Internet não podem se conectar diretamente ao banco de dados do RDS, apenas a instância do EC2 está conectada ao banco de dados do RDS.
- Quando você usa o recurso de conexão automática para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS, estes grupos de segurança são automaticamente criados e adicionados:

- O grupo de segurança ec2-rds-*x* é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-*x* como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-*x*.
- O grupo de segurança rds-ec2-*x* é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-*x* como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-*x* atinja o banco de dados do RDS.

Ao usar grupos de segurança separados (um para a instância do EC2 e outro para o banco de dados do RDS), você tem mais controle sobre a segurança da instância e do banco de dados. Se você usasse o mesmo grupo de segurança na instância e no banco de dados e depois modificasse o grupo de segurança para se adequar, digamos, somente ao banco de dados, a modificação afetaria tanto a instância como o banco de dados. Em outras palavras, se usasse um grupo de segurança, você poderia modificar involuntariamente a segurança de um recurso (instância ou banco de dados) porque esqueceu que o grupo de segurança estava anexado a ele.

Os grupos de segurança criados automaticamente também respeitam o privilégio mínimo, pois permitem somente a conexão mútua para essa workload na porta do banco de dados, criando um par de grupos de segurança específico da workload.

Considerações

Considere o seguinte ao concluir as tarefas deste tutorial:

- Dois consoles: você usará estes dois consoles neste tutorial:
  - Console do Amazon EC2: você usará o console do EC2 para iniciar instâncias, conectar automaticamente uma instância do EC2 a um banco de dados do RDS e para a opção manual de configurar a conexão criando os grupos de segurança.
  - Console do Amazon RDS: você usará o console do RDS para criar um banco de dados do RDS e conectar automaticamente uma instância do EC2 a um banco de dados do RDS.
- Uma VPC: para usar o recurso de conexão automática, a instância do EC2 e o banco de dados do RDS devem estar na mesma VPC.

  Se você configurasse manualmente a conexão entre a instância do EC2 e o banco de dados do RDS, poderia iniciar a instância do EC2 em uma VPC e o banco de dados do RDS em outra VPC,

mas precisaria definir uma configuração adicional de encaminhamento e VPC. Este cenário não é abordado neste tutorial.

- Uma Região da AWS: a instância do EC2 e o banco de dados do RDS devem estar localizados na mesma região.
- Dois grupos de segurança: a conectividade entre a instância do EC2 e o banco de dados do RDS é configurada por dois grupos de segurança, um grupo de segurança para a instância do EC2 e um grupo de segurança para o banco de dados do RDS.

  Quando você usa o recurso de conexão automática no console do EC2 ou no console do RDS para configurar a conectividade (opção 1 e opção 2 deste tutorial), os grupos de segurança são criados automaticamente e atribuídos à instância do EC2 e ao banco de dados do RDS.

  Se você não usar o recurso de conexão automática, será necessário criar e atribuir os grupos de segurança manualmente. Faça isso na opção 3 deste tutorial.

É hora de concluir o tutorial

30 minutos

Você pode concluir o tutorial inteiro de uma só vez ou pode realizar uma tarefa por vez.

Custos

Ao concluir este tutorial, você poderá incorrer em custos para os recursos da AWS criados.

É possível usar o Amazon EC2 no nível gratuito, desde que a conta da AWS tenha menos de 12 meses e que seus recursos estejam configurados de acordo com os requisitos do nível gratuito.

Se sua instância do EC2 e o banco de dados do RDS estiverem em zonas de disponibilidade diferentes, serão aplicadas taxas de transferências de dados. Para evitar que essas taxas estejam aplicadas, a instância do EC2 e o banco de dados do RDS devem estar na mesma zona de disponibilidade. Para obter informações, consulte a seção Transferência de dados na página Preço sob demanda do Amazon EC2.

Para evitar custos após a conclusão do tutorial, exclua os recursos, caso eles não sejam mais necessários. Para saber as etapas para excluir os recursos, consulte Limpeza.

Opção 1: conectar automaticamente a instância do EC2 ao banco de dados do RDS usando o console do EC2

Objetivo

O objetivo da opção 1 é explorar o recurso de conexão automática do console do EC2 que configura automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego da instância do EC2 para o banco de dados do RDS. Na opção 3, você aprenderá a configurar a conexão manualmente.

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Um banco de dados do RDS que está na mesma VPC da instância do EC2. Você pode usar um banco de dados RDS existente ou seguir as etapas na tarefa 1 para criar um novo banco de dados do RDS.
- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. Você pode usar uma instância do EC2 existente ou seguir as etapas na tarefa 2 para criar uma nova instância do EC2.
- Permissões para chamar estas operações:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tarefas para concluir a opção 1

- Tarefa 1: criar um banco de dados do RDS (opcional)

- Tarefa 2: iniciar uma instância do EC2 (opcional)
- Tarefa 3: conectar automaticamente a instância do EC2 ao banco de dados do RDS
- Tarefa 4: verificar a configuração da conexão

Tarefa 1: criar um banco de dados do RDS (opcional)

> **Note**
>
> O foco deste tutorial não é criar um banco de dados do Amazon RDS. Se você já tiver um banco de dados do RDS e quiser usá-lo neste tutorial, poderá ignorar esta tarefa.

Objetivo da tarefa

O objetivo desta tarefa é criar um banco de dados do RDS para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do RDS. Se você tiver um banco de dados do RDS que possa usar, pode ignorar esta tarefa.

> **Important**
>
> Se usar um banco de dados do RDS existente, certifique-se de que ele esteja na mesma VPC da instância do EC2 para poder usar o recurso de conexão automática.

Etapas para criar um banco de dados do RDS

Use as seguintes etapas para criar um banco de dados do RDS.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: criar um banco de dados do RDS.

Configuração de banco de dados do RDS

As etapas desta tarefa configuram o banco de dados do RDS da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database-1`**
- Classe da instância de banco de dados: `db.t3.micro`

> **Important**
>
> Para um ambiente de produção, é necessário configurar o banco de dados para atender às suas necessidades específicas.

Para criar um banco de dados MySQL RDS

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha uma Região da AWS. O banco de dados e a instância do EC2 devem estar na mesma região para usar o recurso de conexão automática no console do EC2.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), verifique se a opção Standard Create (Criação padrão) está selecionada. Se você escolher Easy create (Criação fácil), o seletor VPC não estará disponível. Verifique se o banco de dados está na mesma VPC da sua instância do EC2 para usar o recurso de conexão automática no console do EC2.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em Templates (Modelos), escolha um modelo de exemplo que atenda às suas necessidades. Neste tutorial, escolha o Free tier (Nível gratuito) para criar um banco de dados sem nenhum custo. Porém, o nível gratuito estará disponível somente se a conta tiver menos de 12 meses. Aplicam-se outras restrições. Você pode ler mais escolhendo o link Info (Informações) na caixa Free tier (Nível gratuito).
7. Em Configurações, faça o seguinte:
   a. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados. Para este tutorial, insira **`tutorial-database-1`**.
   b. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **`admin`**.
   c. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.
8. Em Instance configuration (Configuração da instância), em DB instance class (Classe de instância de banco de dados), deixe o padrão, que é db.t3.micro. Se a conta tiver menos de

12 meses, você poderá usar essa classe de banco de dados gratuitamente. Aplicam-se outras restrições. Para obter mais informações, consulte Nível gratuito da AWS.

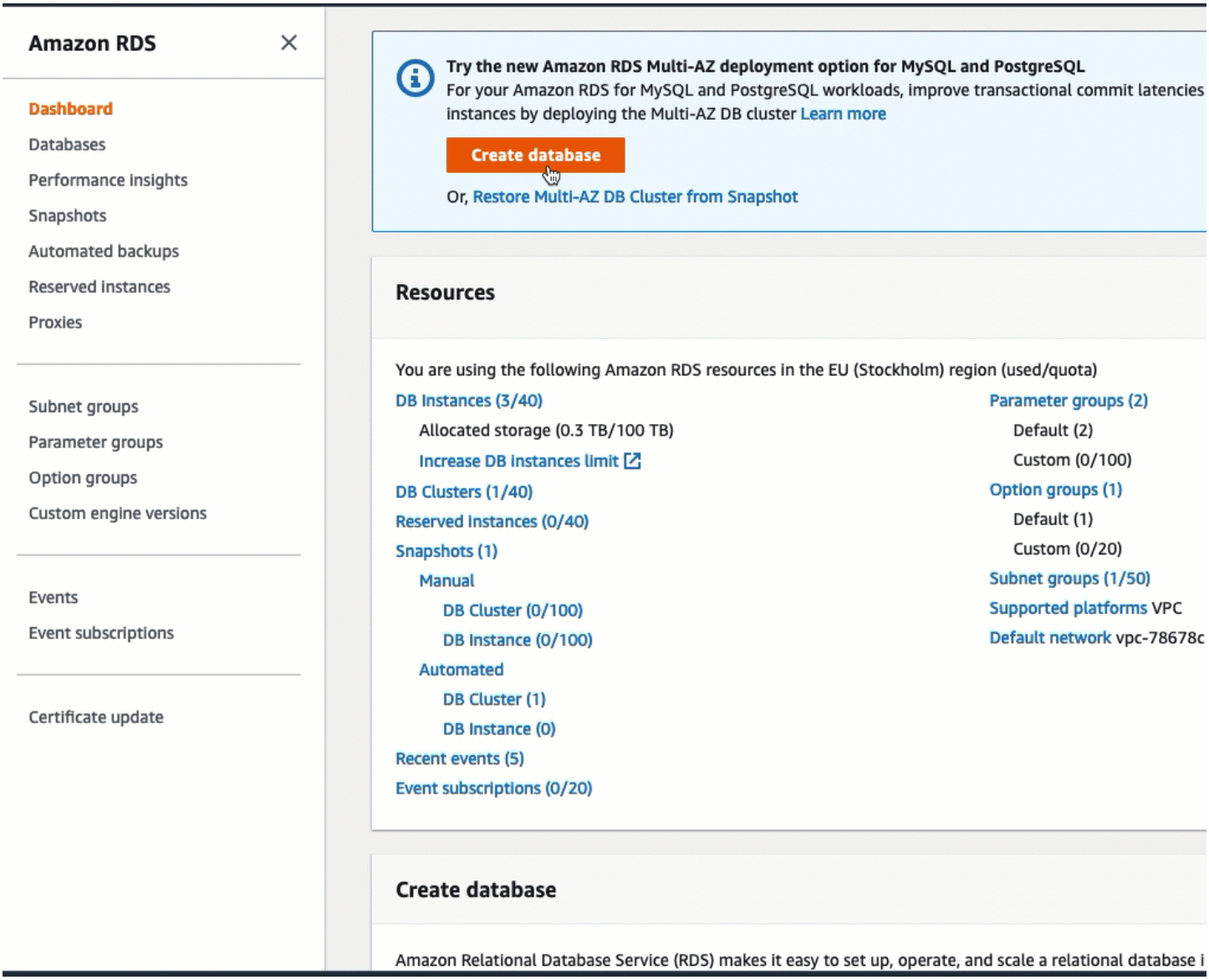
9. Em Connectivity (Conectividade), em Compute resource (Recurso de computação), escolha Don't connect to an EC2 compute resource (Não se conectar a um recurso computacional do EC2), pois você conectará a instância do EC2 e o banco de dados do RDS posteriormente na tarefa 3.

   (Posteriormente, na opção 2 deste tutorial, você experimentará o recurso de conexão automática no console do RDS escolhendo Connect to an EC2 compute resource [Conectar a um recurso computacional do EC2].)

10. Em Virtual private cloud (VPC) (Nuvem privada virtual [VPC]), selecione uma VPC. A VPC deve ter um grupo de sub-redes de banco de dados. Para usar o recurso de conexão automática, a instância do EC2 e o banco de dados do RDS devem estar na mesma VPC.
11. Mantenha os valores padrão para os outros campos desta página.
12. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status do novo banco de dados é Creating (Criando) até que o banco de dados esteja pronto para uso. Quando o status mudar para Available (Disponível), será possível conectar-se ao banco de dados. Dependendo da classe de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que o novo banco de dados esteja disponível.

Visualizar uma animação: criar um banco de dados do RDS



Agora está tudo pronto para Tarefa 2: iniciar uma instância do EC2 (opcional).

Tarefa 2: iniciar uma instância do EC2 (opcional)

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.

Objetivo da tarefa

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS. Se você tiver uma instância do EC2 que possa usar, pode ignorar esta tarefa.

> **Important**
>
> Se usar uma instância do EC2 existente, certifique-se de que ela esteja na mesma VPC do banco de dados do RDS para poder usar o recurso de conexão automática.

Etapas para iniciar uma instância do EC2

Para iniciar uma instância do EC2, use as seguintes etapas.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: iniciar uma instância do EC2.

Configuração de instância do EC2

As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No seletor Region (Região), no canto superior direito, escolha uma Região da AWS. A instância e o banco de dados do RDS devem estar na mesma região para usar o recurso de conexão automática no console do EC2.
3. No painel do EC2, escolha Launch Instance (Iniciar instância).
4. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-1`**. Embora o nome da instância não seja obrigatório, ao selecionar a instância no console do EC2, o nome ajudará você a identificá-la facilmente.
5. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux 2.
6. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

   > **Note**
   >
   > É possível usar o Amazon EC2 no nível gratuito, desde que a conta da AWS tenha menos de 12 meses e que você tenha escolhido um tipo de instância `t2.micro` (ou `t3.micro` em regiões onde `t2.micro` não esteja disponível).

7. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
8. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

      Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

      i. A instância do EC2 e o banco de dados do RDS devem estar na mesma VPC para usar o recurso de conexão automática. Por padrão, você tem apenas uma VPC.

      ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

   Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (security groups) (Firewall [grupos de segurança]), na lista suspensa ao lado da caixa de seleção Allow SSH traffic from (Permitir tráfego SSH de), escolha My IP (Meu IP).

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

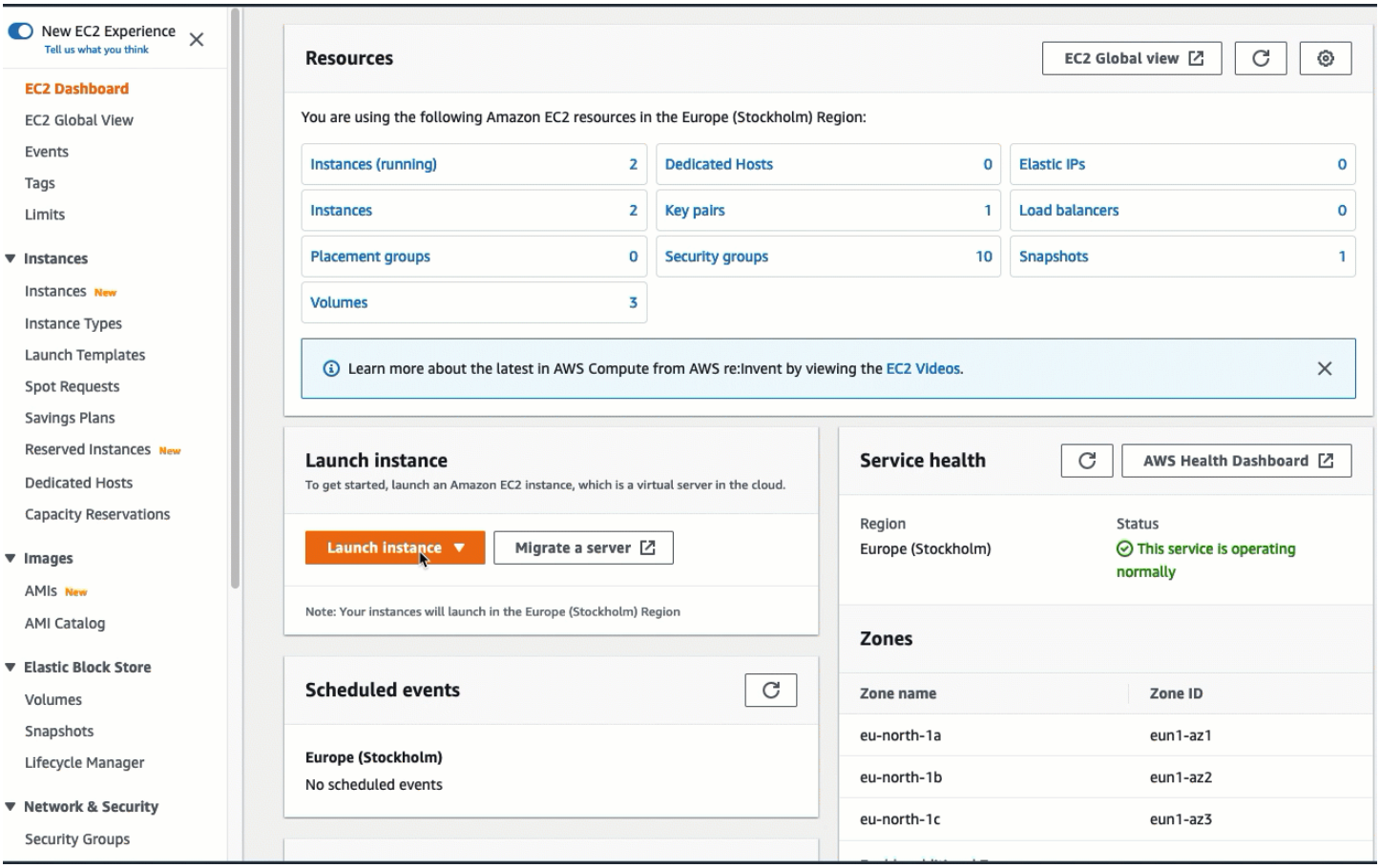
   - Permitir tráfego HTTPs da Internet
   - Permitir tráfego HTTP da Internet

9. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
10. Deixe a página de confirmação aberta. Você precisará dela na próxima tarefa ao conectar automaticamente a instância ao banco de dados.

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Visualizar uma animação: iniciar uma instância do EC2



Agora está tudo pronto para Tarefa 3: conectar automaticamente a instância do EC2 ao banco de dados do RDS.

Tarefa 3: conectar automaticamente a instância do EC2 ao banco de dados do RDS

Objetivo da tarefa

O objetivo desta tarefa é usar o recurso de conexão automática no console do EC2 para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS.

Etapas para conectar sua instância do EC2 e o banco de dados do RDS

Use as seguintes etapas para conectar a instância do EC2 e o banco de dados do RDS usando o recurso automático no console do EC2.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS.

Para conectar automaticamente uma instância do EC2 a um banco de dados do RDS usando o console do EC2

1. Na página de confirmação de inicialização da instância (ela deve ser aberta na tarefa anterior), escolha Connect an RDS database (Conectar um banco de dados do RDS).

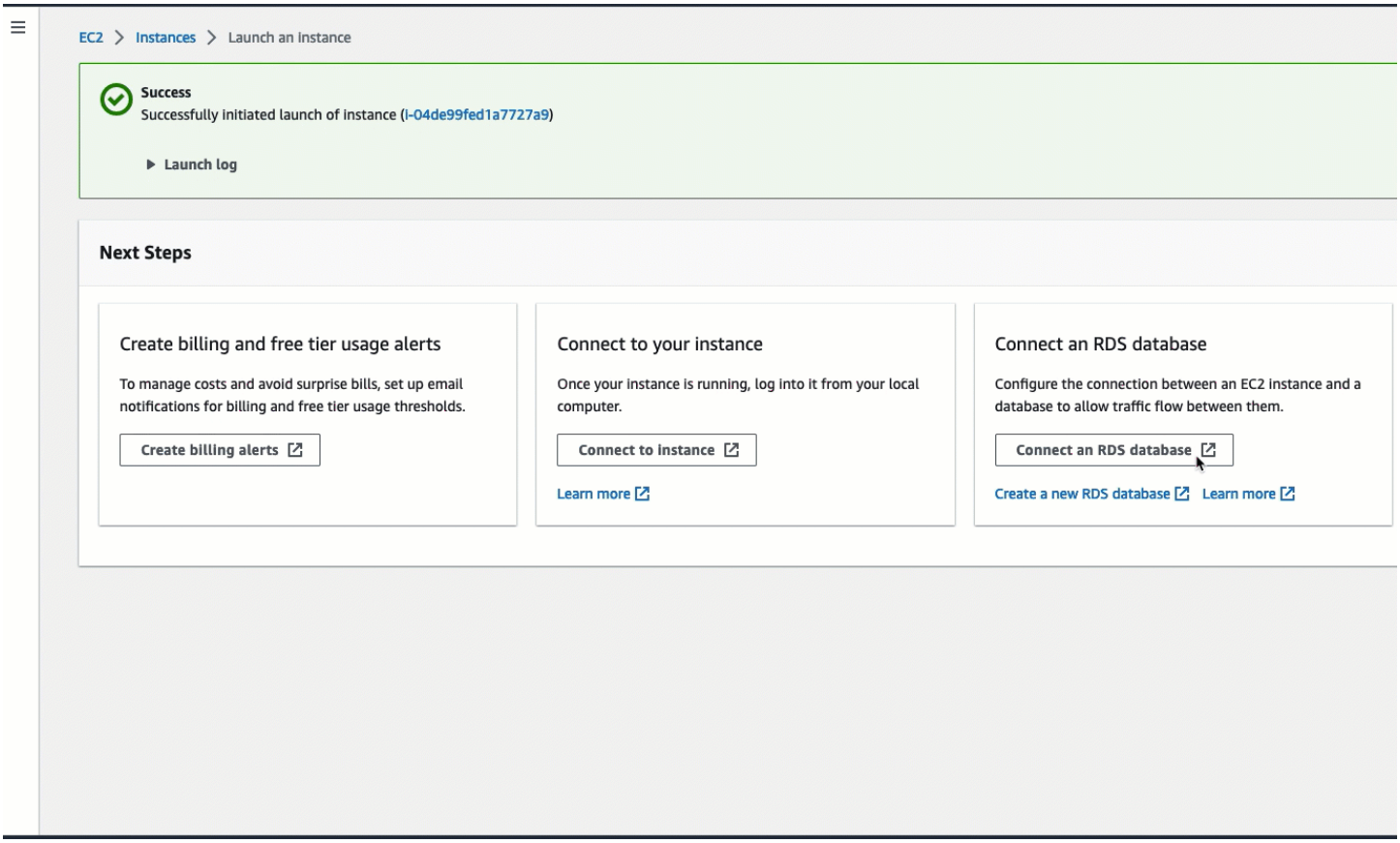
   Se você fechou a página de confirmação, siga estas etapas:

   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. No painel de navegação, escolha Instances (Instâncias).
   c. Selecione a instância do EC2 que você acabou de criar e escolha Actions (Ações), Networking (Redes), Connect RDS database (Conectar banco de dados do RDS).

      Se Connect RDS database (Conectar banco de dados do RDS) não estiver disponível, verifique se a instância do EC2 está no estado Running (Em execução).
2. Em Database role (Perfil de banco de dados), escolha Instance (Instância). Nesse caso, Instance (Instância) refere-se à instância do banco de dados.
3. Em RDS database (Banco de dados do RDS), escolha o banco de dados do RDS que você criou na tarefa 1.

   > **Note**
   >
   > A instância do EC2 e o banco de dados do RDS devem estar na mesma VPC para se conectarem um ao outro.
4. Selecione Conectar.

Visualizar uma animação: conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS



Agora está tudo pronto para Tarefa 4: verificar a configuração da conexão.

Tarefa 4: verificar a configuração da conexão

Objetivo da tarefa

O objetivo desta tarefa é verificar se os dois grupos de segurança foram criados e atribuídos à instância e ao banco de dados.

Quando você usa o recurso de conexão automática no console do EC2 para configurar a conectividade, os grupos de segurança são criados automaticamente e atribuídos à instância e ao banco de dados, da seguinte forma:

- O grupo de segurança rds-ec2-***x*** é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-***x*** como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-***x*** atinja o banco de dados do RDS.

- O grupo de segurança ec2-rds-*x* é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-*x* como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-*x*.

Etapas para verificar a configuração da conexão

Use as seguintes etapas para verificar a configuração da conexão.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: verificar a configuração da conexão.

Para verificar a configuração da conexão usando o console

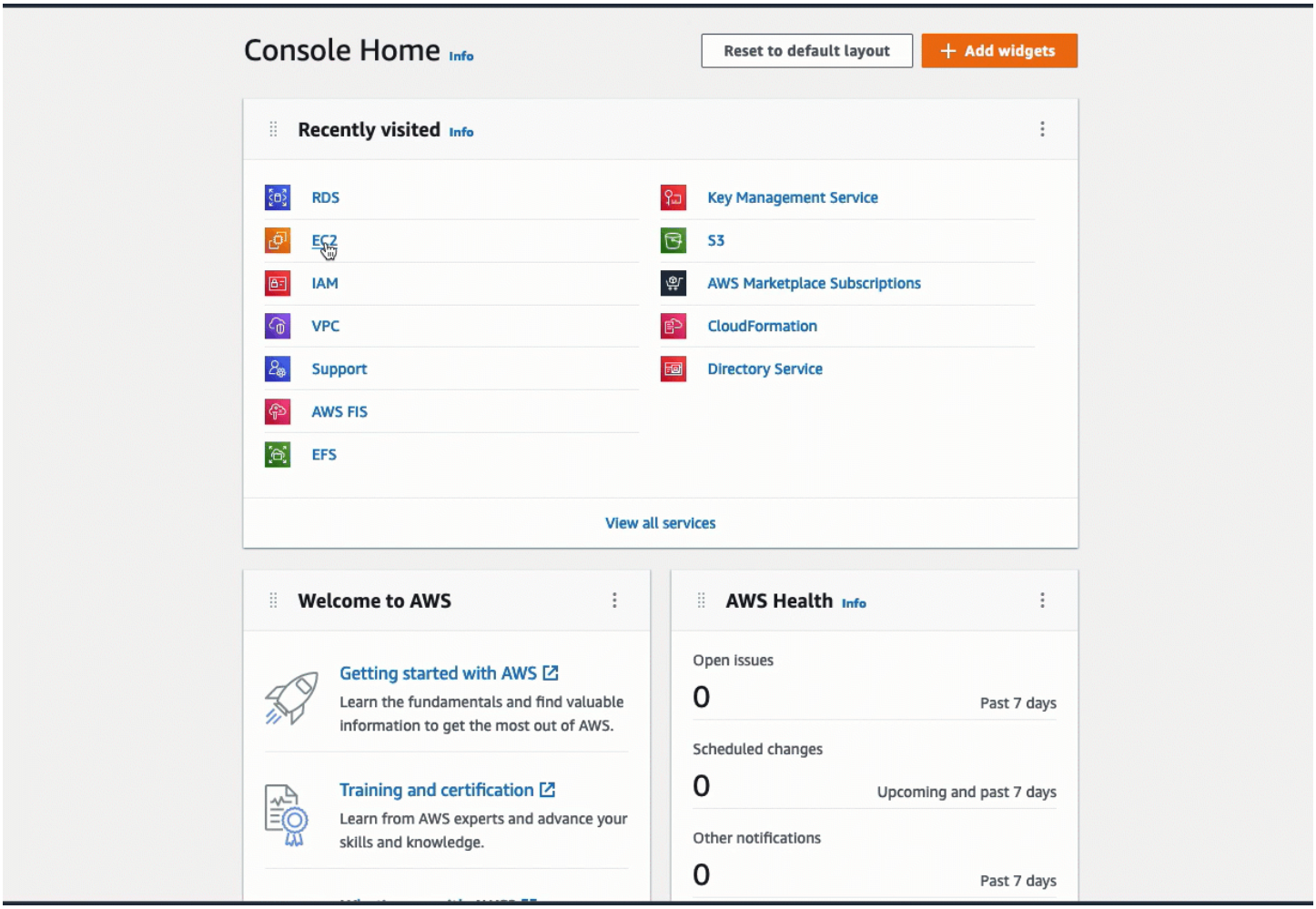
1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. Na página de navegação, escolha Databases (Bancos de dados).
3. Escolha o banco de dados do RDS que você criou para este tutorial.
4. Na guia Connectivity and security (Conectividade e segurança), em Security (Segurança), VPC security groups (Grupos de segurança da VPC), verifique se um grupo de segurança chamado rds-ec2-*x* está sendo exibido.
5. Escolha o grupo de segurança rds-ec2-*x*. A tela Security Groups (Grupos de segurança) no console do EC2 é aberta.
6. Escolha o grupo de segurança rds-ec2-*x* para abrir.
7. Escolha a guia Regras de entrada.
8. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:
   - Digite: MySQL/Aurora
   - Intervalo de porta: 3306
   - Origem: ***sg-0987654321example*** / ec2-rds-*x*: este é o grupo de segurança atribuído à instância do EC2 que você verificou nas etapas anteriores.
   - Descrição: regra para permitir conexões de instâncias do EC2 com ***sg-1234567890example*** anexado
9. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
10. No painel de navegação, escolha Instances (Instâncias).
11. Escolha a instância do EC2 que você selecionou para se conectar ao banco de dados do RDS na tarefa anterior e escolha a guia Security (Segurança).

12. Em Security details (Detalhes de segurança), Security groups (Grupos de segurança), verifique se um grupo de segurança chamado ec2-rds-*x* está na lista. *x* é um número.
13. Escolha o grupo de segurança ec2-rds-*x* para abrir.
14. Escolha a guia Outbound rules (Regras de saída).
15. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:

    - Digite: MySQL/Aurora
    - Intervalo de porta: 3306
    - Destino: ***sg-1234567890example*** / rds-ec2-***x***
    - Descrição: regra para permitir conexões a **`database-tutorial`** de qualquer instância à qual esse grupo de segurança esteja vinculado

Ao verificar se esses grupos de segurança e regras de grupos de segurança existem e se estão atribuídos ao banco de dados do RDS e à instância do EC2, conforme descrito neste procedimento, você pode verificar se a conexão foi configurada automaticamente usando o recurso de conexão automática.

Visualizar uma animação: verificar a configuração da conexão



Você concluiu a opção 1 deste tutorial. Agora você pode concluir a opção 2, que ensina a usar o console do RDS para conectar automaticamente uma instância do EC2 a um banco de dados do RDS, ou pode concluir a opção 3, que ensina a configurar manualmente os grupos de segurança que foram criados automaticamente na opção 1.

Opção 2: conectar automaticamente a instância do EC2 ao banco de dados do RDS usando o console do RDS

Objetivo

O objetivo da opção 2 é explorar o recurso de conexão automática do console do RDS que configura automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego da instância do EC2 para o banco de dados do RDS. Na opção 3, você aprenderá a configurar a conexão manualmente.

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. Você pode usar uma instância do EC2 existente ou seguir as etapas na tarefa 1 para criar uma nova instância.
- Permissões para chamar estas operações:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tarefas para concluir a opção 2

- Tarefa 1: iniciar uma instância do EC2 (opcional)
- Tarefa 2: criar um banco de dados do RDS e conectá-lo automaticamente à instância do EC2
- Tarefa 3: verificar a configuração da conexão

Tarefa 1: iniciar uma instância do EC2 (opcional)

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.

Objetivo da tarefa

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 2, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS. Se você tiver uma instância do EC2 que possa usar, pode ignorar esta tarefa.

Etapas para iniciar uma instância do EC2

Para iniciar uma instância do EC2, use as seguintes etapas.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: iniciar uma instância do EC2.

Configuração de instância do EC2

As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do EC2, escolha Launch Instance (Iniciar instância).
3. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-2`**. Embora o

nome da instância não seja obrigatório, quando você selecionar a instância no console do RDS, o nome o ajudará a identificá-la facilmente.

4. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

   > **Note**
   >
   > É possível usar o Amazon EC2 no nível gratuito, desde que a conta da AWS tenha menos de 12 meses e que você tenha escolhido um tipo de instância `t2.micro` (ou `t3.micro` em regiões onde `t2.micro` não esteja disponível).

6. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
7. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

      Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

      i. A instância e o banco de dados do RDS devem estar na mesma VPC para usar a configuração de conexão automática. Por padrão, você tem apenas uma VPC.

      ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

      iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

   b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (security groups) (Firewall [grupos de segurança]), na lista suspensa ao lado da caixa de seleção Allow SSH traffic from (Permitir tráfego SSH de), escolha My IP (Meu IP).

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

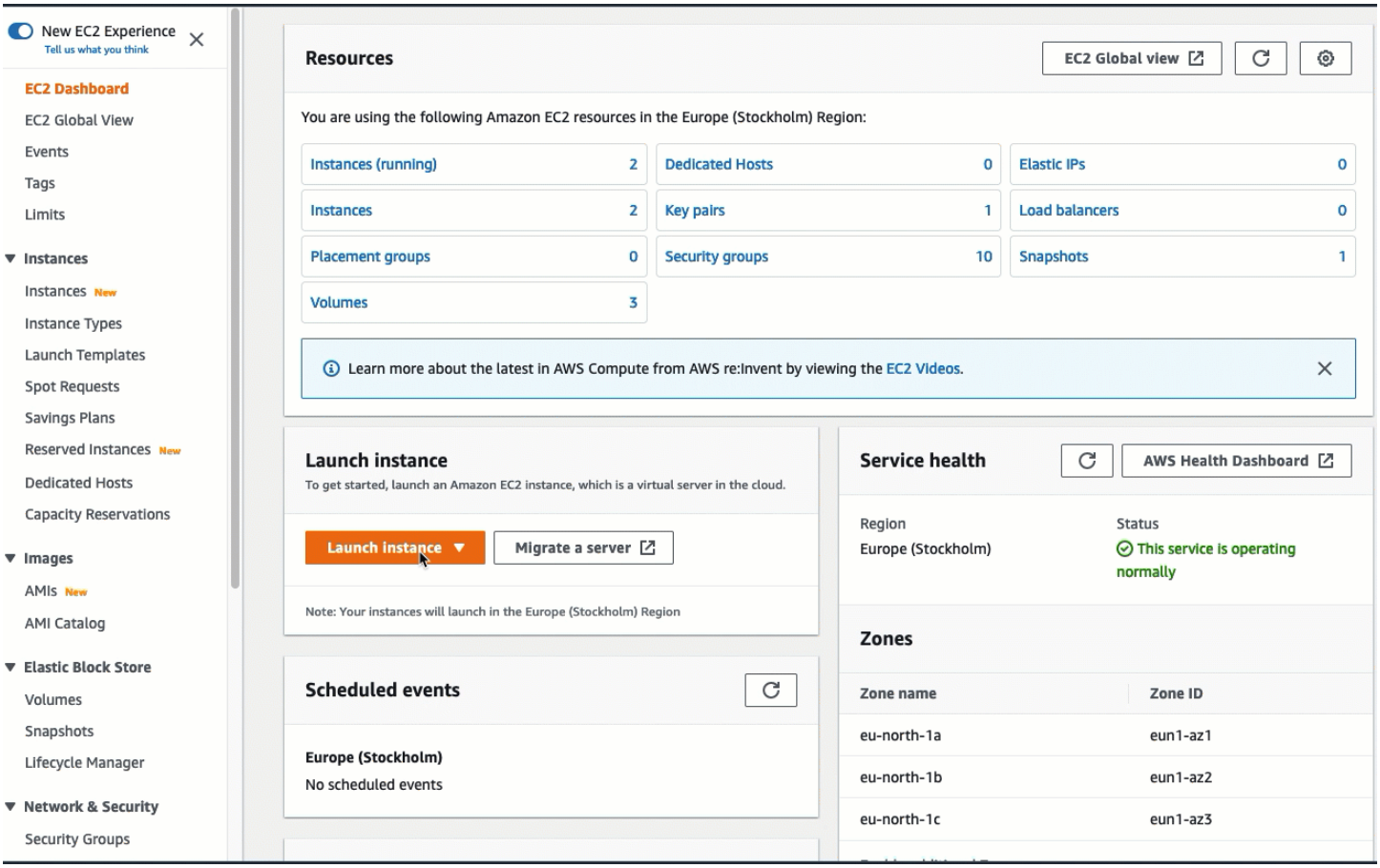
- Permitir tráfego HTTPs da Internet
- Permitir tráfego HTTP da Internet

8. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
9. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. Sua instância estará primeiro em um estado `pending` e depois entrará no estado `running`.

   Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Visualizar uma animação: iniciar uma instância do EC2



Agora está tudo pronto para Tarefa 2: criar um banco de dados do RDS e conectá-lo automaticamente à instância do EC2.

Tarefa 2: criar um banco de dados do RDS e conectá-lo automaticamente à instância do EC2

Objetivo da tarefa

O objetivo desta tarefa é criar um banco de dados do RDS e usar o recurso de conexão automática no console do RDS para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS.

Etapas para criar um banco de dados do RDS

Use as seguintes etapas para criar um banco de dados do RDS e conectá-lo à instância do EC2 usando o recurso automático no console do RDS.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: criar um banco de dados do RDS e conectar automaticamente a uma instância do EC2.

Configuração de instância de banco de dados

As etapas desta tarefa configuram a instância do banco de dados da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database`**
- Classe da instância de banco de dados: `db.t3.micro`

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para criar um banco de dados do RDS e conectá-lo automaticamente a uma instância do EC2

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha a Região da AWS na qual você criou a instância do EC2. A instância do EC2 e o banco de dados do RDS devem estar na mesma região.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), verifique se a opção Standard Create (Criação padrão) está selecionada. Se você escolher Easy create (Criação fácil), o recurso de conexão automática não estará disponível.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em Templates (Modelos), escolha um modelo de exemplo que atenda às suas necessidades. Neste tutorial, escolha o Free tier (Nível gratuito) para criar um banco de dados do RDS sem nenhum custo. Porém, o nível gratuito estará disponível somente se a conta tiver menos de 12 meses. Aplicam-se outras restrições. Você pode ler mais escolhendo o link Info (Informações) na caixa Free tier (Nível gratuito).
7. Em Configurações, faça o seguinte:

    a. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados. Para este tutorial, insira **`tutorial-database`**.

b. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **admin**.

c. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.

8. Em Instance configuration (Configuração da instância), em DB instance class (Classe de instância de banco de dados), deixe o padrão, que é db.t3.micro. Se a conta tiver menos de 12 meses, você poderá usar essa instância gratuitamente. Aplicam-se outras restrições. Para obter mais informações, consulte Nível gratuito da AWS.

9. Em Connectivity (Conectividade), para Compute resource (Recurso de computação), escolha Connect to an EC2 compute resource (Conectar-se a um recurso de computação do EC2). Esse é o recurso de conexão automática no console do RDS.

10. Em EC2 instance (Instância do EC2), selecione o nome da instância à qual você deseja se conectar. Para os fins deste tutorial, você pode escolher a instância criada na tarefa anterior, chamada **tutorial-instance**, ou escolher outra instância existente. Caso não veja sua instância na lista, escolha o ícone de atualização à direita de Connectivity (Conectividade).

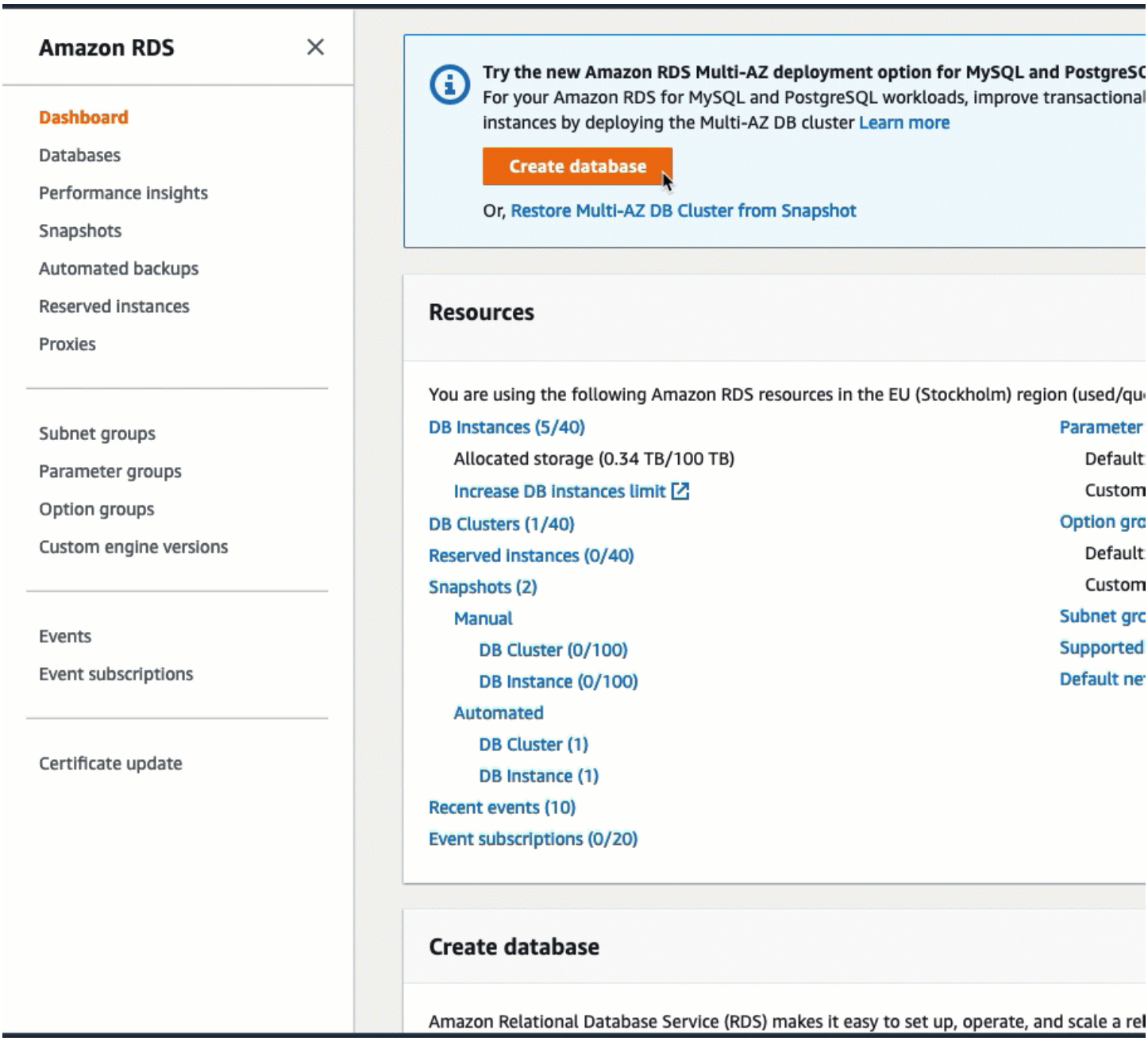
    Quando você usa o recurso de conexão automática, um grupo de segurança é adicionado a essa instância do EC2, e outro grupo de segurança é adicionado ao banco de dados do RDS. Os grupos de segurança são configurados automaticamente para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS. Na próxima tarefa, você verificará se os grupos de segurança foram criados e atribuídos à instância do EC2 e ao banco de dados do RDS.

11. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status do novo banco de dados é Creating (Criando) até que o banco de dados esteja pronto para uso. Quando o status mudar para Available (Disponível), será possível conectar-se ao banco de dados. Dependendo da classe de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que o novo banco de dados esteja disponível.

Para saber mais, consulte Configurar a conectividade automática de rede com uma instância do EC2 no Guia do usuário do Amazon RDS.

Visualizar uma animação: criar um banco de dados do RDS e conectar automaticamente a uma instância do EC2



Agora está tudo pronto para Tarefa 3: verificar a configuração da conexão.

Tarefa 3: verificar a configuração da conexão

Objetivo da tarefa

O objetivo desta tarefa é verificar se os dois grupos de segurança foram criados e atribuídos à instância e ao banco de dados.

Quando você usa o recurso de conexão automática no console do RDS para configurar a conectividade, os grupos de segurança são criados automaticamente e atribuídos à instância e ao banco de dados, da seguinte forma:

- O grupo de segurança rds-ec2-***x*** é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-***x*** como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-***x*** atinja o banco de dados do RDS.
- O grupo de segurança ec2-rds-***x*** é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-***x*** como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-***x***.

Etapas para verificar a configuração da conexão

Use as seguintes etapas para verificar a configuração da conexão.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: verificar a configuração da conexão.

Para verificar a configuração da conexão usando o console

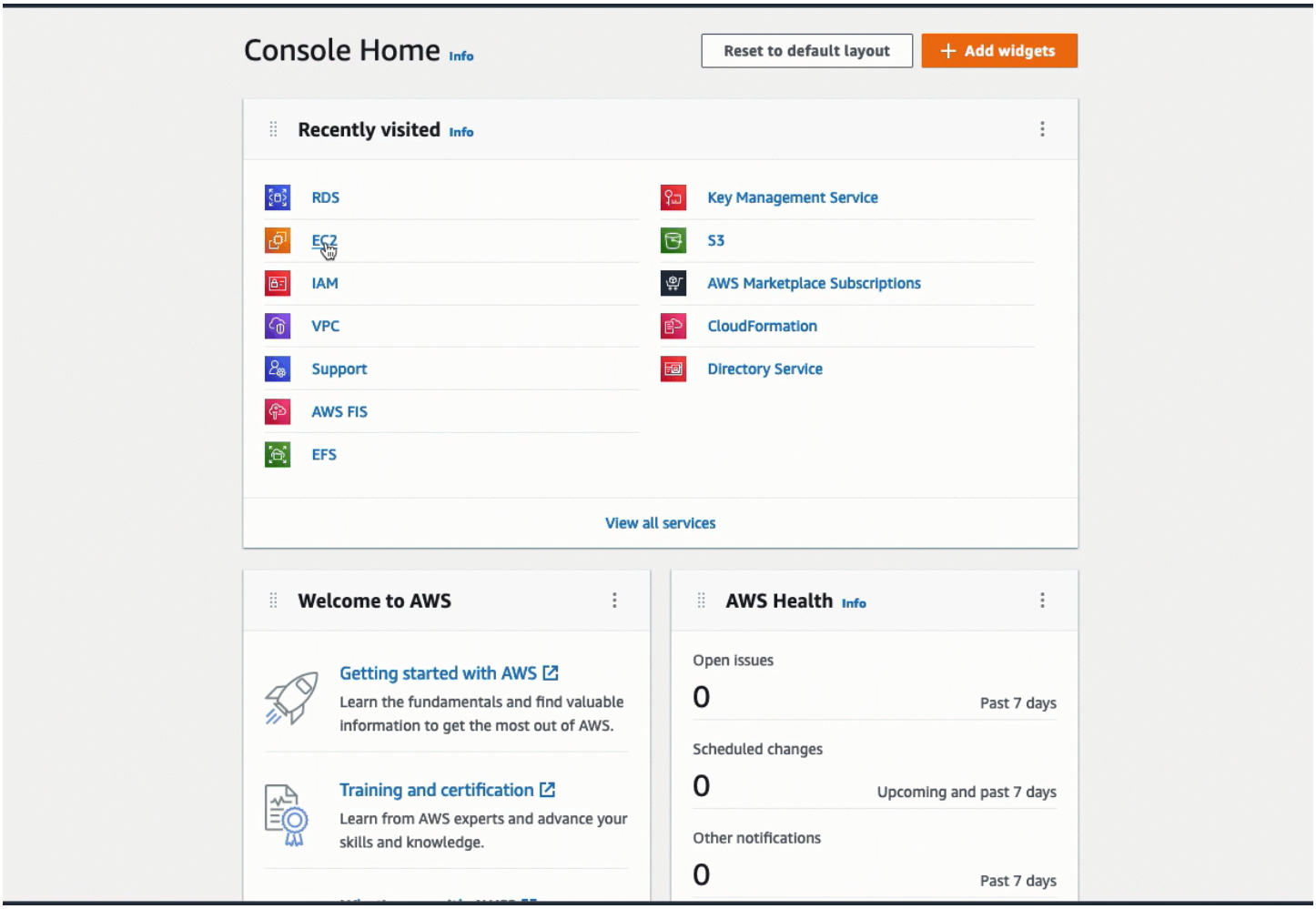
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Escolha a instância do EC2 que você selecionou para se conectar ao banco de dados do RDS na tarefa anterior e escolha a guia Security (Segurança).
4. Em Security details (Detalhes de segurança), Security groups (Grupos de segurança), verifique se um grupo de segurança chamado ec2-rds-***x*** está na lista. *x* é um número.
5. Escolha o grupo de segurança ec2-rds-***x*** para abrir.
6. Escolha a guia Outbound rules (Regras de saída).
7. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:
   - Digite: MySQL/Aurora
   - Intervalo de porta: 3306
   - Destino: ***sg-1234567890example*** / rds-ec2-***x***
   - Descrição: regra para permitir conexões a **`database-tutorial`** de qualquer instância à qual esse grupo de segurança esteja vinculado
8. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.

9. Na página de navegação, escolha Databases (Bancos de dados).
10. Escolha o banco de dados do RDS que você criou para este tutorial.
11. Na guia Connectivity and security (Conectividade e segurança), em Security (Segurança), VPC security groups (Grupos de segurança da VPC), verifique se um grupo de segurança chamado rds-ec2-***x*** está sendo exibido.
12. Escolha o grupo de segurança rds-ec2-***x***. A tela Security Groups (Grupos de segurança) no console do EC2 é aberta.
13. Escolha o grupo de segurança rds-ec2-***x*** para abrir.
14. Escolha a guia Regras de entrada.
15. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:

    - Digite: MySQL/Aurora
    - Intervalo de porta: 3306
    - Origem: ***sg-0987654321example*** / ec2-rds-***x***: este é o grupo de segurança atribuído à instância do EC2 que você verificou nas etapas anteriores.
    - Descrição: regra para permitir conexões de instâncias do EC2 com ***sg-1234567890example*** anexado

    Ao verificar se esses grupos de segurança e regras de grupos de segurança existem e se estão atribuídos à instância do EC2 e ao banco de dados do RDS, conforme descrito neste procedimento, você pode verificar se a conexão foi configurada automaticamente usando o recurso de conexão automática.

Visualizar uma animação: verificar a configuração da conexão



Você concluiu a opção 2 deste tutorial. Agora você pode concluir a opção 3, que ensina a configurar manualmente os grupos de segurança que foram criados automaticamente na opção 2.

Opção 3: conectar manualmente a instância do EC2 ao banco de dados do RDS imitando o recurso de conexão automática

Objetivo

O objetivo da opção 3 é aprender a configurar manualmente a conexão entre uma instância do EC2 e um banco de dados do RDS reproduzindo manualmente a configuração do recurso de conexão automática.

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. Você pode usar uma instância do EC2 existente ou seguir as etapas na tarefa 1 para criar uma nova instância.
- Um banco de dados do RDS que está na mesma VPC da instância do EC2. Você pode usar um banco de dados do RDS existente ou seguir as etapas na tarefa 2 para criar um novo banco de dados.
- Permissões para chamar estas operações. Caso tenha concluído a opção 1 deste tutorial, você já tem essas permissões.
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tarefas para concluir a opção 3

- Tarefa 1: iniciar uma instância do EC2 (opcional)
- Tarefa 2: criar um banco de dados do RDS (opcional)
- Tarefa 3: conectar manualmente sua instância do EC2 ao banco de dados do RDS criando grupos de segurança e atribuindo-os às instâncias

Tarefa 1: iniciar uma instância do EC2 (opcional)

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.

Objetivo da tarefa

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS.

Etapas para iniciar uma instância do EC2

Para iniciar uma instância do EC2, use as seguintes etapas.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: iniciar uma instância do EC2.

Configuração de instância do EC2

As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do EC2, escolha Launch Instance (Iniciar instância).

3. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-manual-1`**. Embora o nome da instância não seja obrigatório, o nome o ajudará a identificá-la facilmente.
4. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

   > **Note**
   >
   > É possível usar o Amazon EC2 no nível gratuito, desde que a conta da AWS tenha menos de 12 meses e que você tenha escolhido um tipo de instância `t2.micro` (ou `t3.micro` em regiões onde `t2.micro` não esteja disponível).

6. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
7. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

      Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

      i. A instância deve estar na mesma VPC do banco de dados do RDS. Por padrão, você tem apenas uma VPC.

      ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

      iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

   b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (security groups) (Firewall [grupos de segurança]), na lista suspensa ao lado da caixa de seleção Allow SSH traffic from (Permitir tráfego SSH de), escolha My IP (Meu IP).

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

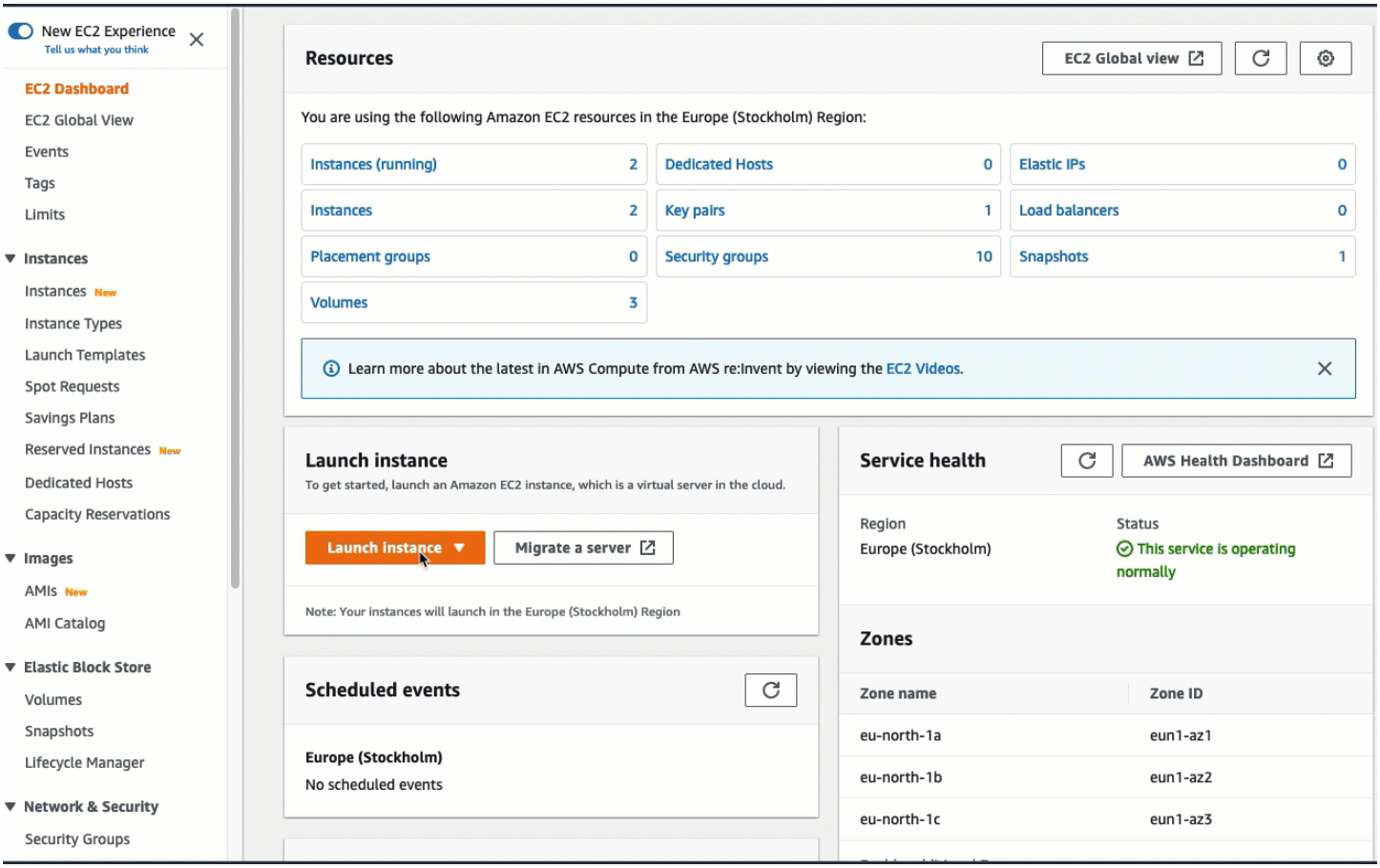
- Permitir tráfego HTTPs da Internet
- Permitir tráfego HTTP da Internet

8. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
9. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. Sua instância estará primeiro em um estado `pending` e depois entrará no estado `running`.

   Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de execução de instâncias.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Visualizar uma animação: iniciar uma instância do EC2



Agora está tudo pronto para Tarefa 2: criar um banco de dados do RDS (opcional).

Tarefa 2: criar um banco de dados do RDS (opcional)

> **Note**
>
> O foco desta parte do tutorial não é criar um banco de dados do RDS. Se você já tiver um banco de dados do RDS e quiser usá-lo para este tutorial, pode ignorar esta tarefa.

Objetivo da tarefa

O objetivo desta tarefa é criar um banco de dados do RDS. Você usará essa instância na tarefa 3 ao conectá-la à instância do EC2.

Etapas para criar um banco de dados do RDS

Use as seguintes etapas para criar um banco de dados do RDS para a opção 3 deste tutorial.

Para ver uma animação dessas etapas, consulte Visualizar uma animação: criar uma instância de banco de dados.

Configuração de banco de dados do RDS

As etapas desta tarefa configuram o banco de dados do RDS da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database-manual`**
- Classe da instância de banco de dados: `db.t3.micro`

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

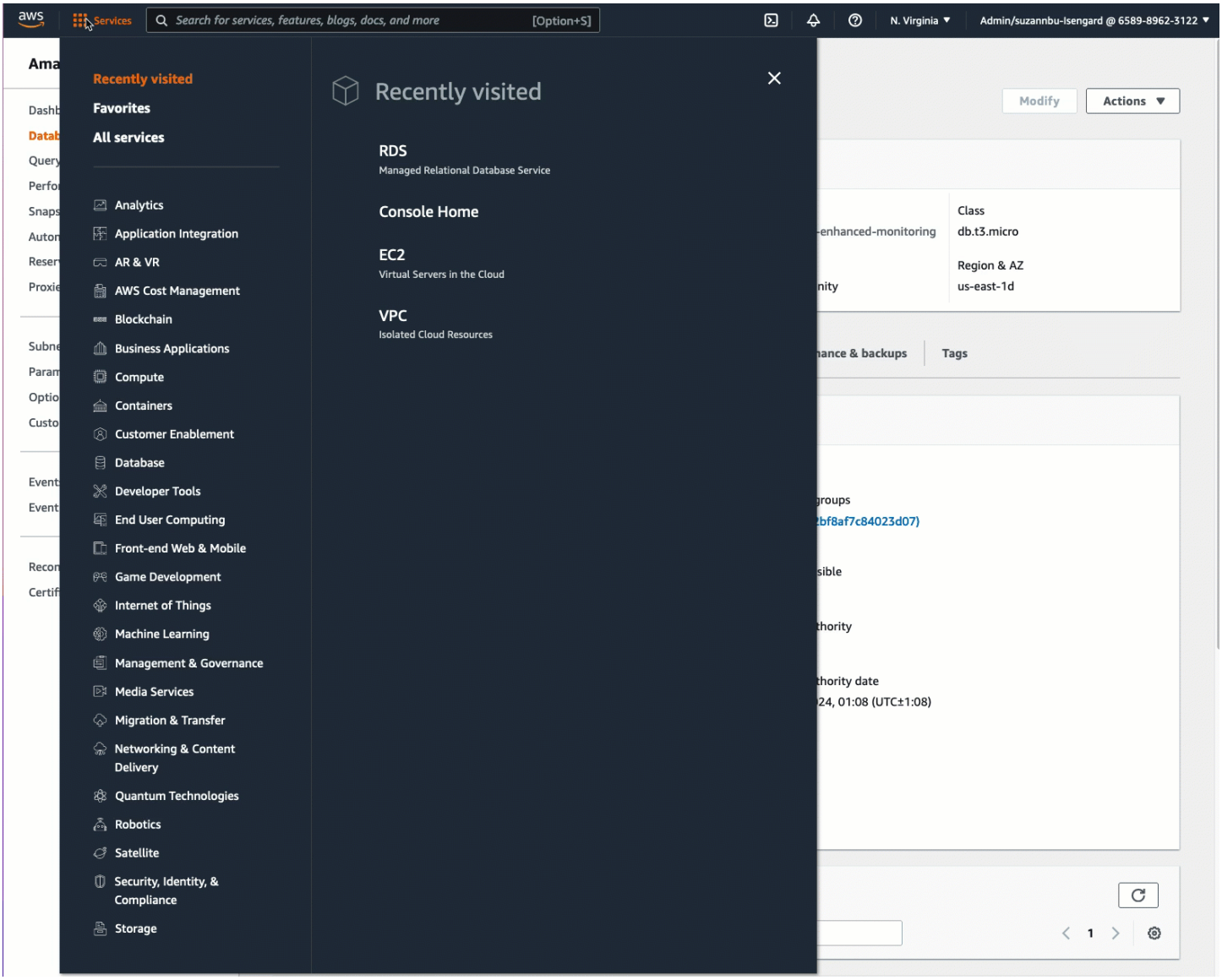
Para criar uma instância de banco de dados MySQL

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha a Região da AWS na qual você criou a instância do EC2. A instância do ECS e a instância de banco de dados devem estar na mesma região.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), escolha Easy create (Criação fácil). Quando você escolhe essa opção, o recurso de conexão automática para configurar automaticamente a conexão não está disponível.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em DB instance size (Tamanho da instância de banco de dados), escolha Free tier (Nível gratuito).
7. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados do RDS. Para este tutorial, insira **`tutorial-database-manual`**.
8. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **`admin`**.

9. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.
10. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status da nova instância de banco de dados será Creating (Criando) até que a instância de banco de dados esteja pronta para uso. Quando o status muda para Available (Disponível), você pode se conectar à instância de banco de dados. Dependendo da classe da instância de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que a nova instância esteja disponível.

Visualizar uma animação: criar uma instância de banco de dados



Agora está tudo pronto para Tarefa 3: conectar manualmente sua instância do EC2 ao banco de dados do RDS criando grupos de segurança e atribuindo-os às instâncias.

Tarefa 3: conectar manualmente sua instância do EC2 ao banco de dados do RDS criando grupos de segurança e atribuindo-os às instâncias

Objetivo da tarefa

O objetivo desta tarefa é reproduzir a configuração de conexão do recurso de conexão automática executando o seguinte manualmente: você cria dois novos grupos de segurança e adiciona um grupo de segurança à instância do EC2 e ao banco de dados do RDS.

Etapas para criar novos grupos de segurança e adicioná-los às instâncias

Use as seguintes etapas para conectar uma instância do EC2 ao banco de dados do RDS criando dois novos grupos de segurança. Em seguida, você adicionará um grupo de segurança à instância do EC2 e ao banco de dados do RDS.

Para criar dois novos grupos de segurança e atribuir à instância do EC2 e outro ao banco de dados do RDS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Primeiro, crie o grupo de segurança para adicionar à instância do EC2, da seguinte forma:
    a. No painel de navegação, escolha Grupos de segurança.
    b. Escolha Create grupo de segurança (Criar grupo de segurança).
    c. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança. Para este tutorial, insira **`ec2-rds-manual-configuration`**.
    d. Em Description (Descrição), insira uma breve descrição. Para este tutorial, insira **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.
    e. Escolha Create security group (Criar grupo de segurança). Você voltará a esse grupo de segurança para adicionar uma regra de saída depois de criar o grupo de segurança de banco de dados do RDS.
3. Agora, crie o grupo de segurança a ser adicionado ao banco de dados do RDS, da seguinte forma:
    a. No painel de navegação, escolha Grupos de segurança.

b. Escolha Create grupo de segurança (Criar grupo de segurança).

c. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança. Para este tutorial, insira **`rds-ec2-manual-configuration`**.

d. Em Description (Descrição), insira uma breve descrição. Para este tutorial, insira **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.

e. Em Inbound rules (Regras de entrada), selecione Add rule (Adicionar regra) e siga estas etapas:

   i. Em Type (Tipo), escolha MySQL/Aurora.

   ii. Em Source (Origem), escolha o grupo de segurança de instâncias ec2-rds-manual-configuration do EC2 que você criou na etapa 2 deste procedimento.

f. Escolha Create security group (Criar grupo de segurança).

4. Edite o grupo de segurança da instância do EC2 para adicionar uma regra de saída, da seguinte forma:

   a. No painel de navegação, escolha Security Groups (Grupos de segurança).

   b. Selecione o grupo de segurança da instância do EC2 (chamado **`ec2-rds-manual-configuration`**) e escolha a guia Outbound rules (Regras de saída).

   c. Escolha Edit outbound rules (Editar regras de saída).

   d. Selecione Add rule (Adicionar regra) e faça o seguinte:

      i. Em Type (Tipo), escolha MySQL/Aurora.

      ii. Em Source (Origem), escolha o grupo de segurança do banco de dados do RDS rds-ec2-manual-configuration criado na Etapa 3 deste procedimento.

      iii. Escolha Salvar regras.

5. Adicione o grupo de segurança da instância do EC2 à instância do EC2 da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias).

   b. Selecione a instância do EC2 e escolha Actions (Ações), Security (Segurança), Change security groups (Alterar grupos de segurança).

   c. Em Associated security groups (Grupos de segurança associados), escolha o campo Select security groups (Selecionar grupos de segurança), escolha ec2-rds-manual-configuration criado anteriormente e escolha Add security group (Adicionar grupo de segurança).

   d. Escolha Salvar.

6. Adicione o grupo de segurança do banco de dados do RDS ao banco de dados do RDS, da seguinte forma:

   a. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
   b. No painel de navegação, escolha Databases (Bancos de dados) e selecione o banco de dados.
   c. Escolha Modificar.
   d. Em Connectivity (Conectividade), para Security group (Grupo de segurança), escolha rds-ec2-manual-configuration criado anteriormente e escolha Continue (Continuar).
   e. Em Scheduling of modifications (Programação de modificações), escolha Apply immediately (Aplicar imediatamente).
   f. Selecione Modify DB instance (Modificar instância de banco de dados).

   Agora você concluiu as etapas manuais que imitam as etapas automáticas que ocorrem ao usar o recurso de conexão automática.

Você concluiu a opção 3 deste tutorial. Se você concluiu as opções 1, 2 e 3 e não precisa mais dos recursos criados neste tutorial, exclua-os para evitar custos desnecessários. Para ter mais informações, consulte Limpeza.

Limpeza

Agora que você concluiu o tutorial, é uma prática recomendada limpar (excluir) os recursos que não queira mais usar. Limpar os recursos da AWS evita que sua conta incorra em cobranças adicionais.

Tópicos

- Terminar a instância do EC2
- Excluir banco de dados do RDS

Terminar a instância do EC2

Se você iniciou uma instância do EC2 especificamente para este tutorial, pode encerrá-la para parar de incorrer em quaisquer cobranças associadas a ela.

Para encerrar uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância criada para este tutorial e escolha Instance state (Estado da instância), Terminate instance (Terminar instância).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Excluir banco de dados do RDS

Se você criou um banco de dados do RDS especificamente para este tutorial, pode excluí-lo para parar de incorrer em quaisquer cobranças associadas a ele.

Para excluir um banco de dados do RDS usando o console

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No painel de navegação, escolha Databases (Bancos de dados).
3. Selecione o banco de dados do RDS criado para este tutorial e escolha Actions (Ações), Delete (Excluir).
4. Insira **`delete me`** na caixa e escolha Delete (Excluir).

Identificação de instâncias do EC2

Talvez seja necessário determinar se a aplicação está sendo executada em uma instância do EC2, especialmente se você tiver um ambiente de computação misto. Cada instância tem um documento de identidade de instância assinado que você pode verificar criptograficamente. É possível encontrar esses documentos neste endereço local não roteável: `http://169.254.169.254/latest/dynamic/instance-identity/`. Para ter mais informações, consulte Documentos de identidade da instância.

Inspecione o UUID do sistema

Você pode obter o UUID do sistema e procurar no octeto inicial do UUID por `EC2` (no Linux, pode ser `ec2` em letras minúsculas). Esse método é rápido, mas potencialmente impreciso, pois há uma pequena possibilidade de que um sistema que não seja uma instância do EC2 possa ter um UUID que comece com esses caracteres. Além disso, algumas versões do SMBIOS usam o formato little-endian, que não inclui `EC2` no início do UUID. Esse pode ser o caso de instâncias do EC2 que usam o SMBIOS 2.4 para Windows ou de distribuições do Linux diferentes do Amazon Linux 2 que têm as próprias implementações de SMBIOS.

Exemplo do Linux: obtenha o UUID da DMI (somente para AMIs de HVM)

Use o seguinte comando para obter o UUID usando a Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

No exemplo de saída a seguir, o UUID é representado no formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Como alternativa, para instâncias criadas no sistema Nitro, é possível usar o seguinte comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Se a saída for um ID de instância, como a saída de exemplo a seguir, o sistema será uma instância do EC2:

```
i-0af01c0123456789a
```

Exemplo do Linux: obtenha o UUID do hipervisor (somente para AMIs PV)

Use o seguinte comando para obter o UUID do hipervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Na próxima saída de exemplo, o UUID começa com "ec2", que indica que o sistema é provavelmente uma instância do EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Exemplo do Windows: obtenha o UUID usando o WMI ou o Windows PowerShell

Use a linha de comando de Instrumentação de Gerenciamento do Windows (WMIC) da seguinte forma:

```
wmic path win32_computersystemproduct get uuid
```

Alternativamente, se você estiver usando o Windows PowerShell, use o cmdlet Get-WmiObject da seguinte maneira:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Para instâncias que usam o SMBIOS 2.4, o UUID pode ser representado no formato little-endian; por exemplo:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Inspecione o identificador de geração da máquina virtual do sistema

Um identificador de geração de máquina virtual consiste em um buffer exclusivo de 128 bits interpretado como identificador de inteiro aleatório criptográfico. É possível recuperar o identificador de geração de máquina virtual para identificar sua instância do Amazon Elastic Compute Cloud. O identificador de geração é exposto no sistema operacional convidado da instância por meio de uma entrada de tabela ACPI. O valor mudará se sua máquina for clonada, copiada ou importada para AWS, como com VM Import/Export.

Exemplo: como recuperar o identificador de geração de máquina virtual do Linux

É possível usar os seguintes comandos para recuperar o identificador de geração de máquina virtual de suas instâncias que executem o Linux:

Amazon Linux 2

1. Atualize seus pacotes de software existentes, conforme necessário, usando o seguinte comando:

   ```
   sudo yum update
   ```

2. Se necessário, utilize o pacote busybox com o seguinte comando:

```
sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
```

3. Se necessário, instale os pacotes de pré-requisitos usando o seguinte comando:

```
sudo yum install busybox.rpm iasl -y
```

4. Execute o seguinte `iasl` para produzir saída da tabela ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Execute o seguinte comando para revisar a saída do comando `iasl`:

```
cat SSDT2.dsl
```

A saída deve gerar o espaço de endereço necessário para recuperar o identificador de geração da máquina virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
```

```
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opcional) Eleve suas permissões de terminal para as etapas restantes com o seguinte comando:

```
sudo -s
```

7. Use o comando a seguir para armazenar o espaço de endereço coletado anteriormente:

```
VMGN_ADDR=0xFED01000
```

8. Use o seguinte comando para iterar pelo espaço de endereço e criar o identificador de geração de máquina virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Recupere o identificador de geração da máquina virtual do arquivo de saída com o seguinte comando:

```
cat vmgenid ; echo
```

Sua saída deve ser similar à seguinte:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Atualize seus pacotes de software existentes, conforme necessário, usando o seguinte comando:

```
sudo apt update
```

2. Se necessário, instale os pacotes de pré-requisitos usando o seguinte comando:

```
sudo apt install busybox iasl -y
```

3. Execute o seguinte `iasl` para produzir saída da tabela ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Execute o seguinte comando para revisar a saída do comando `iasl`:

```
cat SSDT2.dsl
```

A saída deve gerar o espaço de endereço necessário para recuperar o identificador de geração da máquina virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
```

```
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
```

```
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Opcional) Eleve suas permissões de terminal para as etapas restantes com o seguinte comando:

```
sudo -s
```

6. Use os seguintes comandos para armazenar o espaço de endereço coletado anteriormente:

```
VMGN_ADDR=0xFED01000
```

7. Use o seguinte comando para iterar pelo espaço de endereço e criar o identificador de geração de máquina virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Recupere o identificador de geração da máquina virtual do arquivo de saída com o seguinte comando:

```
cat vmgenid ; echo
```

Sua saída deve ser similar à seguinte:

```
EC2F335D979132C4165896753E72BD1C
```

Exemplo: como recuperar o identificador de geração de máquina virtual do Windows

É possível criar uma aplicação de exemplo para recuperar o identificador de geração de máquina virtual de suas instâncias que executam o Windows. Para obter mais informações, consulte Obter o identificador de geração de máquina virtual na documentação da Microsoft.

Gerenciamento das configurações do sistema para a instância do Amazon EC2

Depois de iniciar a instância, você poderá fazer login como administrador para fazer alterações. Esta seção se concentra no gerenciamento das configurações do sistema para a instância.

Conteúdo

- Definição do horário para a instância do Amazon EC2
- Controle do estado do processo para sua instância do Amazon Linux do EC2
- Otimizar as opções de CPU
- AMD SEV-SNP no Amazon EC2
- Adição de componentes do sistema do Windows usando a mídia de instalação
- Gerenciamento de usuários do sistema na instância do Linux
- Definição da senha do administrador do Windows para a instância

Definição do horário para a instância do Amazon EC2

Uma referência de horário consistente e precisa na instância do Amazon EC2 é crucial para muitas tarefas e processos de servidor. Os timestamps nos logs do sistema desempenham um papel essencial na identificação de quando os problemas ocorreram e na ordem cronológica dos eventos. Se você usar a AWS CLI ou um SDK da AWS para fazer solicitações à instância, essas ferramentas assinarão as solicitações em seu nome. Se as configurações de data e hora da instância não forem exatas, poderá haver uma discrepância entre a data na assinatura e a data da solicitação, levando a AWS a rejeitar suas solicitações.

Para lidar com esse aspecto importante, a Amazon oferece o Serviço de Sincronização Temporal da Amazon, que é acessível em todas as instâncias do EC2 e é usado por vários Serviços da AWS. Esse serviço usa uma frota de relógios de referência atômicos e conectados via satélite em cada Região da AWS para fornecer leituras de hora exatas e atuais do padrão global do Horário Universal Coordenado (UTC).

O Serviço de Sincronização Temporal da Amazon usa o Network Time Protocol (NTP) ou fornece um relógio Precision Time Protocol (PTP) físico local nas instâncias compatíveis. O relógio PTP físico é compatível tanto com uma conexão NTP quanto com uma conexão PTP direta. As conexões NTP e PTP diretas usam a mesma fonte de hora extremamente exata, mas a conexão PTP direta é mais precisa do que a conexão NTP. A conexão NTP com o Serviço de Sincronização Temporal da

Amazon usa a difusão de segundos bissextos, enquanto a conexão PTP com o relógio PTP físico não usa. Para ter mais informações, consulte Segundos bissextos.

Para obter o melhor desempenho, recomendamos usar o Serviço de Sincronização Temporal da Amazon local nas instâncias do EC2. Para fazer backup no Serviço de Sincronização Temporal da Amazon local nas instâncias e para conectar recursos externos ao Amazon EC2 ao Serviço de Sincronização Temporal da Amazon, é possível usar o Serviço de Sincronização Temporal da Amazon público localizado em `time.aws.com`. O Serviço de Sincronização Temporal da Amazon público, como o Serviço de Sincronização Temporal da Amazon local, faz automaticamente a difusão de qualquer segundo bissexto adicionado ao UTC. O Serviço de Sincronização Temporal da Amazon público é compatível globalmente com nossa frota de relógios atômicos de referência conectados via satélite em cada Região da AWS.

Tópicos

- Definir a instância para usar o Serviço de Sincronização Temporal da Amazon
- Configure a instância ou qualquer dispositivo conectado à Internet para usar o Serviço de Sincronização Temporal da Amazon público
- Comparação dos carimbos de data/hora das instâncias do Linux
- Alteração do fuso horário da instância
- Segundos bissextos
- Recursos relacionados

Definir a instância para usar o Serviço de Sincronização Temporal da Amazon

As instâncias podem acessar o Serviço de Sincronização Temporal da Amazon da seguinte forma:

- Por NTP nos seguintes endpoints de endereço IP:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (acessível somente por instâncias desenvolvidas no AWS Nitro System.)
- (Somente para o Linux) Por meio de uma conexão PTP direta para se conectar a um relógio de hardware PTP local:
  - `PHC0`

As AMIs do Amazon Linux, as AMIs do Windows e a maioria das AMIs de parceiros configuram a instância para usar o endpoint do protocolo NTP para IPv4 por padrão. Esta é a configuração

recomendada para a maioria das workloads do cliente. Nenhuma configuração adicional é necessária para instâncias iniciadas dessas AMIs, a menos que você queira usar o endpoint IPv6 ou se conectar diretamente ao relógio PTP físico.

As conexões NTP e PTP não exigem nenhuma alteração na configuração da VPC e a instância não requer acesso à Internet.

> **Note**
>
> Somente as instâncias do Linux podem usar uma conexão PTP direta para se conectar ao relógio de hardware PTP local. As instâncias do Windows usam o protocolo NTP para se conectar ao relógio de hardware PTP local.

Tópicos

- Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon
- Conectar-se ao endpoint IPv6 do Serviço de Sincronização Temporal da Amazon
- Conectar-se ao relógio PTP físico

Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon

Esta seção descreve como configurar a instância para usar o Serviço de Sincronização Temporal da Amazon local por meio do endpoint IPv4.

Use as instruções para o sistema operacional da sua instância.

Linux

O AL2023 e as versões mais recentes das AMIs do Amazon Linux 2 e do Amazon Linux são configuradas para usar o endpoint IPv4 do Serviço de Sincronização Temporal da Amazon por padrão. Nenhuma configuração adicional é necessária para as instâncias iniciadas usando essas AMIs, e você pode ignorar o procedimento apresentado a seguir.

Se estiver usando uma AMI que não tem o Amazon Time Sync Service configurado por padrão, use um dos seguintes procedimentos para configurar o Serviço de Sincronização Temporal da Amazon na instância usando o cliente `chrony`. É necessário adicionar uma entrada de servidor para o Serviço de Sincronização Temporal da Amazon no arquivo de configuração `chrony`.

Use as instruções para o sistema operacional da sua instância.

Amazon Linux

Para se conectar ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon no Amazon Linux usando o chrony

1. Conecte-se à sua instância e desinstale o serviço NTP.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Instale o pacote `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Abra o arquivo `/etc/chrony.conf` usando um editor de texto (como vim ou nano). Verifique se o arquivo inclui a seguinte linha:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

   Se a linha estiver presente, o Amazon Time Sync Service já estará configurado para usar o endpoint IPv4 do Serviço de Sincronização Temporal da Amazon e você poderá passar para a próxima etapa. Caso contrário, adicione a linha depois de todas as outras instruções `server` ou `pool` já presentes no arquivo e salve as alterações.

4. Reinicie o daemon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

> **Note**
>
> No RHEL e no CentOS (até a versão 6), o nome do serviço é `chrony` em vez de `chronyd`.

5. Para configurar o `chronyd` para ser iniciado a cada inicialização do sistema, use o comando `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Confirme que o `chrony` está usando o endpoint IPv4 `169.254.169.123` para sincronizar a hora.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                                 .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
||                                \     |          |  zzzz = estimated
error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample


===============================================================================
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-
 287us
^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-
  11ms
^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/-
1959us
^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
```

Na saída retornada, `^*` indica a fonte de hora preferida.

7. Verifique as métricas de sincronização da hora informadas pelo `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
        Stratum         : 4
        Ref time (UTC)  : Wed Nov 22 13:18:34 2017
        System time     : 0.000000626 seconds slow of NTP time
        Last offset     : +0.002852759 seconds
        RMS offset      : 0.002852759 seconds
        Frequency       : 1.187 ppm fast
        Residual freq   : +0.020 ppm
        Skew            : 24.388 ppm
        Root delay      : 0.000504752 seconds
        Root dispersion : 0.001112565 seconds
        Update interval : 64.4 seconds
        Leap status     : Normal
```

Ubuntu

Para conectar ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon no Ubuntu usando o chrony

1. Conecte-se à sua instância e use `apt` para instalar o pacote `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Se necessário, atualize sua instância primeiro executando `sudo apt update`.

2. Abra o arquivo `/etc/chrony/chrony.conf` usando um editor de texto (como vim ou nano). Adicione a seguinte linha antes de todas as outras instruções `server` ou `pool` já presentes no arquivo, e salve as alterações:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Reinicie o serviço `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Confirme que o chrony está usando o endpoint IPv4 169.254.169.123 para sincronizar a hora.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

             .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
 combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
 variable.
           ||                                                .- xxxx [ yyyy ]
 +/- zzzz
           ||      Reachability register (octal) -.          |  xxxx =
 adjusted offset,
           ||      Log2(Polling interval) --.      |         |  yyyy =
 measured offset,
           ||                                \     |         |  zzzz =
 estimated error.
           ||                                 |    |          \
           MS Name/IP address         Stratum Poll Reach LastRx Last sample

 ===============================================================================
           ^* 169.254.169.123               3   6    17    12    +15us[  +57us]
 +/-  320us
           ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us]
 +/- 1779us
           ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us]
 +/- 7710us
           ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
           ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
           ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

```
            ^? bray.walcz.net               0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

Na saída retornada, a linha que começa com `^*` indica a fonte de horas preferida.

5. Verifique as métricas de sincronização da hora informadas pelo `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
            Stratum         : 4
            Ref time (UTC)  : Wed Nov 29 07:41:57 2017
            System time     : 0.000000011 seconds slow of NTP time
            Last offset     : +0.000041659 seconds
            RMS offset      : 0.000041659 seconds
            Frequency       : 10.141 ppm slow
            Residual freq   : +7.557 ppm
            Skew            : 2.329 ppm
            Root delay      : 0.000544 seconds
            Root dispersion : 0.000631 seconds
            Update interval : 2.0 seconds
            Leap status     : Normal
```

SUSE Linux

A partir do SUSE Linux Enterprise Server 15, o `chrony` é a implementação padrão do NTP.

Para se conectar ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon no SUSE usando o chrony

1. Abra o arquivo `/etc/chrony.conf` usando um editor de texto (como vim ou nano).
2. Verifique se o arquivo contém a seguinte linha:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Se essa linha não estiver presente, adicione-a.

3. Comente qualquer outro servidor ou linhas de consulta.
4. Abra o yaST e ative o serviço chrony.

Windows

A versão das AMIs do Windows de agosto de 2018 em diante usam o Amazon Time Sync Service por padrão. Nenhuma configuração adicional é necessária para instâncias iniciadas dessas AMIs e você pode ignorar os procedimentos a seguir.

Se você estiver usando uma AMI que não tenha o Serviço de Sincronização Temporal da Amazon configurado por padrão, primeiro verifique sua configuração atual do protocolo NTP. Se a instância já estiver usando o endpoint IPv4 do Serviço de Sincronização Temporal da Amazon, nenhuma configuração adicional será necessária. Se a instância não estiver usando o Serviço de Sincronização Temporal da Amazon, faça o procedimento para alterar o servidor NTP para que use o Serviço de Sincronização Temporal da Amazon.

Para verificar a configuração de NTP

1. Na instância, abra uma janela de prompt de comando.
2. Obtenha a configuração de NTP atual digitando o seguinte comando:

   ```
   w32tm /query /configuration
   ```

   Esse comando retorna as definições de configuração atuais para a instância do Windows e mostrará se você está conectado ao Serviço de Sincronização Temporal da Amazon.
3. (Opcional) Obtenha o status da configuração atual digitando o seguinte comando:

   ```
   w32tm /query /status
   ```

   Esse comando retorna informações, como o último horário em que a instância foi sincronizada com o servidor NTP e o intervalo de sondagem.

Para alterar o servidor NTP para usar o Amazon Time Sync Service

1. Na janela de prompt de comando, execute o seguinte comando:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```
2. Verifique suas novas configurações usando o seguinte comando:

   ```
   w32tm /query /configuration
   ```

Na saída retornada, verifique se `NtpServer` exibe o endpoint IPv4 `169.254.169.123`.

Configurações de NTP (Network Time Protocol) padrão para AMIs do Windows da Amazon

As Imagens de máquina da Amazon (AMIs) geralmente aderem aos padrões prontos para uso, exceto em casos em que alterações são necessárias para que funcionem na infraestrutura do EC2. As seguintes configurações foram determinadas para funcionar de maneira adequada em um ambiente virtual, bem como manter qualquer desvio de relógio dentro um segundo de precisão:

- Intervalo de atualização: rege a frequência com que o serviço de hora acertará a hora do sistema para garantir sua precisão. A AWS configura o intervalo de atualização para ocorrer uma vez a cada dois minutos.
- Servidor NTP: a partir da versão de agosto de 2018, as AMIs usam o Serviço de Sincronização Temporal da Amazon por padrão. Esse serviço de horário pode ser acessado em qualquer Região da AWS no endpoint IPv4 169.254.169.123. Além disso, o sinalizador 0x9 indica que o serviço de horário está atuando como um cliente e utiliza o `SpecialPollInterval` para determinar a frequência com a qual realizar verificações com o servidor de horário configurado.
- Tipo – "NTP" significa que o serviço atua como um cliente NTP autônomo em vez de agir como parte de um domínio.
- Habilitado e InputProvider: o serviço de hora está habilitado e fornece a hora ao sistema operacional.
- Intervalo de pesquisa especial: verifica o servidor NTP configurado a cada 900 segundos (15 minutos).

Caminho de registro	Nome da chave	Dados
HKLM:\System\CurrentControlSet\services\w32time\Config	UpdateInterval	120
HKLM:\System\CurrentControlSet\services\w32time\Parameters	NtpServer	169.254.169.123,0x9

Caminho de registro	Nome da chave	Dados
HKLM:\System\CurrentControlSet\services\w32time\Parameters	Tipo	NTP
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	Enabled	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	InputProvider	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	SpecialPollInterval	900

Conectar-se ao endpoint IPv6 do Serviço de Sincronização Temporal da Amazon

Esta seção explica como as etapas descritas no Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon diferem se você estiver configurando a instância para usar o Serviço de Sincronização Temporal da Amazon local por meio do endpoint IPv6. Ela não explica todo o processo de configuração do Amazon Time Sync Service.

O endpoint IPv6 pode ser acessado somente em instâncias desenvolvidas no AWS Nitro System.

> **Note**
>
> Não recomendamos usar as entradas de endpoint IPv4 e IPv6 em conjunto. Os pacotes IPv4 e IPv6 NTP vêm do mesmo servidor local para a sua instância. Configurar ambos os endpoints IPv4 e IPv6 é desnecessário e não melhorará a precisão da hora na instância.

Use as instruções para o sistema operacional da sua instância.

Linux

Dependendo da distribuição do Linux que está usando, ao chegar à etapa de edição do arquivo chrony.conf, você estará usando o endpoint IPv6 do Serviço de Sincronização Temporal da Amazon (`fd00:ec2::123`) em vez do endpoint IPv4 (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Salve o arquivo e confirme que o `chrony` está usando o endpoint IPv6 `fd00:ec2::123` para sincronizar a hora:

```
[ec2-user ~]$ chronyc sources -v
```

Na saída, se você vir o endpoint IPv6 `fd00:ec2::123`, a configuração estará concluída.

Windows

Ao chegar à etapa de alteração do servidor NTP para usar o Serviço de Sincronização Temporal da Amazon, você estará usando o endpoint IPv6 do Serviço de Sincronização Temporal da Amazon (`fd00:ec2::123`) em vez do endpoint IPv4 (`169.254.169.123`):

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Verifique se as novas configurações estão usando o endpoint IPv6 `fd00:ec2::123` para sincronizar o horário:

```
w32tm /query /configuration
```

Na saída, verifique se `NtpServer` exibe o endpoint IPv6 `fd00:ec2::123`.

Conectar-se ao relógio PTP físico

O relógio de hardware baseado em PTP faz parte do AWS Nitro System, portanto, pode ser acessado diretamente em instâncias bare metal e virtualizadas do EC2 com suporte, sem a necessidade de usar recursos do cliente.

Os endpoints NTP para o relógio de hardware PTP são os mesmos do Serviço de Sincronização Temporal da Amazon normal. Se a instância tiver um relógio de hardware PTP e você

tiver configurado a conexão NTP (com o endpoint IPv4 ou IPv6), a hora da instância será automaticamente obtida do relógio de hardware PTP via NTP.

Para instâncias do Linux, é possível configurar uma conexão PTP direta, o que fornecerá uma hora mais precisa do que a conexão NTP. As instâncias do Windows só são compatíveis com uma conexão NTP para o relógio de hardware PTP.

Requisitos

O relógio PTP físico está disponível em uma instância quando os seguintes requisitos são atendidos:

- Regiões da AWS com suporte: Leste dos EUA (Norte da Virgínia) e Ásia-Pacífico (Tóquio)
- Famílias de instâncias suportadas:
  - Uso geral: M7a, M7g, M7gd e M7i
  - Otimizada para computação: C7a, C7gd e C7i
  - Otimizada para memória: R7a, R7g, R7gd e R7i
- (Somente Linux) Driver do ENA, na versão 2.10.0 ou em versões posteriores, instalado em um sistema operacional compatível. Para obter mais informações sobre os sistemas operacionais compatíveis, consulte os pré-requisitos do driver no GitHub.

(Somente Linux) Configurar uma conexão PTP direta com o relógio de hardware PTP

Esta seção descreve como configurar a instância do Linux para usar o Serviço de Sincronização Temporal da Amazon local por meio do relógio de hardware PTP usando uma conexão PTP direta. É necessário adicionar uma entrada do servidor para o relógio de hardware PTP ao arquivo de configuração do `chrony`.

Para configurar uma conexão PTP direta com o relógio de hardware PTP (somente instâncias do Linux)

1. Conecte-se à sua instância do Linux e faça o seguinte:

   a. Instale o driver do kernel Linux para o Adaptador de Rede Elástica (ENA) versão 2.10.0 ou posterior.

   b. Habilite o relógio de hardware PTP.

   Para obter as instruções de instalação, consulte Linux kernel driver for Elastic Network Adapter (ENA) family no GitHub.

2. Verifique se o dispositivo `/dev/ptp0` aparece na instância.

```
[ec2-user ~]$ ls /dev/ptp0
```

A saída esperada é mostrada a seguir. Se `/dev/ptp0` não estiver na saída, o driver ENA não foi instalado corretamente. Revise a etapa 1 desse procedimento para instalar o driver.

```
/dev/ptp0
```

3. Edite o `/etc/chrony.conf` o usando um editor de texto e adicione a linha a seguir em qualquer ponto no arquivo.

```
refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
```

4. Reinicie o chrony.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Verifique se o chrony está usando o relógio PTP físico para sincronizar a hora nessa instância.

```
[ec2-user ~]$ chronyc sources
```

Saída esperada

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

Na saída retornada, `*` indica a fonte de hora preferida. `PHC0` corresponde ao relógio PTP físico. Pode ser necessário esperar alguns segundos após reiniciar o chrony para que o asterisco apareça.

Configure a instância ou qualquer dispositivo conectado à Internet para usar o Serviço de Sincronização Temporal da Amazon público

Você pode configurar a instância ou qualquer dispositivo conectado à Internet, como seu computador local ou um servidor local, para usar o Serviço de Sincronização Temporal da Amazon público, que pode ser acessado pela Internet em `time.aws.com`. Você pode usar o Serviço de Sincronização

Temporal da Amazon público como backup para o Serviço de Sincronização Temporal da Amazon e para conectar recursos de fora da AWS ao Serviço de Sincronização Temporal da Amazon.

> **Note**
>
> Para obter o melhor desempenho, recomendamos usar o Serviço de Sincronização Temporal da Amazon local nas instâncias e usar o Serviço de Sincronização Temporal da Amazon público somente como backup.

Use as instruções referentes ao sistema operacional da sua instância ou do seu dispositivo.

Linux

Para definir que a instância ou dispositivo com Linux use o Serviço de Sincronização Temporal da Amazon público usando chrony ou ntpd

1. Edite o `/etc/chrony.conf` (se você usar o chrony) ou o `/etc/ntp.conf` (se você usar o ntpd) usando um de texto da seguinte maneira:

   a. Para evitar que a instância ou o dispositivo tente misturar servidores com difusão de tempo e servidores sem difusão de tempo, remova ou comente as linhas que começam com `server`, exceto qualquer conexão existente com o Serviço de Sincronização Temporal da Amazon local.

   > **Important**
   >
   > Se você estiver configurando sua instância do EC2 para se conectar ao Serviço de Sincronização Temporal da Amazon público, não remova a linha a seguir que a instância deve se conectar ao Serviço de Sincronização Temporal da Amazon local. O Serviço de Sincronização Temporal da Amazon local é uma conexão mais direta e garantirá uma maior precisão do relógio. O Serviço de Sincronização Temporal da Amazon público só deve ser usado como backup.
   >
   > ```
   > server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   > ```

   b. Adicione a seguinte linha para se conectar ao Serviço de Sincronização Temporal da Amazon.

```
pool time.aws.com iburst
```

2. Reinicie o daemon usando um dos comandos a seguir.

   - chrony

     ```
     sudo service chronyd force-reload
     ```

   - ntpd

     ```
     sudo service ntp reload
     ```

macOS

Para definir que a instância ou dispositivo com macOS use o Serviço de Sincronização Temporal da Amazon público

1. Abra System Preferences (Preferências do sistema).
2. Escolha Date & Time (Data e hora) e, em seguida, escolha a guia Date & Time (Data e hora).
3. Para fazer alterações, escolha o ícone de cadeado e digite sua senha quando solicitado.
4. Em Set date and time automatically (Definir data e hora automaticamente), insira **`time.aws.com`**.

Windows

Para definir que a instância ou dispositivo com Windows use o Serviço de Sincronização Temporal da Amazon público

1. Abra o Control Panel (Painel de controle).
2. Escolha o ícone de Date and Time (Data e hora).
3. Escolha a guia Internet Time (Horário da Internet). Essa guia não estará disponível se o PC fizer parte de um domínio. Nesse caso, a hora será sincronizada com o controlador de domínio. Você pode configurar o controlador para usar o Serviço de Sincronização Temporal da Amazon público.
4. Escolha Change settings (Alterar configurações).

5. Marque a caixa de seleção em Synchronize with an Internet time server (Sincronizar com um servidor de hora na Internet).
6. Ao lado de Server (Servidor), insira **`time.aws.com`**.

Para definir que a instância ou dispositivo com Windows Server use o Serviço de Sincronização Temporal da Amazon público

- Siga as instruções da Microsoft para atualizar o registro.

Comparação dos carimbos de data/hora das instâncias do Linux

Se estiver usando o Serviço de Sincronização Temporal da Amazon, você poderá comparar os carimbos de data/hora nas instâncias do Linux do Amazon EC2 com o ClockBound para determinar o horário real de um evento. O ClockBound mede a precisão do relógio da instância do EC2 e permite que você confira se um determinado carimbo de data/hora está no passado ou no futuro em relação ao relógio atual da instância. Essas informações são valiosas para determinar a ordem e a consistência de eventos e transações entre instâncias do EC2, independentemente da localização geográfica de cada instância.

O ClockBound é um daemon e uma biblioteca de código aberto. Para saber mais sobre o ClockBound, incluindo instruções de instalação, consulte Clockbound no GitHub.

O ClockBound é compatível somente com instâncias do Linux.

Se você estiver usando a conexão PTP direta com o relógio PTP físico, seu daemon de hora, como o chrony, subestimará o limite de erro do relógio. Isso ocorre porque um relógio PTP físico não passa as informações corretas de limite de erro para o chrony, como o NTP faz. Como resultado, o daemon de sincronização de relógio pressupõe que o relógio esteja certo em UTC e que, portanto, tenha um limite de erro de `0`. Para medir o limite total de erro, o Sistema Nitro calcula o limite de erro do relógio PTP físico e o disponibiliza para a instância do EC2 via sistema de arquivos `sysfs` do driver ENA. Isso pode ser lido diretamente como um valor em nanossegundos.

Para recuperar o limite de erro do relógio de hardware PTP

1. Primeiro, obtenha a localização correta do dispositivo de relógio de hardware PTP usando um dos comandos a seguir. O caminho no comando pode ser diferente dependendo da AMI usada para iniciar a instância.

   - Para Amazon Linux 2:

```
cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
```

- Para Amazon Linux 2023:

```
cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
```

A saída é o nome do slot PCI, que é a localização do dispositivo de relógio de hardware PTP físico. Neste exemplo, o local é `0000:00:03.0`.

```
PCI_SLOT_NAME=0000:00:03.0
```

2. Para recuperar erro do relógio de hardware PTP vinculado execute o comando a seguir. Inclua o nome do slot PCI da etapa anterior.

```
cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
```

A saída é o limite de erro do relógio PTP físico, em nanossegundos.

Para calcular o limite de erro de relógio certo em um dado momento específico ao usar a conexão PTP direta com o relógio PTP físico, você deve adicionar o limite de erro do relógio do chrony ou do ClockBound no momento em que o chrony consultar o relógio PTP físico. Para obter mais informações sobre como medir e monitorar a precisão do relógio, consulte Manage Amazon EC2 instance clock accuracy using Amazon Time Sync Service and Amazon CloudWatch – Part 1.

Alteração do fuso horário da instância

As instâncias do Amazon EC2 são definidas para o fuso horário UTC (Tempo Universal Coordenado), por padrão. É possível alterar a hora de uma instância para o horário local ou para outro fuso horário em sua rede.

Use as instruções para o sistema operacional da sua instância.

Linux

> **Important**
>
> Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para alterar o fuso horário de uma instância do AL2023 ou do Amazon Linux 2

1. Exiba a configuração atual de fuso horário do sistema.

```
[ec2-user ~]$ timedatectl
```

2. Liste os fusos horários disponíveis.

```
[ec2-user ~]$ timedatectl list-timezones
```

3. Defina o fuso horário escolhido.

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. (Opcional) Confirme se o fuso horário atual foi atualizado para o novo fuso horário executando o comando timedatectl novamente.

```
[ec2-user ~]$ timedatectl
```

Para alterar o fuso horário de uma instância do Amazon Linux

1. Identifique o fuso horário a ser usado na instância. O diretório `/usr/share/zoneinfo` contém uma hierarquia de arquivos de dados de fuso horário. Navegue a estrutura do diretório no local para localizar um arquivo para seu fuso horário.

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile    GB         Indian       Mideast   posixrules  US
America     CST6CDT  GB-Eire    Iran         MST       PRC         UTC
Antarctica  Cuba     GMT        iso3166.tab  MST7MDT   PST8PDT     WET
Arctic      EET      GMT0       Israel       Navajo    right       W-SU
...
```

Algumas das entradas nesse local são diretórios (como `America`), e esses diretórios contêm arquivos de fuso horário para cidades específicas. Encontre sua cidade (ou uma cidade em seu fuso horário) para ser usada para a instância.

2. Atualize o arquivo `/etc/sysconfig/clock` com o novo fuso horário. Neste exemplo, usamos o arquivo de dados do fuso horário de Los Angeles, `/usr/share/zoneinfo/America/Los_Angeles`.

   a. Abra o arquivo `/etc/sysconfig/clock` usando um editor de texto (como vim ou nano). Você precisa usar sudo com o comando do editor, pois `/etc/sysconfig/clock` é de propriedade de `root`.

   ```
   [ec2-user ~]$ sudo nano /etc/sysconfig/clock
   ```

   b. Localize a entrada `ZONE` e a altere para o fuso horário (omitindo a seção `/usr/share/zoneinfo` do caminho). Por exemplo, para alterar o fuso horário de Los Angeles, altere a entrada `ZONE` para:

   ```
   ZONE="America/Los_Angeles"
   ```

   > **Note**
   >
   > Não altere a entrada `UTC=true` para outro valor. Essa entrada é para o relógio de hardware e não precisa ser ajustada quando você está configurando um fuso horário diferente em sua instância.

   c. Salve o arquivo e saia do editor de texto.

3. Crie um link simbólico entre `/etc/localtime` e o arquivo de fuso horário para que a instância localize o arquivo de fuso horário quando fizer referência a informações do horário local.

   ```
   [ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
   ```

4. Reinicialize o sistema para obter as informações do novo fuso horário em todos os serviços e aplicações.

   ```
   [ec2-user ~]$ sudo reboot
   ```

5. (Opcional) Confirme se o fuso horário atual foi atualizado para o novo fuso horário usando o comando date. O fuso horário atual aparecerá na saída. No exemplo a seguir, o fuso horário atual é PDT, que corresponde ao fuso horário de Los Angeles.

```
[ec2-user ~]$ date
Sun Aug 16 05:45:16 PDT 2020
```

Windows

Para alterar o fuso horário de uma instância do Windows

1. Na instância, abra uma janela de prompt de comando.
2. Identifique o fuso horário a ser usado na instância. Para obter uma lista de fusos horários, use o seguinte comando:

```
tzutil /l
```

Esse comando retorna uma lista com todos os fusos horários disponíveis no seguinte formato:

```
display name
time zone ID
```

3. Localize o ID do fuso horário a ser atribuído à instância.
4. Atribua outro fuso horário usando o seguinte comando:

```
tzutil /s "Pacific Standard Time"
```

O novo fuso horário deve entrar em funcionamento imediatamente.

> **Note**
>
> Você pode atribuir o fuso horário UTC usando o seguinte comando:
>
> ```
> tzutil /s "UTC"
> ```

Para evitar que seu fuso horário mude depois de configurá-lo para o Windows Server

Quando você altera o fuso horário em uma instância do Windows, deve garantir que ele seja mantido durante as reinicializações de sistema. Caso contrário, quando a instância for reiniciada, ela voltará a usar o horário UTC. É possível conservar o horário adicionando a chave do registro RealTimeIsUniversal. Essa chave é definida por padrão em todas as instâncias da geração atual. Para verificar se a chave do registro RealTimeIsUniversal está definida, consulte a etapa 4 no procedimento a seguir. Se a chave não estiver definida, siga estas etapas desde o início.

Para definir a chave do Registro RealTimeIsUniversal

1. Na instância, abra uma janela de prompt de comando.
2. Use o seguinte comando para adicionar a chave de Registro:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Se estiver usando uma AMI do Windows Server 2008 (não do Windows Server 2008 R2) que tenha sido criada antes de 22 de fevereiro de 2013, recomendamos que você atualize para a versão mais recente da AMI do Windows da AWS. Se estiver usando uma AMI que executa o Windows Server 2008 R2 (não o Windows Server 2008), você deverá verificar se o hotfix da Microsoft KB2922223 está instalado. Se esse hotfix não estiver instalado, recomendamos atualizar para o AMI mais recente do Windows da AWS.
4. (Opcional) Verifique se a instância salvou a chave com êxito usando o seguinte comando:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

   Esse comando retorna as subchaves da chave de Registro TimeZoneInformation. É necessário ver a chave RealTimeIsUniversal na parte inferior da lista, semelhante à chave a seguir:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
```

```
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Segundos bissextos

Os segundos bissextos, introduzidos em 1972, são ajustes ocasionais de um segundo no horário UTC para considerar as irregularidades na rotação da Terra, a fim de acomodar as diferenças entre o Tempo Atômico Internacional (TAI) e o horário solar (Ut1). Para gerenciar os segundos bissextos para os clientes, criamos a difusão de segundos bissextos no Serviço de Sincronização Temporal da Amazon. Para obter mais informações, consulte Look Before You Leap — The Coming Leap Second and AWS.

Os segundos bissextos vão acabar e apoiamos totalmente a decisão tomada na 27ª Conferência Geral sobre Pesos e Medidas de abandonar os segundos bissextos até 2035.

Para apoiar essa transição, ainda planejamos continuar a aplicar a difusão durante um evento de segundos bissextos ao acessar o Serviço de Sincronização Temporal da Amazon via conexão NTP local ou nossos consultas de NTP público (`time.aws.com`). O relógio PTP físico, no entanto, não oferece uma opção de difusão de tempo. No caso de um segundo bissexto, o relógio PTP físico adicionará o segundo bissexto de acordo com os padrões do UTC. As fontes de hora com difusão de segundo bissexto e sem difusão de segundos bissextos são iguais na maioria dos casos. Mas, como elas diferem durante um evento de segundo bissexto, não recomendamos o uso de ambas, as fontes de hora com difusão e sem difusão, na configuração do cliente de hora durante um evento de segundo bissexto.

Recursos relacionados

- Blog de computação da AWS: It’s About Time: Microsecond-Accurate Clocks on Amazon EC2 Instances
- (Linux) https://chrony-project.org/
- (Windows) Como funciona o serviço Horário do Windows (Microsoft)
- (Windows) W32tm (Microsoft)
- (Windows) How the Windows Time service treats a leap second (Microsoft)
- (Windows) The story around Leap Seconds and Windows: It's likely not Y2K (Microsoft)

Controle do estado do processo para sua instância do Amazon Linux do EC2

C-states controlam os níveis de desativação que um núcleo pode assumir quando está inativo. Os C-states são numerados começando com C0 (o estado mais superficial em que o núcleo está totalmente ativo e executando instruções) até C6 (o estado de ociosidade mais profundo em que um núcleo está desativado).

Os P-states controlam a performance desejada (na frequência da CPU) de um núcleo. Os P-states são numerados começando com P0 (a configuração de performance mais elevada em que o núcleo pode usar a Intel Turbo Boost Technology para aumentar a frequência, se possível) e vão de P1 (o P-state que solicita a frequência máxima de linha de base) até P15 (a frequência mais baixa possível).

Estados C e estados P

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states e P-states do processador:

- Uso geral: `m4.10xlarge` | `m4.16xlarge` | `m5.metal` | `m5d.metal` | `m5n.metal` | `m5zn.metal` | `m6i.metal` | `m6id.metal` | `m7a.metal-48xl` | `m7i.metal-24xl` | `m7i.metal-48xl`
- Otimizada para computação: `c4.8xlarge` | `c5.metal` | `c5an.metal` | `c5adn.metal` | `c5n.metal` | `c6i.metal` | `c6id.metal` | `c7a.metal-48xl` | `c7i.metal-24xl` | `c7i.metal-48xl`
- Otimizadas para memória: `r4.8xlarge` | `r4.16xlarge` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r6i.metal` | `r7a.metal-48xl` | `r7i.metal-24xl` | `r7i.metal-48xl` | `r7iz.metal-16xl` | `r7iz.metal-32xl` | `u-6tb1.metal` | `u-9tb1.metal` | `u-12tb1.metal` | `u-18tb1.metal` | `u-24tb1.metal` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge` | `z1d.metal`
- Otimizadas para armazenamento: `d2.8xlarge` | `d3.metal` | `d3en.metal` | `i3.8xlarge` | `i3.16xlarge` | `i3.metal` | `i3en.metal` | `h1.8xlarge` | `h1.16xlarge`
- Computação acelerada: `f1.16xlarge` | `g3.16xlarge` | `g4dn.metal` | `p2.16xlarge` | `p3.16xlarge`

Somente estados C

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states do processador:

- Uso geral:`m5.12xlarge` | `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` | `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` | `m6a.24xlarge` | `m6a.48xlarge` | `m6ad.metal` | `m6i.16xlarge` | `m6i.32xlarge` | `m7a.medium` | `m7a.large` | `m7a.xlarge` | `m7a.2xlarge` | `m7a.4xlarge` | `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` | `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` | `m7i.xlarge` | `m7i.2xlarge` | `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge` | `m7i.24xlarge` | `m7i.48xlarge`
- Otimizadas para computação: `c5.9xlarge` | `c5.12xlarge` | `c5.18xlarge` | `c5.24xlarge` | `c5a.24xlarge` | `c5ad.24xlarge` | `c5d.9xlarge` | `c5d.12xlarge` | `c5d.18xlarge` | `c5d.24xlarge` | `c5n.9xlarge` | `c5n.18xlarge` | `c6a.24xlarge` | `c6a.32xlarge` | `c6a.48xlarge` | `c6i.16xlarge` | `c6i.32xlarge` | `c7a.medium` | `c7a.large` | `c7a.xlarge` | `c7a.2xlarge` | `c7a.4xlarge` | `c7a.8xlarge` | `c7a.12xlarge` | `c7a.16xlarge` | `c7a.24xlarge` | `c7a.32xlarge` | `c7a.48xlarge` | `c7i.large` | `c7i.xlarge` | `c7i.2xlarge` | `c7i.4xlarge` | `c7i.8xlarge` | `c7i.12xlarge` | `c7i.16xlarge` | `c7i.24xlarge` | `c7i.48xlarge`
- Otimizadas para memória:`r5.12xlarge` | `r5.24xlarge` | `r5d.12xlarge` | `r5d.24xlarge` | `r5n.12xlarge` | `r5n.24xlarge` | `r5dn.12xlarge` | `r5dn.24xlarge` |`r6a.24xlarge` | `r6a.48xlarge` | `r6i.16xlarge` | `r6i.32xlarge` | `r6id.32xlarge` | `r6in.32xlarge` | `r7a.medium` | `r7a.large` | `r7a.xlarge` | `r7a.2xlarge` | `r7a.4xlarge` | `r7a.8xlarge` | `r7a.12xlarge` | `r7a.16xlarge` | `r7a.24xlarge` | `r7a.32xlarge` | `r7a.48xlarge` | `r7i.large` | `r7i.xlarge` | `r7i.2xlarge` | `r7i.4xlarge` | `r7i.8xlarge` | `r7i.12xlarge` | `r7i.16xlarge` | `r7i.24xlarge` | `r7i.48xlarge` | `r7iz.large` | `r7iz.xlarge` | `r7iz.2xlarge` | `r7iz.4xlarge` | `r7iz.8xlarge` | `r7iz.12xlarge` | `r7iz.16xlarge` | `r7iz.32xlarge` | `u-6tb1.56xlarge` | `u-6tb1.112xlarge` | `u-9tb1.112xlarge` | `u-12tb1.112xlarge` | `u-18tb1.112xlarge` | `u-24tb1.112xlarge` | `u7i-12tb.224xlarge` | `u7in-16tb.224xlarge` | `u7in-24tb.224xlarge` | `u7in-32tb.224xlarge` | `z1d.6xlarge` | `z1d.12xlarge`
- Otimizadas para armazenamento: `d3en.12xlarge` | `dl1.24xlarge` | `i3en.12xlarge` | `i3en.24xlarge` | `i4i.metal` | `r5b.12xlarge` | `r5b.24xlarge` | `i4i.16xlarge`
- Com computação acelerada: `dl1.24xlarge` | `g5.24xlarge` | `g5.48xlarge` | `g6.24xlarge` | `g6.48xlarge` | `inf1.24xlarge` | `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `vt1.24xlarge`

Os processadores Graviton da AWS têm modos de economia de energia integrados e operam em uma frequência fixa. Portanto, eles não fornecem a capacidade para o sistema operacional controlar os C-states e P-states.

Talvez você queira alterar as configurações de C-state ou P-state para aumentar a consistência de performance do processador, reduzir a latência ou ajustar sua instância para uma workload específica. As configurações padrão de C-state e P-state proporcionam o performance máxima, que é o ideal para a maioria das workloads. Contudo, se sua aplicação se beneficiaria de latência reduzida ao custo de frequências superiores de single ou dual core, ou de uma performance consistente em frequências menores em oposição às frequências Turbo Boost expansíveis, considere experimentar as configurações de C-state ou P-state que estão disponíveis para essas instâncias.

Para obter informações sobre diferentes configurações de processador e como monitorar os efeitos da configuração para o Amazon Linux, consulte Processor state control for Amazon EC2 Amazon Linux instance no Amazon Linux 2 User Guide. Esses procedimentos foram escritos para o Amazon Linux e se aplicam a ele, mas também podem funcionar para outras distribuições do Linux com o kernel do Linux versão 3.9 ou mais recente. Para obter mais informações sobre outras distribuições do Linux e controle do estado do processador, consulte a documentação específica do seu sistema.

Otimizar as opções de CPU

Muitas instâncias do Amazon EC2 oferecem suporte a multithreading simultâneo, o que permite a execução de vários threads simultaneamente em um único núcleo de CPU. Cada thread é representado como uma CPU virtual (vCPU) na instância. Uma instância tem um número padrão de núcleos de CPU, que varia de acordo com o tipo de instância. Por exemplo, um tipo de instância `m5.xlarge` tem dois núcleos de CPU e dois threads por núcleo por padrão—: quatro vCPUs no total.

> **Note**
>
> Cada vCPU é um thread de um núcleo de CPU, exceto instâncias T2, M7a, Apple Silicon Mac e plataformas ARM de 64 bits como instâncias com processadores AWS Graviton.

Na maioria dos casos, há um tipo de instância do Amazon EC2 que tem uma combinação de memória e número de vCPUs para atender às suas workloads. No entanto, é possível especificar as seguintes opções de CPU para otimizar a instância para workloads ou necessidades de negócios específicas:

- Número de núcleos de CPU: é possível personalizar o número de núcleos de CPU para a instância. É possível fazer isso para otimizar potencialmente os custos de licenciamento do software com uma instância que tem quantidade de RAM suficiente para workloads com uso intensivo de memória, mas menos núcleos de CPU.
- Threads por núcleo: é possível desabilitar o multithreading especificando um único thread por núcleo de CPU. É possível fazer isso para determinadas workloads, como workloads de computação de alta performance (HPC).

É possível especificar essas opções de CPU durante a execução da instância. Não há cobrança adicional ou reduzida para especificar opções de CPU. Você será cobrado da mesma forma das instâncias executadas com opções de CPU padrão.

Tópicos

- Regras para especificar opções de CPU
- Núcleos de CPU e threads por núcleo de CPU por tipo de instância
- Especificar opções de CPU para a instância
- Visualizar as opções de CPU para a instância

Regras para especificar opções de CPU

Para especificar as opções de CPU para a instância, lembre-se das seguintes regras:

- Não é possível especificar opções de CPU para instâncias bare metal.
- As opções de CPU podem ser especificadas somente durante a execução da instância e não podem ser alteradas após a execução.
- Ao executar uma instância, especifique o número de núcleos de CPU e threads por núcleo na solicitação. Por obter exemplos de solicitação, consulte Especificar opções de CPU para a instância.
- O número total de vCPUs para a instância é o número de núcleos de CPU multiplicado pelos threads por núcleo. Para especificar um número personalizado de vCPUs, especifique um número válido de núcleos de CPU e threads por núcleo para o tipo de instância. Você não pode exceder o número padrão de vCPUs para a instância. Para ter mais informações, consulte Núcleos de CPU e threads por núcleo de CPU por tipo de instância.
- Para desabilitar o multithreading, especifique um thread por núcleo.

- Quando você altera o tipo de instância de uma instância existente, as opções de CPU são alteradas automaticamente para as opções de CPU padrão no novo tipo de instância.
- As opções de CPU especificadas depois de você interromper, iniciar ou reinicializar uma instância.

Núcleos de CPU e threads por núcleo de CPU por tipo de instância

As tabelas a seguir listam os tipos de instância que oferecem suporte à especificação de opções de CPU.

Conteúdo

- Instâncias de uso geral
- Instâncias otimizadas para computação
- Instâncias otimizadas para memória
- Instâncias otimizadas para armazenamento
- Instâncias computacionais aceleradas
- Instâncias de computação de alta performance

Instâncias de uso geral

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instâncias otimizadas para computação

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instâncias otimizadas para memória

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-6tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-12tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-24tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instâncias otimizadas para armazenamento

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instâncias computacionais aceleradas

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instâncias de computação de alta performance

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				48, 50, 52, 54, 56, 58, 60, 62, 64	

Especificar opções de CPU para a instância

É possível especificar as opções de CPU durante a execução da instância.

Os exemplos a seguir descrevem como especificar as opções de CPU ao usar o assistente de inicialização de instâncias no console do EC2 e o comando run-instances da AWS CLI, a página de criação de modelo de execução no console do EC2 e o comando create-launch-template da AWS CLI. Para frota do EC2 ou frota spot, especifique as opções da CPU em um modelo de execução.

Os seguintes exemplos são para um tipo de instância `r5.4xlarge`, que tem os seguintes valores padrão:

- Núcleos de CPU padrão: 8
- Threads padrão por núcleo: 2
- vCPUs padrão: 16 (8 x 2)
- Número válido de núcleos de CPU: 2, 4, 6 e 8
- Número válido de threads por núcleo: 1, 2

Desativar multithreading

Para desabilitar o multithreading, especifique 1 thread por núcleo.

New console

Como desabilitar o multithreading durante a execução da instância

1. Siga o procedimento Iniciar rapidamente uma instância e configure sua instância conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.

3. Em Core count (Contagem de núcleos), defina o número de núcleos de CPU necessário. Neste exemplo, para especificar a contagem de núcleos de CPU para uma instância `r5.4xlarge`, escolha 8.
4. Para desabilitar o multithreading, em Threads per core (Threads por núcleo), escolha 1.
5. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Old console

Como desabilitar o multithreading durante a execução da instância

1. Siga o procedimento do Inicie uma instância usando o assistente de inicialização de instância.
2. Na página Configure Instance Details (Configurar detalhes da instância), em CPU options (Opções de CPU), escolha Specify CPU options (Especificar opções de CPU).
3. Em Core count (Contagem de núcleos), defina o número de núcleos de CPU necessário. Neste exemplo, para especificar a contagem de núcleos de CPU para uma instância `r5.4xlarge`, escolha 8.
4. Para desabilitar o multithreading, em Threads per core (Threads por núcleo), escolha 1.
5. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para ter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância.

AWS CLI

Como desabilitar o multithreading durante a execução da instância

Use o comando run-instances da AWS CLI e especifique um valor de 1 para `ThreadsPerCore` no parâmetro `--cpu-options`. Em `CoreCount`, especifique o número de núcleos de CPU. Neste exemplo, para especificar a contagem de núcleos de CPU padrão para uma instância `r5.4xlarge`, especifique um valor de 8.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
```

```
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Especificar um número personalizado de vCPUs na inicialização

É possível personalizar o número de núcleos de CPU e de thread por núcleo da instância.

O exemplo apresentado a seguir inicia uma instância `r5.4xlarge` com quatro vCPUs.

New console

Para especificar um número personalizado de vCPUs durante a execução da instância

1. Siga o procedimento Iniciar rapidamente uma instância e configure sua instância conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.
3. Para obter quatro vCPUs, especifique dois núcleos de CPU e dois threads por núcleo, da seguinte forma:
   - Em Contagem de núcleos, escolha 2.
   - For Threads per core (Threads por núcleo), escolha 2.
4. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Old console

Para especificar um número personalizado de vCPUs durante a execução da instância

1. Siga o procedimento do Inicie uma instância usando o assistente de inicialização de instância.
2. Na página Configure Instance Details (Configurar detalhes da instância), em CPU options (Opções de CPU), escolha Specify CPU options (Especificar opções de CPU).
3. Para obter quatro vCPUs, especifique dois núcleos de CPU e dois threads por núcleo, da seguinte forma:
   - Em Contagem de núcleos, escolha 2.

- For Threads per core (Threads por núcleo), escolha 2.

4. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para ter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância.

AWS CLI

Para especificar um número personalizado de vCPUs durante a execução da instância

Use o comando run-instances da AWS CLI e especifique o número de núcleos de CPU e o número de threads no parâmetro `--cpu-options`. É possível especificar dois núcleos de CPU e dois threads por núcleo para obter quatro vCPUs.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

Como alternativa, especifique quatro núcleos de CPU e um thread por núcleo (desabilite o multithreading) para obter quatro vCPUs:

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Especificar um número personalizado de vCPUs em um modelo de execução

É possível personalizar o número de núcleos de CPU e de threads por núcleo para a instância em um modelo de execução.

O exemplo apresentado a seguir cria um modelo de execução que especifica a configuração para uma instância `r5.4xlarge` com quatro vCPUs.

Console

Para especificar um número personalizado de vCPUs em um modelo de execução

1. Siga o procedimento Criar um modelo de execução usando parâmetros e configure seu modelo de execução conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.
3. Para obter quatro vCPUs, especifique dois núcleos de CPU e dois threads por núcleo, da seguinte forma:
   - Em Contagem de núcleos, escolha 2.
   - For Threads per core (Threads por núcleo), escolha 2.
4. No painel Resumo, analise a configuração da sua instância e selecione Criar modelo de execução. Para ter mais informações, consulte Executar uma instância a partir de um modelo de execução.

AWS CLI

Para especificar um número personalizado de vCPUs em um modelo de execução

Use o comando create-launch-template da AWS CLI e especifique o número de núcleos de CPU e o número de threads no parâmetro `CpuOptions`. É possível especificar dois núcleos de CPU e dois threads por núcleo para obter quatro vCPUs.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo de arquivo JSON que contém os dados do modelo de execução, que incluem as opções de CPU, para a configuração da instância para este exemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
```

```
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Como alternativa, especifique quatro núcleos de CPU e um thread por núcleo (desabilite o multithreading) para obter quatro vCPUs:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

Visualizar as opções de CPU para a instância

É possível visualizar as opções de CPU de uma instância existente no console do Amazon EC2 ou descrevendo a instância usando a AWS CLI.

Console

Para visualizar as opções de CPU para uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Details (Detalhes), em Host and placement group (Host e grupo de posicionamento), localize Number of vCPUs (Número de vCPUs).

AWS CLI

Para visualizar as opções de CPU de uma instância (AWS CLI)

Use o comando describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
```

```
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

Na saída que é retornada, o campo `CoreCount` indica o número de núcleos para a instância. O campo `ThreadsPerCore` indica o número de threads por núcleo.

Como alternativa, para visualizar as informações da CPU, é possível realizar a conexão com a instância e usar uma das seguintes ferramentas do sistema:

- O Windows `Task Manager` na instância do Windows
- O comando lscpu na instância do Linux

É possível usar o AWS Config para fazer registros, auditorias e avaliações de alterações de configuração para instâncias, incluindo instâncias encerradas. Para obter mais informações, consulte Conceitos básicos do AWS Config no Guia do desenvolvedor do AWS Config.

AMD SEV-SNP no Amazon EC2

O AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) é um recurso de CPU que fornece as seguintes propriedades:

- Declaração: o AMD SEV-SNP permite que você recupere um relatório de declaração assinado que contém uma medida criptográfica que pode ser usada para validar o estado e a identidade da instância e se ela está sendo executada em hardware original da AMD. Para ter mais informações, consulte Declaração com o AMD SEV-SNP.
- Criptografia de memória: começando com os processadores AMD EPYC (Milan), AWS Graviton2 e Intel Xeon Scalable (Ice Lake), a memória da instância é sempre criptografada. As instâncias habilitadas para o AMD SEV-SNP usam uma chave específica da instância para sua criptografia de memória.

Conceitos e terminologia

Antes de começar a usar o AMD SEV-SNP, certifique-se de estar familiarizado com os conceitos e a terminologia a seguir.

Relatório de declaração AMD SEV-SNP

O relatório de declaração AMD SEV-SNP é um documento que uma instância pode solicitar para a CPU. O relatório de declaração AMD SEV-SNP pode ser usado para validar o estado e a identidade de uma instância e para verificar se ela está sendo executada em um ambiente AMD sancionado. O relatório inclui uma medição de inicialização, que é um hash criptográfico do estado inicial de inicialização de uma instância, incluindo o conteúdo da memória da instância inicial e o estado inicial das vCPUs. O relatório de declaração AMD SEV-SNP é assinado com uma assinatura VLEK que remonta a uma raiz de confiança da AMD.

VLEK

A Versioned Loaded Endossement Key (VLEK) é uma chave de assinatura versionada certificada pela AMD e usada pela CPU da AMD para assinar os relatórios de declaração do AMD SEV-SNP. As assinaturas VLEK podem ser validadas usando certificados fornecidos pela AMD.

Binário OVMF

O Open Virtual Machine Firmware (OVMF) é o código de inicialização antecipada usado para fornecer um ambiente UEFI para a instância. O código de inicialização antecipada é executado antes que o código na AMI seja inicializado. O OVMF também encontra e executa o carregador de inicialização fornecido na AMI. Para obter mais informações, consulte o repositório do OVMF.

Requisitos

Para usar o AMD SEV-SNP, você deve fazer o seguinte:

- Use um dos seguintes tipos de instância com suporte:
  - Uso geral: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Otimizadas para computação: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Otimizadas para memória: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Execute sua instância em um Região da AWS com suporte. Atualmente, há suporte apenas para Leste dos EUA (Ohio) e Europa (Irlanda).

- Use uma AMI com modo de inicialização `uefi` ou `uefi-preferred` e um sistema operacional com suporte a AMD SEV-SNP. Para obter mais informações sobre o suporte ao AMD SEV-SNP em seu sistema operacional, consulte a documentação do respectivo sistema operacional. Na AWS, o AMD SEV-SNP é compatível com AL2023, RHEL 9.3, SLES 15 SP4 e Ubuntu 23.04 e posterior.

Considerações

É possível ativar o AMD SEV-SNP somente ao iniciar uma instância. Quando o AMD SEV-SNP está ativado para a inicialização da instância, as regras apresentadas a seguir se aplicam.

- O AMD SEV-SNP não pode ser desativado. Ele permanece ativado durante todo o ciclo de vida da instância.
- É possível alterar o tipo de instância somente para outro tipo de instância com suporte para o AMD SEV-SNP.
- Não há suporte para o Hibernation e o Nitro Enclaves.
- Não há suporte para hosts dedicados.
- Se o host subjacente para a instância estiver programado para manutenção, você receberá uma notificação do evento programado 14 dias antes do evento. Você deverá interromper ou reiniciar manualmente sua instância para movê-la para um novo host.

Definição de preço

Quando você executa uma instância do Amazon EC2 com o AMD SEV-SNP ativado, é cobrada uma taxa adicional de uso por hora que equivale a 10% da taxa sob demanda por hora do tipo de instância selecionado.

Essa taxa de uso do AMD SEV-SNP é uma cobrança separada do uso da instância do Amazon EC2. Instâncias reservadas, Savings Plans e uso do sistema operacional não afetam essa taxa.

Se você configurar uma instância spot para iniciar com AMD SEV-SNP ativado, uma tarifa adicional de uso por hora será cobrada. Essa tarifa equivale a 10% da taxa sob demanda por hora do tipo de instância selecionado. Se a estratégia de alocação usar o preço como entrada, a frota spot não incluirá essa tarifa adicional; somente o preço spot será usado.

Trabalho com o AMD SEV-SNP no Amazon EC2

Conclua as tarefas apresentadas a seguir para trabalhar com o AMD SEV-SNP no Amazon EC2.

Tarefas

- Encontrar tipos de instância com suporte
- Ative o AMD SEV-SNP na execução
- Verificar o status do AMD SEV-SNP

Encontrar tipos de instância com suporte

É possível usar a AWS CLI para encontrar tipos de instância com suporte para o AMD SEV-SNP.

Para encontrar os tipos de instância que oferecem suporte ao AMD SEV-SNP usando a AWS CLI, use o comando describe-instance-types a seguir.

```
$ C:\> aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Saída de exemplo.

```
[
 "r6a.2xlarge",
 "m6a.large",
 "m6a.2xlarge",
 "r6a.xlarge",
 "c6a.16xlarge",
 "c6a.8xlarge",
 "m6a.4xlarge",
 "c6a.12xlarge",
 "r6a.4xlarge",
 "c6a.xlarge",
 "c6a.4xlarge",
 "c6a.2xlarge",
 "m6a.xlarge",
 "c6a.large",
 "r6a.large",
 "m6a.8xlarge"
]
```

Ative o AMD SEV-SNP na execução

É possível usar a AWS CLI para iniciar uma instância com o AMD SEV-SNP ativado.

Para iniciar uma instância com o AMD SEV-SNP ativado usando a AWS CLI, use o comando run-instances e inclua a opção `--cpu-options AmdSevSnp=enabled`. Em `--image-id`, especifique uma AMI com modo de inicialização `uefi` ou `uefi-prefered` e um sistema operacional com suporte a AMD SEV-SNP. Em `--instance-type`, especifique um tipo de instância com suporte.

```
$ C:\> aws ec2 run-instances \
--image-id supported_ami_id \
--instance-type supported_instance_type \
--key-name key_pair_name \
--subnet-id subnet_id \
--cpu-options AmdSevSnp=enabled
```

Verificar o status do AMD SEV-SNP

É possível usar um dos métodos apresentados a seguir para verificar o status do AMD SEV-SNP.

AWS CLI

Para verificar se o AMD SEV-SNP está ativado em uma instância usando a AWS CLI, use o comando describe-instances. Em `--instance-ids`, especifique o ID da instância a ser verificada.

```
$ C:\> aws ec2 describe-instances --instance-ids instance_id
```

Na saída do comando, o valor de `AmdSevSnp` em `CpuOptions` indica se o AMD SEV-SNP está ativado ou desativado.

AWS CloudTrail

No evento de AWS CloudTrail para a solicitação de execução da instância, um valor de `"cpuOptions": {"AmdSevSnp": enabled}` indica que o AMD SEV-SNP está ativado para a instância.

Declaração com o AMD SEV-SNP

A declaração é um processo que permite que sua instância prove seu estado e sua identidade. Ao ativar o AMD SEV-SNP para sua instância, é possível solicitar um relatório de declaração AMD SEV-SNP para o processador subjacente. O relatório de declaração do AMD SEV-SNP contém um hash criptográfico, chamado de medição de lançamento, do conteúdo inicial da memória do convidado e do estado inicial da vCPU. O relatório de declaração é assinado com uma assinatura VLEK que

remonta a uma raiz de confiança da AMD. É possível usar a medida de inicialização incluída no relatório de declaração para validar se a instância está sendo executada em um ambiente AMD genuíno e para validar o código de inicialização inicial usado para iniciar a instância.

Para realizar a declaração com o AMD SEV-SNP, conclua as etapas a seguir.

Etapa 1: obter o relatório de declaração

Nessa etapa, você instala e cria o utilitário `snpguest` e, em seguida, usa-o para solicitar o relatório de atestado e os certificados do AMD SEV-SNP.

1. Execute os comandos apresentados a seguir para desenvolver o utilitário `snpguest` usando o repositório snpguest repository.

```
$ C:\> git clone https://github.com/virtee/snpguest.git
$ C:\> cd snpguest
$ C:\> cargo build -r
$ C:\> cd target/release
```

2. Gere uma solicitação para o relatório de atestado. O utilitário solicita o relatório de atestado usando o host e o grava em um arquivo binário com os dados de solicitação fornecidos.

   O exemplo apresentado a seguir cria uma string de solicitação randômica e a utiliza como arquivo de solicitação (`request-file.txt`). Quando o comando retorna o relatório de atestado, ele é armazenado no caminho do arquivo especificado (`report.bin`). Nesse caso, o utilitário armazena o relatório no diretório atual.

```
$ C:\> ./snpguest report report.bin request-file.txt --random
```

3. Solicite os certificados usando a memória do host e armazene-os como arquivos PEM. O exemplo apresentado a seguir armazena os arquivos no mesmo diretório do utilitário `snpguest`. Se já existirem certificados no diretório especificado, esses certificados serão substituídos.

```
$ C:\> ./snpguest certificates PEM ./
```

Etapa 2: validar a assinatura do relatório de atestado

O relatório de declaração é assinado com um certificado, chamado Versioned Loaded Endossement Key (VLEK), emitido pela AMD para a AWS. Nessa etapa, é possível validar se o certificado VLEK é emitido pela AMD e se o relatório de atestado é assinado por esse certificado VLEK.

1. Faça o download dos certificados VLEK de raiz de confiança do site oficial da AMD para o diretório atual.

```
$ C:\> sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/
Milan/cert_chain -o ./cert_chain.pem
```

2. Use `openssl` para validar se o certificado VLEK está assinado pela raiz dos certificados de confiança da AMD.

```
$ C:\> sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

   Saída esperada:

```
certs/vcek.pem: OK
```

3. Use o utilitário `snpguest` para validar se o relatório de declaração foi assinado pelo certificado VLEK.

```
$ C:\> ./snpguest verify attestation ./ report.bin
```

   Saída esperada.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Adição de componentes do sistema do Windows usando a mídia de instalação

Os sistemas operacionais do Windows Server incluem muitos componentes opcionais. Não é prático incluir todos os componentes opcionais em cada AMI do Windows Server do Amazon EC2. Em vez disso, nós fornecemos a você snapshots do EBS de mídia de instalação que têm os arquivos necessários para configurar ou instalar componentes em sua instância do Windows.

Para acessar e instalar os componentes adicionais, é necessário encontrar o snapshot do EBS correto para sua versão do Windows Server, criar um novo volume do snapshot e anexar o volume à sua instância.

Antes de começar

Use o AWS Management Console ou a ferramenta da linha de comando para obter o ID da instância e a zona de disponibilidade de sua instância. É necessário criar seu volume do EBS na mesma zona de disponibilidade de sua instância.

Adicionar componentes do Windows usando o console

Use o seguinte procedimento para usar o AWS Management Console para adicionar componentes do Windows à sua instância.

Para adicionar componentes do Windows à sua instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Na barra Filter (Filtro), escolha Public Snapshots (Snapshots públicos).
4. Adicione o filtro Owner Alias (Alias de proprietário) e escolha amazon.
5. Adicione o filtro Description (Descrição) e insira **`Windows`**.
6. Pressione Enter
7. Selecione o snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo, selecione Windows 2019 English Installation Media se sua instância estiver executando o Windows Server 2019.
8. Escolha Actions (Ações), Create volume from snapshot (Criar volume a partir do snapshot).
9. Para Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade que corresponde à instância do Windows. Escolha Add Tag (Adicionar tag) e insira **`Name`** para a chave de tag e um nome descritivo para o valor da tag. Escolha Create volume (Criar volume).
10. Na mensagem Volume Successfully Created (Volume criado com êxito, banner verde), escolha o volume que você acabou de criar.
11. Escolha Actions (Ações), Attach volume (Anexar volume).
12. Em Instance (Instância) selecione o ID da instância.

13. Em Device name (Nome do dispositivo), insira o nome do dispositivo para o anexo. Se precisar de ajuda com o nome do dispositivo, consulte Nomes de dispositivos em instâncias do Amazon EC2.
14. Selecione Attach volume (Anexar volume).
15. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

    > **Important**
    >
    > Não inicialize o volume.

16. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
17. (Opcional) Ao terminar de usar a mídia de instalação, será possível desanexar o volume. Depois de desanexar o volume, será possível excluí-lo.

Adicionar componentes do Windows usando o Tools for Windows PowerShell

Use o seguinte procedimento para usar a Tools for Windows PowerShell para adicionar componentes do Windows à sua instância.

Adição de componentes do Windows à instância usando o Tools for Windows PowerShell

1. Use o cmdlet Get-EC2Snapshot com os filtros `Owner` e `description` para obter uma lista dos snapshots de mídia de instalação disponíveis.

   ```
   PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";
    Values="Windows*" }
   ```

2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

   ```
   ...
   DataEncryptionKeyId :
   Description         : Windows 2019 English Installation Media
   Encrypted           : False
   KmsKeyId            :
   OwnerAlias          : amazon
   ```

```
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-22da283e
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-be5eafcb
VolumeSize          : 6
...
```

3. Use o cmdlet New-EC2Volume para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. Na saída, observe o ID do volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-22da283e
State            : creating
Tags             : {}
VolumeId         : vol-06aa9e1fbf8b82ed1
VolumeType       : gp2
```

5. Use o cmdlet Add-EC2Volume para associar o volume à sua instância.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

> **Important**
>
> Não inicialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
8. (Opcional) Ao terminar de usar a mídia de instalação, use o cmdlet Dismount-EC2Volume para desanexar o volume da instância. Depois de desanexar o volume, é possível usar o cmdlet Remove-EC2Volume para excluir o volume.

Adicionar componentes do Windows usando a AWS CLI

Use o seguinte procedimento para usar o AWS CLI para adicionar componentes do Windows à sua instância.

Para adicionar componentes do Windows à sua instância usando a AWS CLI

1. Use o comando describe-snapshots com o parâmetro `owner-ids` e o filtro `description` para obter uma lista dos snapshots de mídia de instalação disponíveis.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
 Name=description,Values=Windows*
```

2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
```

```
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Use o comando create-volume para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-
zone us-east-1a
```

4. Na saída, observe o ID do volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-0c98b37f30bcbc290",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-22da283e",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Use o comando attach-volume para associar o volume à sua instância.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

> **Important**
>
> Não inicialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.

8. (Opcional) Ao terminar de usar a mídia de instalação, use o comando detach-volume para desanexar o volume da instância. Depois de desanexar o volume, é possível usar o comando delete-volume para excluir o volume.

Gerenciamento de usuários do sistema na instância do Linux

Cada tipo de instância do Linux é iniciada com um usuário padrão do sistema Linux. Você pode adicionar e excluir usuários da instância.

Para o usuário padrão, o nome de usuário padrão é determinado pela AMI especificada quando você iniciou a instância.

> **Note**
>
> Por padrão, a autenticação por senha e o login raiz estão desabilitados e o sudo está habilitado. Para fazer login na instância, você deve criar um par de chaves. Para obter mais informações sobre login, consulte Conecte-se à sua instância do Linux.
> Você pode permitir a autenticação por senha e o login raiz na instância. Para obter mais informações, consulte a documentação do seu sistema operacional.

> **Note**
>
> Os usuários do sistema Linux não devem ser confundidos com os usuários do IAM. Para obter mais informações, consulte Usuários IAM no Manual do usuário IAM.

Conteúdo

- Nomes de servidores padrão
- Considerações
- Criar um usuário
- Remover um usuário

Nomes de servidores padrão

O nome de usuário padrão para a instância do EC2 é determinado pela AMI especificada quando você iniciou instância.

Os nomes de usuário padrão são:

- Para AL2023, Amazon Linux 2 ou Amazon Linux AMI, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Debian, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.

> **Note**
>
> Para encontrar o nome de usuário padrão para outras distribuições Linux, verifique com o fornecedor da AMI.

Considerações

O uso do usuário padrão é adequado para muitas aplicações. Porém, você pode escolher adicionar usuários para que as pessoas possam ter seus próprios arquivos e espaços de trabalho. Além disso, a criação usuários para novos usuários é muito mais segura do que conceder a vários usuários (possivelmente inexperientes) acesso ao usuário padrão, pois essa conta pode causar muitos danos a um sistema quando usada de modo inadequado. Para obter mais informações, consulte Dicas para proteger sua instância do EC2.

Para permitir aos usuários acesso SSH à sua instância do EC2 usando um usuário do sistema Linux, é necessário compartilhar a chave SSH com o usuário. Uma outra opção é usar o EC2 Instance Connect para fornecer acesso aos usuários sem precisar compartilhar e gerenciar as chaves SSH. Para ter mais informações, consulte Conectar-se à instância do Linux com o EC2 Instance Connect.

Criar um usuário

Primeiro crie o usuário e, depois, adicione a chave pública SSH que permitirá que ele se conecte e faça login na instância.

Como criar um usuário

1. Crie um novo par de chaves. É necessário fornecer o arquivo `.pem` ao usuário para o qual você está criando o usuário. Ele deve usar esse arquivo para se conectar à instância.
2. Recupere a chave pública do par de chaves criado na etapa anterior.

   ```
   $ C:\>  ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   O comando retorna a chave pública, como mostrado no exemplo a seguir.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Conecte-se à instância.
4. Use o comando adduser para criar o usuário e adicioná-lo ao sistema (com uma entrada no arquivo `/etc/passwd`). O comando também cria um grupo e um diretório inicial para o usuário. Neste exemplo de configuração, o usuário é deniminado *`newuser`*.

   - Amazon Linux e Amazon Linux 2

     Com o Amazon Linux e o Amazon Linux 2, o usuário é criada com a autenticação por senha desabilitada por padrão.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Inclua o parâmetro `--disabled-password` para criar o usuário com autenticação por senha desabilitada.

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. Mude para o novo usuário, de modo que o diretório e o arquivo criados pertençam aos proprietários adequados.

```
[ec2-user ~]$ sudo su - newuser
```

O prompt é alterado de `ec2-user` para *`newuser`* para indicar que você mudou a sessão do shell para o novo usuário.

6. Adicione a chave pública SSH ao usuário. Primeiro, crie um diretório no diretório inicial do usuário para o arquivo de chave SSH. Depois disso, crie o arquivo de chave e, por fim, cole a chave pública no arquivo de chave, conforme descrito nas etapas secundárias a seguir.

   a. Crie um diretório `.ssh` no diretório inicial *`newuser`* e altere suas permissões de arquivos para `700` (somente o proprietário pode ler, gravar ou abrir o diretório).

   ```
   [newuser ~]$ mkdir .ssh
   ```

   ```
   [newuser ~]$ chmod 700 .ssh
   ```

   > **Important**
   >
   > Sem essas permissões de arquivos, o usuário não poderá se conectar.

   b. Crie um arquivo chamado `authorized_keys` no diretório `.ssh` e altere suas permissões de arquivos para `600` (somente o proprietário pode ler ou gravar no arquivo).

   ```
   [newuser ~]$ touch .ssh/authorized_keys
   ```

   ```
   [newuser ~]$ chmod 600 .ssh/authorized_keys
   ```

   > **Important**
   >
   > Sem essas permissões de arquivos, o usuário não poderá se conectar.

   c. Abra o arquivo `authorized_keys` usando seu editor de texto favorito (como vim ou nano).

   ```
   [newuser ~]$ nano .ssh/authorized_keys
   ```

   Cole a chave pública recuperada na Etapa 2 no arquivo e salve as alterações.

> **Important**
>
> Cole a chave pública em uma linha contínua. A chave pública não deve ser dividida em várias linhas.

Agora, o usuário deve poder fazer login no usuário *newuser* na instância usando a chave privada correspondente à chave pública adicionada ao arquivo `authorized_keys`. Para obter mais informações sobre os diferentes métodos de conexão a uma instância do Linux, consulte Conecte-se à sua instância do Linux.

Remover um usuário

Se um usuário não for mais necessário, será possível removê-lo para que não possa mais ser usado.

Use o comando userdel para remover o usuário do sistema. Quando você especifica o parâmetro `-r`, o diretório inicial e o spool de e-mail do usuário são excluídos. Para manter o diretório inicial e o spool de e-mail do usuário, omita o parâmetro `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Definição da senha do administrador do Windows para a instância

Quando se conectar a uma instância do Windows, especifique uma conta de usuário e uma senha que tenha permissão para acessar a instância. A primeira vez que se conectar a uma instância, será solicitado que você especifique a conta de administrador e a senha padrão.

Com as AMIs do Windows na AWS para o Windows Server 2012 R2 e para versões anteriores, Configuração de uma instância do Windows usando o serviço EC2Config (herdado) gera a senha padrão. Com as AMIs do Windows na AWS para o Windows Server 2016 e 2019, Configurar uma instância do Windows usando o EC2Launch gera a senha padrão. Com as AMIs do Windows na AWS para o Windows Server 2022 e para versões posteriores, Configurar uma instância do Windows usando o EC2Launch v2 gera a senha padrão.

> **Note**
>
> Com o Windows Server 2016 e posterior, a opção `Password never expires` é desabilitada para o administrador local. Com o Windows Server 2012 R2 e anteriores, a opção `Password never expires` é habilitada para o administrador local.

Alterar a senha de administrador após a conexão

Quando você se conectar a uma instância pela primeira vez, recomendamos alterar a senha de administrador de seu valor padrão. Use o procedimento a seguir para alterar a senha de administrador para uma instância do Windows.

> **Important**
>
> Armazene a nova senha em um lugar seguro. Você não poderá recuperar a nova senha usando o console do Amazon EC2. O console só pode recuperar a senha padrão. Se você tentar se conectar à instância usando a senha padrão depois de alterá-la, será exibido o erro "Suas credenciais não funcionaram".

Para alterar a senha de administrador local

1. Conecte-se à instância e abra o prompt de comando.
2. Execute o seguinte comando. Se sua nova senha incluir caracteres especiais, coloque a senha entre aspas duplas.

```
net user Administrator "new_password"
```

3. Armazene a nova senha em um lugar seguro.

Alterar uma senha perdida ou expirada

Se a senha for perdida ou expirar, será possível gerar uma nova senha. Para obter os procedimentos de redefinição de senha, consulte Redefinir uma senha de administrador do Windows perdida ou expirada.

Gerenciamento de drivers de dispositivo para a instância do Amazon EC2

Alguns drivers não estão instalados previamente na AMI do EC2 de qual você realiza a inicialização. Outros podem necessitar de atualizações para utilizar a funcionalidade expandida. Os tópicos apresentados a seguir abordam a instalação, as atualizações e a configuração de alguns dos drivers de dispositivo conectados às instâncias do EC2.

Conteúdo

- Instalação de drivers da NVIDIA na instância do Amazon EC2
- Instalação de drivers da AMD na instância do Amazon EC2
- Drivers paravirtuais para as instâncias do Windows
- Drivers AWS NVMe para instâncias do Windows

Instalação de drivers da NVIDIA na instância do Amazon EC2

Uma instância com uma GPU NVIDIA conectada, como P3 ou G4dn, deve ter o driver NVIDIA apropriado instalado. Dependendo do tipo de instância, é possível baixar um driver NVIDIA público, um driver do Amazon S3 disponível somente para clientes da AWS ou usar uma AMI com o driver pré-instalado.

Para instalar drivers da AMD em uma instância com uma GPU da AMD conectada, como uma instância G4ad, consulte Instalar drivers AMD. Para instalar os drivers da NVIDIA, consulte Instalar drivers NVIDIA.

Sumário

- Tipos de drivers NVIDIA
- Drivers disponíveis por tipo de instância
- Opções de instalação
  - Opção 1: AMIs com os drivers NVIDIA instalados
  - Opção 2: Drivers NVIDIA públicos
  - Opção 3: drivers GRID (instâncias G6, Gr6, G5, G4dn e G3)
  - Opção 4: drivers para jogos NVIDIA (instâncias G5 e G4dn)
- Instalar uma versão adicional do CUDA

Tipos de drivers NVIDIA

A seguir estão os principais tipos de drivers NVIDIA que podem ser usados com as instâncias baseadas em GPU.

Drivers Tesla

Esses drivers são destinados principalmente a workloads de computação, que usam GPUs para tarefas computacionais, como cálculos de ponto flutuante paralelizados para machine learning e transformações rápidas de Fourier para aplicações de computação de alta performance.

Drivers GRID

Esses drivers são certificados para oferecer a melhor performance para aplicações de visualização profissional que renderizam conteúdo, como modelos 3D ou vídeos de alta resolução. É possível configurar os drivers GRID para oferecer suporte a dois modos. As estações de trabalho virtuais Quadro fornecem acesso a quatro monitores de 4K por GPU. Os GRID vApps oferecem recursos de hospedagem de aplicações RDSH.

Drivers para jogos

Esses drivers contêm otimizações para jogos e são atualizados frequentemente para oferecer melhorias de performance. Eles são compatíveis com um único monitor 4K por GPU.

Modo configurado

No Windows, os drivers Tesla são configurados para serem executados no modo Tesla Compute Cluster (TCC). O driver GRID e o driver para jogos são configurados para executar no modo Windows Display Driver Model (WDDM). No modo TCC, a placa é dedicada a workloads de computação. No modo WDDM, a placa é compatível com workloads de computação e gráficos.

Painel de controle NVIDIA

O painel de controle NVIDIA é compatível com drivers GRID e para jogos. Ele não é compatível com drivers Tesla.

APIs com suporte para drivers Tesla, GRID e para jogos

- OpenCL, OpenGL e Vulkan
- NVIDIA CUDA e bibliotecas relacionadas (por exemplo, cuDNN, TensorRT, nvJPEG e cuBLAS)

- NVENC para codificação de vídeo e NVDEC para decodificação de vídeo
- APIs somente para Windows: DirectX, Direct2D, DirectX Video Acceleration e DirectX Raytracing

Drivers disponíveis por tipo de instância

A tabela a seguir resume os drivers NVIDIA para cada tipo de instância de GPU.

Tipo de instância	Driver Tesla	Driver GRID	Driver para jogos
G3	Sim	Sim	Não
G4dn	Sim	Sim	Sim
G5	Sim	Sim	Sim
G5g	Sim [1]	Não	Não
G6	Sim	Sim	Não
Gr6	Sim	Sim	Não
P2	Sim	Não	Não
P3	Sim	Não	Não
P4d	Sim	Não	Não
P4de	Sim	Não	Não

[1] Esse driver da Tesla também oferece suporte a aplicações gráficas otimizadas, específicas da plataforma ARM64

[2] Usando somente AMIs Marketplace

Opções de instalação

Use uma das opções a seguir para obter os drivers NVIDIA necessários para a instância de GPU.

Opções

- Opção 1: AMIs com os drivers NVIDIA instalados
- Opção 2: Drivers NVIDIA públicos
- Opção 3: drivers GRID (instâncias G6, Gr6, G5, G4dn e G3)
- Opção 4: drivers para jogos NVIDIA (instâncias G5 e G4dn)

Opção 1: AMIs com os drivers NVIDIA instalados

A AWS e a NVIDIA oferecem imagens de máquina da Amazon (AMIs) diferentes com drivers NVIDIA instalados.

- Ofertas do Marketplace com o driver Tesla
- Ofertas do Marketplace com o driver GRID
- Ofertas do Marketplace com o driver para jogos

Para analisar as considerações que dependem da plataforma do seu sistema operacional (SO), escolha a guia que se aplica à sua AMI.

Linux

Para atualizar a versão do driver instalada usando uma dessas AMIs, será necessário desinstalar os pacotes do NVIDIA da instância para evitar conflitos de versão. Use este comando para desinstalar os pacotes do NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

O pacote do toolkit CUDA tem dependências nos drivers NVIDIA A desinstalação dos pacotes NVIDIA apaga o toolkit CUDA. É necessário reinstalar o toolkit CUDA depois de instalar o driver NVIDIA.

Windows

Se você criar uma AMI do Windows personalizada usando uma das ofertas do AWS Marketplace, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o driver do GRID funcione. Para ter mais informações, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.

Opção 2: Drivers NVIDIA públicos

As opções oferecidas pela AWS são acompanhadas da licença necessária para o driver. Também é possível instalar os drivers públicos e trazer sua própria licença. Para instalar um driver público, baixe-o do site da NVIDIA conforme descrito aqui.

Também é possível usar as opções oferecidas pela AWS em vez dos drivers públicos. Para usar um driver GRID em uma instância P3, use as AMIs do AWS Marketplace conforme descrito na Opção 1. Para usar um driver GRID em uma instância G6, Gr6, G5, G4dn ou G3, use as AMIs do AWS Marketplace, conforme descrito na Opção 1, ou instale os drivers NVIDIA fornecidos pela AWS, conforme descrito na Opção 3: drivers GRID (instâncias G6, Gr6, G5, G4dn e G3).

Como fazer download de um driver NVIDIA público

Entre em sua instância e faça o download do driver da NVIDIA de 64 bits apropriado para o tipo de instância em http://www.nvidia.com/Download/Find.aspx. Para Tipo de produto, Séries de produtos e Produto, use as opções na tabela a seguir.

Instância	Tipo de produto	Séries de produtos	Produto
G3	Tesla	M-Class	M60
G4dn	Tesla	Série T	T4
G5 [1]	Tesla	A-Series	A10
G5g [2]	Tesla	Série T	NVIDIA T4G
G6 [3]	Tesla	L-Series	L4
Gr6 [3]	Tesla	L-Series	L4
P2	Tesla	K-Series	K80
P3	Tesla	V-Series	V100
P4d	Tesla	A-Series	A100
P4de	Tesla	A-Series	A100
P5[4]	Tesla	H-Series	H100

[1] As instâncias G5 requerem a versão de driver 470.00 ou posterior.

[2] As instâncias G5g requerem a versão de driver 470.82.01 ou posterior. O sistema operacional é o Linux aarch64.

[3] As instâncias G6 e Gr6 requerem um driver que esteja na versão 525.0 ou em versões posteriores.

[4] As instâncias P5 requerem um driver que esteja na versão 530 ou em versões posteriores.

Para instalar o driver da NVIDIA em sistemas operacionais do Linux, consulte o NVIDIA Driver Installation Quickstart Guide.

Para instalar o driver da NVIDIA no Windows, siga estas etapas:

1. Abra a pasta onde você fez download do driver e execute o arquivo de instalação. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.
2. Desabilite o adaptador de vídeo chamado Microsoft Basic Display Adapter, que está marcado com um ícone de aviso, usando o Gerenciador de dispositivos. Instale esses recursos do Windows: Media Foundation e Quality Windows Audio Video Experience.

   > **Important**
   >
   > Não desabilite o adaptador de vídeo chamado Microsoft Remote Display Adapter. Se o Microsoft Remote Display Adapter estiver desabilitado, sua conexão poderá ser interrompida e as tentativas de conexão com a instância após a reinicialização poderão falhar.

3. Verifique o gerenciador de dispositivos para certificar-se de que a GPU está funcionando corretamente.
4. Para obter a melhor performance na GPU, siga as etapas de otimização em Otimização das configurações de GPU em instâncias do Amazon EC2.

Opção 3: drivers GRID (instâncias G6, Gr6, G5, G4dn e G3)

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer o download, para cumprir os requisitos da solução da AWS que estão mencionados no Contrato de Licença de Usuário Final (EULA) da nuvem da NVIDIA GRID, você concorda em usar o software baixado somente para desenvolver AMIs para uso com os hardwares NVIDIA L4, NVIDIA A10G, NVIDIA Tesla T4 ou

NVIDIA Tesla M60. Após a instalação do software, você estará vinculado aos termos do Contrato de licença de usuário final em nuvem do NVIDIA GRID. Para obter informações sobre a versão do driver NVIDIA GRID para seu sistema operacional, consulte a documentação do software NVIDIA® Virtual GPU (vGPU) no site da NVIDIA.

Considerações

- As instâncias G6 e Gr6 requerem GRID 17 ou versões posteriores.
- As instâncias G5 requerem o GRID 13.1 ou posterior (ou o GRID 12.4 ou posterior).
- A resolução de DNS fornecida pela AWS é exigida pelas instâncias G3 para que o licenciamento do GRID funcione.
- IMDSv2 só é compatível com o driver NVIDIA versão 14.0 ou superior.
- Para instâncias do Windows, se você iniciar a instância usando uma AMI do Windows personalizada, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o driver do GRID funcione. Para ter mais informações, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.
- O GRID 17.0 e as versões posteriores não são compatíveis com o Windows Server 2019.
- O GRID 14.2 e as versões posteriores não são compatíveis com o Windows Server 2016.
- O GRID 17.0 e as versões posteriores não são compatíveis com as instâncias G3.

Amazon Linux e Amazon Linux 2

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância do Linux.
2. Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

   > **Important**
   >
   > Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo yum install gcc make
```

4. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

5. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

6. Reconecte-se à sua instância depois de reinicializá-la.
7. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

8. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Se você estiver usando o Amazon Linux 2 com o kernel versão 5.10, use o comando a seguir para instalar o driver GRID.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

    ```
    [ec2-user ~]$ nvidia-smi -q | head
    ```

12. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
    etc/modprobe.d/nvidia.conf
    ```

13. Reinicialize a instância.

    ```
    [ec2-user ~]$ sudo reboot
    ```

14. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, NICE DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Para CentOS 7 e Red Hat Enterprise Linux 7

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Recompile a configuração do Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

13. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, NICE DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

    c. Instale o pacote de GUI de desktop/estação de trabalho.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 e Red Hat Enterprise Linux 8

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, NICE DCV.

b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

c. Instale o pacote de GUI de estação de trabalho.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

Como instalar o driver NVIDIA GRID na instância do Linux

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, NICE DCV.

b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Ubuntu e Debian

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Atualize o pacote `linux-aws` para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Atualize o pacote para receber a versão mais recente.

```
$ sudo apt-get upgrade -y
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
```

```
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Recompile a configuração do Grub.

```
$ sudo update-grub
```

8. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
$ nvidia-smi -q | head
```

12. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

```
$ sudo reboot
```

14. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, NICE DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

    c. Instale o pacote de GUI de desktop/estação de trabalho.

    ```
    $ sudo apt-get install -y lightdm ubuntu-desktop
    ```

Sistemas operacionais do Windows

Como instalar o driver NVIDIA GRID na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

> **Important**
>
> Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Faça download dos drivers e do Contrato de licença de usuário final do NVIDIA GRID do Amazon S3 para o seu desktop usando os comandos do PowerShell a seguir.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Várias versões de driver NVIDIA GRID são armazenadas nesse bucket. É possível fazer download de todas as versões do Windows disponíveis no bucket removendo a opção `-KeyPrefix $KeyPrefix`. Para obter informações sobre a versão do driver NVIDIA GRID para seu sistema operacional, consulte a documentação do software NVIDIA® Virtual GPU (vGPU) no site da NVIDIA.

   Começando no GRID versão 11.0, é possível usar os drivers no `latest` para instâncias G3 e G4dn. Não adicionaremos versões posteriores à 11.0 ao `g4/latest`, mas manteremos a versão 11.0 e as versões anteriores específicas ao G4dn no `g4/latest`.

   As instâncias G5 requerem o GRID 13.1 ou posterior (ou o GRID 12.4 ou posterior).

4. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos.

5. (Opcional) Use o comando a seguir para desabilitar a página de licenciamento no painel de controle a fim de impedir que os usuários mudem acidentalmente o tipo de produto (a NVIDIA GRID Virtual Workstation é habilitada por padrão). Para obter mais informações, consulte Guia do usuário de licenciamento do GRID.

   PowerShell

   Execute os seguintes comandos da PowerShell para criar o valor do registro e desativar a página de licenciamento no painel de controle. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

   Prompt de comando

   Execute o comando de registro a seguir para criar o valor do registro para desabilitar a página de licenciamento no painel de controle. É possível executá-lo usando a janela do prompt de comando ou uma versão de 64 bits do PowerShell.

   ```
   reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
    NvCplDisableManageLicensePage /t REG_DWORD /d 1
   ```

6. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

   a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, NICE DCV.

   b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Opção 4: drivers para jogos NVIDIA (instâncias G5 e G4dn)

Esses drivers estão disponíveis somente para clientes da AWS. Ao baixá-los, você concorda em usar o software baixado somente para desenvolver AMIs para uso com os hardwares NVIDIA A10G e

NVIDIA Tesla T4. Após a instalação do software, você estará vinculado aos termos do Contrato de licença de usuário final em nuvem do NVIDIA GRID.

Considerações

- A resolução de DNS fornecida pela AWS é exigida pelas instâncias G3 para que o licenciamento do GRID funcione.
- IMDSv2 só é compatível com o driver NVIDIA versão 495.x ou superior.

Pré-requisito

Antes de instalar os drivers de jogos da NVIDIA, verifique se a AWS CLI está instalada na sua instância e as credenciais padrão estão configuradas. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

> **Important**
>
> Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

Amazon Linux e Amazon Linux 2

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux.
2. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.

6. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

7. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Se você estiver usando o Amazon Linux 2 com o kernel versão 5.10, use o comando a seguir para instalar os drivers de jogos NVIDIA.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Para versões de 440.68 a 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Para versões anteriores

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

13. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

14. Reinicialize a instância.

    ```
    [ec2-user ~]$ sudo reboot
    ```

15. (Opcional) Para ajudar a aproveitar um único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV.

Para CentOS 7 e Red Hat Enterprise Linux 7

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Recompile a configuração do Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

    Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Use o comando a seguir para fazer download e renomear o arquivo de certificação.

    - Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

14. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

15. (Opcional) Para ajudar a aproveitar um único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

CentOS Stream 8 e Red Hat Enterprise Linux 8

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

14. (Opcional) Para ajudar a aproveitar um único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV.

Rocky Linux 8

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
[ec2-user ~]$ sudo yum update -y
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Reconecte-se à sua instância depois de reinicializá-la.
5. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-devel kernel-devel-$(uname -r)
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
```

```
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Para versões de 440.68 a 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Para versões anteriores

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Reinicialize a instância.

    ```
    [ec2-user ~]$ sudo reboot
    ```

14. (Opcional) Para ajudar a aproveitar um único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV.

Ubuntu e Debian

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.

2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
$ sudo apt-get update -y
```

3. Atualize o pacote `linux-aws` para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Recompile a configuração do Grub.

```
$ sudo update-grub
```

8. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. Execute o instalador usando o comando a seguir:

```
$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

12. Use o comando a seguir para criar o arquivo de configuração necessário.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Para versões de 440.68 a 445.48:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

- Para versões anteriores

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Reinicialize a instância.

```
$ sudo reboot
```

16. (Opcional) Para ajudar a aproveitar um único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

Sistemas operacionais do Windows

Antes de instalar um driver NVIDIA para jogos na instância, é necessário garantir que os pré-requisitos apresentados a seguir sejam atendidos, além das considerações mencionadas para todos os drivers para jogos.

- Se você iniciar a instância do Windows usando uma AMI do Windows personalizada, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o driver de jogo funcione. Para ter mais informações, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.
- Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

Como instalar o driver para jogos NVIDIA na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download e instale o driver para jogos usando os seguintes comandos do PowerShell.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Muitas versões do driver NVIDIA GRID são armazenadas neste bucket do S3. Você pode baixar todas as versões disponíveis no bucket se alterar o valor da variável `$KeyPrefix` de “windows/latest” para "windows".
3. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o Gerenciador de Dispositivos.
4. Use um dos métodos a seguir para registrar o driver.

   Version 527.27 or above

   Crie a chave de registro a seguir com a versão de 64 bits do PowerShell ou a janela do prompt de comando.

   chave: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   nome: VGamingMarketplace

   tipo: DWord

   value: 2

PowerShell

Execute o comando a seguir do PowerShell para criar esse valor de registro. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
 -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt de comando

Execute o seguinte comando do registro para criar esse valor de registro. É possível executá-lo usando a janela do prompt de comando ou uma versão de 64 bits do PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Crie a chave de registro a seguir com a versão de 64 bits do PowerShell ou a janela do prompt de comando.

chave: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nome: VGamingMarketplace

tipo: DWord

value: 2

PowerShell

Execute o comando a seguir do PowerShell para criar esse valor de registro. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt de comando

Execute o seguinte comando do registro para criar essa chave de registro com a janela do prompt de comando. Você também pode usar esse comando na versão de 64 bits do PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Execute o seguinte comando no PowerShell. Essa ação baixará o arquivo de certificação, renomeará o arquivo como `GridSwCert.txt` e o moverá para a pasta Public Documents (Documentos Públicos) no drive do sistema. Normalmente, o caminho da pasta é `C:\Users\Public\Documents`.

   - Para a versão 461.40 ou posterior:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Para a versão 445.87:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Para versões anteriores

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   > **Note**
   >
   > Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell.

Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

6. Reinicie a instância.
7. Verifique a licença do NVIDIA Gaming usando o comando a seguir.

```
C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\nvidia-smi.exe -q
```

A saída deve ser semelhante ao seguinte.

```
vGPU Software Licensed Product
Product Name                : NVIDIA Cloud Gaming
License Status              : Licensed (Expiry: N/A)
```

8. (Opcional) Para ajudar a aproveitar o único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance NICE DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

Instalar uma versão adicional do CUDA

Depois de instalar um driver gráfico NVIDIA em sua instância, será possível instalar uma versão do CUDA diferente da versão fornecida com o driver gráfico. O procedimento a seguir demonstra como configurar várias versões do CUDA na instância.

Instalação do kit de ferramentas CUDA no Linux

Siga estas etapas para instalar o kit de ferramentas CUDA no Linux:

1. Conecte-se à sua instância do Linux.
2. Abra o site da NVIDIA e selecione a versão do CUDA que você precisa.
3. Selecione a arquitetura, a distribuição e a versão do sistema operacional em sua instância. Em Installer Type (Tipo de instalador), selecione runfile (local).
4. Siga as instruções para fazer download do script de instalação.

5. Adicione permissões de execução ao script de instalação que você obteve por download usando o comando a seguir.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Execute o script de instalação como mostrado a seguir para instalar o toolkit do CUDA e adicionar o número da versão do CUDA ao caminho do toolkit.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --
samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-
opengl-libs
```

7. (Opcional) Defina a versão padrão do CUDA da seguinte forma.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Instalação do kit de ferramentas CUDA no Windows

Siga estas etapas para instalar o kit de ferramentas CUDA no Windows:

Como instalar o toolkit do CUDA

1. Conecte-se à sua instância do Windows.
2. Abra o site da NVIDIA e selecione a versão do CUDA que você precisa.
3. Em Installer Type (Tipo de instalador), selecione exe (local) e escolha Download (Fazer download).
4. Usando seu navegador, execute o arquivo de instalação obtido por download. Siga as instruções para instalar o toolkit do CUDA. Talvez seja necessário reinicializar a instância.

Instalação de drivers da AMD na instância do Amazon EC2

Uma instância com uma GPU AMD conectada, como uma instância G4ad, deve ter o driver AMD apropriado instalado. Dependendo de suas necessidades, você pode usar uma AMI com o driver pré-instalado ou baixar um driver de Amazon S3.

Para instalar drivers NVIDIA em uma instância com uma GPU NVIDIA conectada, como uma instância G4dn, consulte Instalar drivers NVIDIA.

Sumário

- Software AMD Radeon Pro para driver empresarial
- AMIs com o driver AMD instalado
- Download do driver AMD
- Configuração de uma área de trabalho interativa para o Linux

Software AMD Radeon Pro para driver empresarial

O driver AMD Radeon Pro Software for Enterprise foi criado para oferecer suporte a casos de uso de gráficos de nível profissional. Usando o driver, é possível configurar suas instâncias com dois monitores 4K por GPU.

APIs compatíveis

- OpenGL, OpenCL
- Vulkan
- Framework de mídia avançada da AMD
- API de aceleração de vídeo
- DirectX 9 e posterior
- Transformação do Microsoft Hardware Media Foundation

AMIs com o driver AMD instalado

A AWS oferece diferentes imagens de máquina da Amazon (AMIs) com os drivers AMD instalados. AbraOfertas do Open Marketplace com o driver AMD.

Download do driver AMD

Se você não estiver usando uma AMI com o driver AMD instalado, é possível fazer download do driver AMD e instalá-lo em sua instância. Somente as seguintes versões de sistema operacional são compatíveis com drivers da AMD:

- Amazon Linux 2 com o kernel versão 4.14

> **Note**
>
> A versão do driver AMD amdgpu-pro-20.20-1184451 e versões mais recentes do driver exigem a versão 5.15 ou superior do kernel.

- Windows Server 2016
- Windows Server 2019

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer download, você concorda que usará o software submetido a download somente para desenvolver AMIs para uso com o hardware AMD Radeon Pro V520. Após a instalação do software, você estará vinculado aos termos do Contrato de licença de usuário final do software AMD.

Instalação do driver da AMD na instância do Linux

1. Conecte-se à sua instância do Linux.
2. Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

   > **Important**
   >
   > Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Instale gcc e make, caso ainda não tenham sido instalados.

   ```
   $ sudo yum install gcc make
   ```

4. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

   - Para Amazon Linux 2:

     ```
     $ sudo amazon-linux-extras install epel -y
     $ sudo yum update -y
     ```

   - Para Ubuntu 22.04:

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-
install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /
etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

- Para outras versões do Ubuntu:

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

- Para o CentOS:

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

5. Reinicialize a instância.

```
$ sudo reboot
```

6. Reconecte-se à instância depois que ela for reinicializada.
7. Faça download do driver AMD mais recente.

> **Note**
>
> Ignore esta etapa para o Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Extraia o arquivo.

- Para Amazon Linux 2 e CentOS:

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

- Para o Ubuntu:

> **Note**
>
> Ignore esta etapa para o Ubuntu 22.04.

```
$ tar -xf amdgpu-pro*ubuntu*.xz
```

9. Mude para a pasta do driver extraído.
10. Adicione os módulos ausentes para a instalação do driver.
    - Para Amazon Linux 2 e CentOS:

      Pule esta etapa.
    - Para o Ubuntu:

      > **Note**
      >
      > Ignore esta etapa para o Ubuntu 22.04.

      ```
      $ sudo apt install linux-modules-extra-$(uname -r) -y
      ```
11. Execute o script de instalação automática para instalar a pilha completa de gráficos.
    - Para Ubuntu 22.04:

      ```
      $ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
      ```
    - Para Amazon Linux 2 e CentOS e outras versões do Ubuntu:

      ```
      $ ./amdgpu-pro-install -y --opencl=pal,legacy
      ```
12. Reinicialize a instância.

    ```
    $ sudo reboot
    ```
13. Verifique se o driver está funcionando.

```
$ dmesg | grep amdgpu
```

A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

Instalação do driver da AMD na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

   > **Important**
   >
   > Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Faça download dos drivers de Amazon S3 para seu desktop usando os seguintes comandos do PowerShell.

   ```
   $Bucket = "ec2-amd-windows-drivers"
   $KeyPrefix = "latest" # use "archives" for Windows Server 2016
   $LocalPath = "$home\Desktop\AMD"
   $Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
   foreach ($Object in $Objects) {
   $LocalFileName = $Object.Key
   if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
       $LocalFilePath = Join-Path $LocalPath $LocalFileName
       Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
   Region us-east-1
   }
   }
   ```

4. Descompacte o arquivo de driver obtido por download e execute o instalador usando os comandos do PowerShell a seguir.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Agora, verifique o conteúdo do novo diretório. O nome do diretório pode ser recuperado usando o comando `Get-ChildItem` do PowerShell.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

A saída deve ser semelhante à seguinte:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Instalar os drivers:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

5. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.
6. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos. É necessário ver “AMD Radeon Pro V520 MxGPU” listado como um adaptador de exibição.
7. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, NICE DCV.

Configuração de uma área de trabalho interativa para o Linux

Após confirmar que a instância do Linux tem o driver de GPU da AMD instalado e que o driver AMDgpu está em uso, você poderá instalar um gerenciador de área de trabalho interativa. Recomendamos o ambiente de desktop MATE para obter a melhor compatibilidade e performance.

Pré-requisito

Abra um editor de texto e salve o seguinte como um arquivo chamado `xorg.conf`. Você precisará desse arquivo em sua instância.

```
Section "ServerLayout"
```

```
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
```

```
Device          "Device0"
Monitor         "Monitor0"
DefaultDepth    24
Option          "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual     3840 2160
    Depth       32
EndSubSection
EndSection
```

Para configurar um desktop interativo no Amazon Linux 2

1. Instale o repositório EPEL.

```
$ C:\> sudo amazon-linux-extras install epel -y
```

2. Instale o desktop MATE.

```
$ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.
4. Reinicialize a instância.

```
$ C:\> sudo reboot
```

5. (Opcional) Instale o servidor NICE DCV para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, conecte-se a uma sessão NICE DCV usando seu cliente preferido.

Para configurar um desktop interativo no Ubuntu

1. Instale o desktop MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ C:\> sudo apt purge ifupdown -y
```

2. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.
3. Reinicialize a instância.

```
$ sudo reboot
```

4. Instale o codificador AMF para a versão apropriada do Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Opcional) Instale o servidor NICE DCV para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, conecte-se a uma sessão NICE DCV usando seu cliente preferido.
6. Após a instalação do DCV, dê permissões de vídeo ao usuário DCV:

```
$ sudo usermod -aG video dcv
```

Para configurar um desktop interativo no CentOS

1. Instale o repositório EPEL.

```
$ sudo yum update -y
$ C:\> sudo yum install epel-release -y
```

2. Instale o desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.
4. Reinicialize a instância.

```
$ sudo reboot
```

5. (Opcional) Instale o servidor NICE DCV para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, conecte-se a uma sessão NICE DCV usando seu cliente preferido.

Drivers paravirtuais para as instâncias do Windows

As AMIs do Windows contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. A tabela a seguir mostra as principais diferenças entre os diferentes drivers.

	RedHat PV	Citrix PV	AWS PV
Tipo de instância	Não tem suporte para todos os tipos de instâncias. Se você especificar um tipo de instância sem suporte, a instância ficará danificada.	Com suporte para os tipos de instância Xen.	Com suporte para os tipos de instância Xen.
Volumes anexados	Oferece suporte a até 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.
Rede	O driver tem problemas conhecidos em que a conexão de rede é redefinida em cargas altas, por exemplo, transferências rápidas de arquivos via FTP.		O driver configura automaticamente quadros jumbo no adaptador da rede quando está em um tipo de instância compatível. Quando a instância está em um grupo de

	RedHat PV	Citrix PV	AWS PV
			posiciona mento de cluster, isso oferece melhor desempenh o de rede entre as instâncias que estão no grupo de posiciona mento de cluster. Para ter mais informaçõ es, consulte Grupos de posiciona mento.

A tabela a seguir mostra quais drivers PV é necessário executar em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão PV driver
Windows Server 2022	Versão mais recente do AWS PV
Windows Server 2019	Versão mais recente do AWS PV
Windows Server 2016	Versão mais recente do AWS PV
Windows Server 2012 R2	Versão mais recente do AWS PV
Windows Server 2012	Versão mais recente do AWS PV

Versão Windows Server	Versão PV driver
Windows Server 2008 R2	AWS PV versão 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Tópicos

- Drivers AWS PV
- Drivers do Citrix PV
- Drivers RedHat PV
- Assinar notificações do
- Atualizar drivers de PV em instâncias do Windows
- Solução de problemas em drivers PV em instâncias do Windows

Drivers AWS PV

Os drivers AWS PV são armazenadas no diretório `%ProgramFiles%\Amazon\Xentools`. Esse diretório também contém símbolos públicos e uma ferramenta da linha de comando, `xenstore_client.exe`, que permite acessar entradas no XenStore. Por exemplo, o seguinte comando de PowerShell retorna o horário atual do Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Os componentes do driver AWS PV são listados no Registro do Windows em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Esses componentes do driver são os seguintes: xenbus, xeniface, xennet, xenvbd e xenvif.

Os drivers AWS PV também têm um serviço do Windows chamado LiteAgent, que é executado no modo de usuário. Ele lida com tarefas como eventos de desligamento e reinicialização a partir das APIs da AWS em instâncias de geração Xen. É possível acessar e gerenciar serviços executando `Services.msc` a partir da linha de comando. Quando executados em instâncias de geração Nitro, os drivers AWS PV não são usados e o serviço LiteAgent será interrompido automaticamente

começando pela versão do driver 8.2.4. A atualização para o driver AWS PV mais recente também atualiza o LiteAgent e melhora a confiabilidade em todas as gerações de instâncias.

Instalar os drivers AWS PV mais recentes

As AMIs Windows da Amazon contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. Recomendamos que você instale os drivers mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows.

Opções de instalação

- É possível usar o AWS Systems Manager automaticamente para atualizar os drivers PV. Para obter mais informações, consulte Demonstração: atualizar drivers de PV automaticamente em instâncias do EC2 para Windows Server (console) no Guia do usuário do AWS Systems Manager.
- É possível fazer download do pacote de configuração do driver e executar o programa de instalação manualmente. Verifique o arquivo `readme.txt` quanto aos requisitos do sistema. Para obter informações sobre como fazer download e instalar os drivers AWS PV ou se você estiver atualizando um controlador de domínio, consulte Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV).

Histórico do pacote de drivers AWS PV

A tabela a seguir mostra as alterações nos drivers AWS PV para cada versão de driver.

Versão do pacote	Detalhes	Data de lançamento
8.4.3	Erros corrigidos no instalador de pacotes para melhorar a experiência de atualização.	24 de janeiro de 2023
8.4.2	Correções de estabilidade para lidar com a condição da corrida.	13 de abril de 2022
8.4.1	Instalador de pacotes aprimorado.	7 de janeiro de 2022
8.4.0	• Correções de estabilidade para resolver casos raros de E/S de disco preso.	2 de março de 2021

Versão do pacote	Detalhes	Data de lançamento
	• Correções de estabilidade para resolver casos raros de falhas durante a desanexação do volume EBS. • Recurso adicionado para distribuir carga em vários núcleos para workloads que usam mais de 20.000 IOPS e experimen tam degradação devido a gargalos. Para ativar esse recurso, consulte Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU. • A instalação do AWS PV 8.4 no Windows Server 2008 R2 falhará. AWS O PV versão 8.3.5 e versões anteriores são compatíveis com o Windows Server 2008 R2.	
8.3.5	Instalador de pacotes aprimorado.	7 de janeiro de 2022
8.3.4	Maior confiabilidade do anexo do dispositivo de rede.	4 de agosto de 2020
8.3.3	• Atualize para o componente voltado para o XenStore a fim de evitar a verificação de bugs durante os caminhos de manipulação de erros. • Atualize para o componente de armazenamento para evitar falhas quando um SRB inválido for enviado. Para atualizar esse driver em instâncias do Windows Server 2008 R2, é necessário primeiro verificar se os patches apropriad os estão instalados para abordar o seguinte Aviso de segurança da Microsoft: Aviso de segurança da Microsoft 3033929.	4 de fevereiro de 2020
8.3.2	Confiabilidade aprimorada de componentes da rede.	30 de julho de 2019
8.3.1	Melhora na performance e na robustez do componente de armazenamento.	12 de junho de 2019

Versão do pacote	Detalhes	Data de lançamento
8.2.7	Maior eficiência para oferecer suporte à migração para os tipos de instância de última geração.	20 de maio de 2019
8.2.6	Eficiência aumentada do caminho de despejo de memória.	15 de janeiro de 2019
8.2.5	Melhorias de segurança adicionais. O instalador do PowerShell agora está disponível no pacote.	12 de dezembro de 2018
8.2.4	Melhorias na confiabilidade.	2 de outubro de 2018
8.2.3	Correções de erros e melhorias na performance. Relate o ID de volume do EBS como o número de série do disco para volumes do EBS. Isso permite cenários de cluster, como o S2D.	29 de maio de 2018
8.2.1	Melhorias de performance de rede e de armazenamento e várias correções de solidez. Para verificar se esta versão foi instalada, consulte o valor do seguinte registro do Windows: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 de março de 2018
7.4.6	Correções de estabilidade para tornar os drivers AWS PV mais resilientes.	26 de abril de 2017
7.4.3	Adicionado suporte para o Windows Server 2016. Correções de estabilidade para todas as versões dos sistemas operacionais Windows com suporte. *A assinatura da versão 7.4.3 do driver AWS PV expira em 29 de março de 2019. Recomendamos que você atualize para o driver AWS PV mais recente.	18 de nov de 2016

Versão do pacote	Detalhes	Data de lançamento
7.4.2	Correções de estabilidade para suporte do tipo de instância X1.	2 de agosto de 2016
7.4.1	• Melhoria da performance no driver AWS PV Storage. • Correções de estabilidade no driver AWS PV Storage: corrigido um problema em que as instâncias sofriam uma paralisação do sistema com o código de verificação de bugs 0x0000DEAD. • Correções de estabilidade no driver AWS PV Network. • Adicionado suporte para o Windows Server 2008R2.	12 de julho de 2016
7.3.2	• Aperfeiçoados o registro em log e o diagnóstico. • Correção de estabilidade no driver AWS PV Storage. Em alguns casos, os discos podem não ser expostos no Windows depois de anexar novamente o disco à instância. • Adicionado suporte para o Windows Server 2012.	24 de junho de 2015
7.3.1	Atualização TRIM: correção relativa às solicitações TRIM. Essa correção estabiliza as instâncias e melhora a performance da instância ao gerenciar um grande número de solicitações TRIM.	
7.3.0	Suporte TRIM: o driver AWS PV agora envia solicitações TRIM para o hipervisor. Os discos efêmeros processarão adequadamente as solicitações TRIM desde que o armazenamento subjacente ofereça suporte a TRIM (SSD). Observe que o armazenamento baseado em EBS não oferece suporte a TRIM desde março de 2015.	

Versão do pacote	Detalhes	Data de lançamento
7.2.5	• Correção de estabilidade em drivers AWS PV Storage: em alguns casos, o driver AWS PV pode cancelar a referência de memória inválida e causar uma falha de sistema. • Correção de estabilidade ao gerar um despejo de memória: em alguns casos o driver AWS PV trava em um condição de disputa ao gravar um despejo de memória. Antes dessa versão, só era possível resolver o problema forçando o driver a interromper e reiniciar, o que fazia com que o despejo de memória fosse perdido.	
7.2.4	Manutenção do ID de dispositivo: essa correção de driver mascara o ID do dispositivo PCI da plataforma e força o sistema a sempre expor o mesmo ID de dispositivo, mesmo que a instância seja movida. De uma forma mais geral, a correção afeta como o hipervisor expõe dispositivos virtuais. A correção também inclui modificações ao coinstalador dos drivers AWS PV de forma que o sistema mantenha dispositivos virtuais mapeados.	
7.2.2	• Carga dos drivers AWS PV no modo Directory Services Restore Mode (DSRM): o modo Directory Services Restore é uma opção de inicialização do modo de segurança para controladores de domínio do Windows Server. • Manutenção do ID do dispositivo quando o dispositivo de adaptador de rede virtual é anexado novamente: essa correção força o sistema a verificar o mapeamento de endereço MAC e a manter o ID do dispositivo. Essa correção garante que os adaptadores retenham suas configurações estáticas se os adaptadores forem anexados novamente.	

Versão do pacote	Detalhes	Data de lançamento
7.2.1	• Execução no modo de segurança: corrigido o problema em que o driver não era carregado no modo de segurança . Anteriormente, os drivers AWS PV só instanciavam em sistemas de execução normal. • Adição de discos aos grupos de armazenamento do Microsoft Windows: anteriormente, sintetizávamos as consultas da página 83. A correção desabilitou o suporte da página 83. Isso não afeta os grupos de armazenamento que são usados em um ambiente de cluster porque os discos PV não são discos de cluster válidos.	
7.2.0	Base: A versão base do AWS PV.	

Drivers do Citrix PV

Os drivers Citrix PV são armazenados no diretório `%ProgramFiles%\Citrix\XenTools` (instâncias de 32 bits) ou `%ProgramFiles(x86)%\Citrix\XenTools` (instâncias de 64 bits).

Os componentes do driver Citrix PV são listados no Registro do Windows em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Esses componentes de driver são os seguintes: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd e xenvif.

O Citrix também tem um componente de driver chamado XenGuestAgent, que é executado como um serviço do Windows. Ele lida com tarefas como eventos de desligamento e reinicialização a partir da API. É possível acessar e gerenciar serviços executando `Services.msc` a partir da linha de comando.

Se você estiver encontrando erros de redes ao executar determinadas workloads, precisará desabilitar o recurso de descarregamento de TCP para o driver Citrix PV. Para ter mais informações, consulte Descarregamento de TCP.

Drivers RedHat PV

Os drivers RedHat têm suporte para instâncias herdadas, mas não são recomendados em instâncias mais novas com mais de 12 GB de RAM devido às limitações do driver. As instâncias com mais

de 12 GB de RAM que executam drivers RedHat podem não ser iniciadas e se tornar inacessíveis. Recomendamos atualizar os drivers RedHat para drivers Citrix PV e, em seguida, atualizar os drivers Citrix PV para drivers AWS PV.

Os arquivos de origem para os drivers RedHat estão no diretório `%ProgramFiles%\RedHat` (instâncias de 32 bits) ou `%ProgramFiles(x86)%\RedHat` (instâncias de 64 bits). Os dois drivers são `rhelnet`, o driver de rede paravirtualizado RedHat e `rhelscsi`, o driver miniporta SCSI RedHat.

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para assinar essas notificações.

> **Note**
>
> Você deve especificar a região para o tópico do SNS que você assinar.

Assinar as notificações do EC2 no console

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
   a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Para Protocolo, selecione `Email`.
   c. Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações.
   d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Assinar as notificações do EC2 usando o AWS CLI

Para assinar as notificações do EC2 com a AWS CLI, use o comando a seguir.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-
windows-drivers --region us-east-1 --protocol email --notification-
endpoint YourUserName@YourDomainName.ext
```

Assinar as notificações do EC2 usando o AWS Tools for PowerShell

Para assinar as notificações do EC2 com Tools for Windows PowerShell, use o comando a seguir.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver do Windows para o Amazon EC2

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Subscriptions.
3. Marque a caixa de seleção da assinatura e, depois, selecione Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Atualizar drivers de PV em instâncias do Windows

Recomendamos que você instale os drivers de PV mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows. As instruções desta página ajudam você a fazer download do pacote do driver e executar o programa de instalação.

Para verificar qual driver sua instância do Windows usa

Abra Network Connections (Conexões de rede) no Painel de controle e consulte Conexão de área local. Verifique se o driver é um dos seguintes:

- AWS PV Network Device
- Citrix PV Ethernet Adapter

- Driver RedHat PV NIC

Como alternativa, é possível verificar a saída do comando `pnputil -e`.

Requisitos do sistema

Verifique o arquivo `readme.txt` no download quanto aos requisitos do sistema.

Conteúdo

- Atualizar instâncias do Windows Server (atualização do AWS PV) com o Distributor
- Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV)
- Atualizar um controlador de domínio (atualização do AWS PV)
- Atualizar instâncias do Windows Server 2008 e 2008 R2 (atualização do Redhat para Citrix PV)
- Atualizar o serviço de agente convidado do Citrix Xen

Atualizar instâncias do Windows Server (atualização do AWS PV) com o Distributor

É possível usar o Distributor, um recurso do AWS Systems Manager, para instalar ou atualizar o pacote de drivers do AWS PV. Você pode executar a instalação ou atualização uma vez, ou pode executar essas operações de acordo com um cronograma. A opção `In-place update` para Tipo de instalação não é compatível com esse pacote do Distributor.

> **Important**
>
> Se sua instância for um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV). O processo de atualização dessas instâncias do controlador de domínio é diferente das edições padrão do Windows.

1. Recomendamos que você crie um backup, caso precise reverter suas alterações.

   > **Tip**
   >
   > Em vez de criar a AMI no console do Amazon EC2, você poderá usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

b. No painel de navegação, escolha Instances (Instâncias).

c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).

d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).

e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

2. Conectar-se à instância usando o Desktop Remoto. Para ter mais informações, consulte the section called “Conexão com a instância do Windows usando um cliente RDP”.

3. Recomendamos que você deixe offline todos os discos que não sejam do sistema e anote quaisquer mapeamentos de letras de unidade para os discos secundários no Gerenciamento de Disco antes de executar esta atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Também recomendamos definir serviços não essenciais como inicialização Manual no console de Services.

4. Para obter instruções sobre como instalar ou atualizar o pacote de drivers do AWS PV usando o Distributor, consulte os procedimentos em Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager.

5. Em Nome, escolha AWSPVDriver.

6. Em Tipo de instalação, escolha Desinstalar e reinstalar.

7. Configure os outros parâmetros do pacote conforme necessário e execute a instalação ou a atualização seguindo o procedimento indicado em Step 4.

   Após executar o pacote do Distributor, a instância será reinicializada automaticamente e, em seguida, atualizará o driver. A instância não estará disponível por até 15 minutos.

8. Depois que atualização terminar e a instância for aprovada nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se o novo driver foi instalado.

9. Após se conectar, execute o seguinte comando do PowerShell:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

10. Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV Abrir o gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los on-line de acordo com as letras de unidade indicadas em Step 3.

Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Se você aplicou anteriormente um endereço IP estático ou a configuração de DNS à interface de rede, pode ser necessário reaplicar o endereço IP estático ou a configuração de DNS depois de atualizar os drivers AWS PV.

Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV)

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022. Essa atualização não está disponível para drivers RedHat nem outras versões do Windows Server.

Algumas versões mais antigas do Windows Server não podem usar os drivers mais recentes. Para verificar qual versão de driver usar para seu sistema operacional, consulte a tabela de versões dos drivers em Drivers paravirtuais para as instâncias do Windows.

> **Important**
>
> Se sua instância for um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV). O processo de atualização dessas instâncias do controlador de domínio é diferente das edições padrão do Windows.

Para atualizar manualmente os drivers do AWS PV

1. Recomendamos que você crie um backup, caso precise reverter suas alterações.

> **Tip**
>
> Em vez de criar a AMI no console do Amazon EC2, você poderá usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

b. No painel de navegação, escolha Instances (Instâncias).

c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).

d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).

e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

2. Conectar-se à instância usando o Desktop Remoto.

3. Recomendamos que você deixe offline todos os discos que não sejam do sistema e anote quaisquer mapeamentos de letras de unidade para os discos secundários no Gerenciamento de Disco antes de executar esta atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Também recomendamos definir serviços não essenciais como inicialização Manual no console de Services.

4. Faça download do pacote de drivers mais recente na instância.

   Ou execute o seguinte comando do PowerShell:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
 $env:userprofile\pv_drivers
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

5. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, será possível verificar se o novo driver foi instalado conectando-se à instância usando o Remote Desktop e executando o seguinte comando do PowerShell:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV Abrir o gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los on-line de acordo com as letras de unidade indicadas em Step 3.

Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Se você aplicou anteriormente um endereço IP estático ou a configuração de DNS à interface de rede, pode ser necessário reaplicar o endereço IP estático ou a configuração de DNS depois de atualizar os drivers AWS PV.

Atualizar um controlador de domínio (atualização do AWS PV)

Use o procedimento a seguir em um controlador de domínio para executar uma atualização no local dos drivers AWS PV ou atualizar drivers Citrix PV para drivers AWS PV.

Para atualizar um controlador de domínio

1. Recomendamos que você crie um backup do seu controlador de domínio no caso de precisar reverter suas alterações. O uso de uma AMI como backup não é aceito. Para obter mais informações, consulte Considerações de backup e restauração para controladores de domínio virtualizados na documentação da Microsoft.
2. Execute o comando a seguir para configurar o Windows para ser iniciado no Modo de Restauração dos Serviços de Diretório (DSRM):

   > **Warning**
   >
   > Antes de executar esse comando, confirme a senha do DSRM. Você precisará dessas informações para fazer login na sua instância depois que a atualização estiver concluída e a instância tiver sido reiniciada automaticamente.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

   O sistema deve ser inicializado no DSRM porque o utilitário de atualização remove os drivers de armazenamento Citrix PV para que possa instalar os drivers AWS PV. Por isso, recomendamos que anote quaisquer mapeamentos de letras e pastas de unidade para os discos secundários no Gerenciamento de Disco. Quando os drivers de armazenamento Citrix PV não estiverem presentes, as unidades secundárias não serão detectadas. Os controladores de domínio que usam uma pasta NTDS em unidades secundárias não serão inicializados porque o disco secundário não será detectado.

> **Warning**
>
> Depois de executar esse comando não reinicialize o sistema manualmente. O sistema ficará inacessível porque os drivers Citrix PV não oferecem suporte a DSRM.

3. Execute o comando a seguir para adicionar **`DisableDCCheck`** ao registro:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Faça download do pacote de drivers mais recente na instância.
5. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

   Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos.
6. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop. Abra o Gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los online correspondendo ao mapeamento de letras e pastas de unidade observado anteriormente.

   É necessário se conectar à instância especificando o nome do usuário no seguinte formato hostname\administrador. Por exemplo, Win2k12TestBox\administrador.
7. Execute o comando a seguir para remover a configuração de inicialização do DSRM:

```
bcdedit /deletevalue safeboot
```

8. Reinicialize a instância.
9. Para concluir o processo de atualização, verifique se o novo driver foi instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para ter mais informações, consulte Histórico do pacote de drivers AWS PV.
10. Execute o comando a seguir para excluir **`DisableDCCheck`** do registro:

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

> **Note**
>
> Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Atualizar instâncias do Windows Server 2008 e 2008 R2 (atualização do Redhat para Citrix PV)

Antes você começar a atualizar seus drivers RedHat para drivers Citrix PV, faça o seguinte:

- Instale a versão mais recente do serviço EC2Config. Para ter mais informações, consulte Instalar a versão mais recente do EC2Config.
- Verifique se você tem o Windows PowerShell 3.0 instalado. Para verificar a versão que você instalou, execute o seguinte comando em uma janela do PowerShell:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  O Windows PowerShell 3.0 está incluído no pacote de instalação do Windows Management Framework (WMF) versão 3.0. Se você precisar instalar o Windows PowerShell 3.0, consulte Windows Management Framework 3.0 no Centro de Download da Microsoft.
- Faça backup de suas informações importantes sobre a instância ou crie uma AMI da instância. Para obter mais informações sobre a criação de uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

  > **Tip**
  >
  > Em vez de criar a AMI no console do Amazon EC2, você poderá usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

  Se você criar uma AMI, certifique-se de fazer o seguinte:

  - Escreva sua senha.

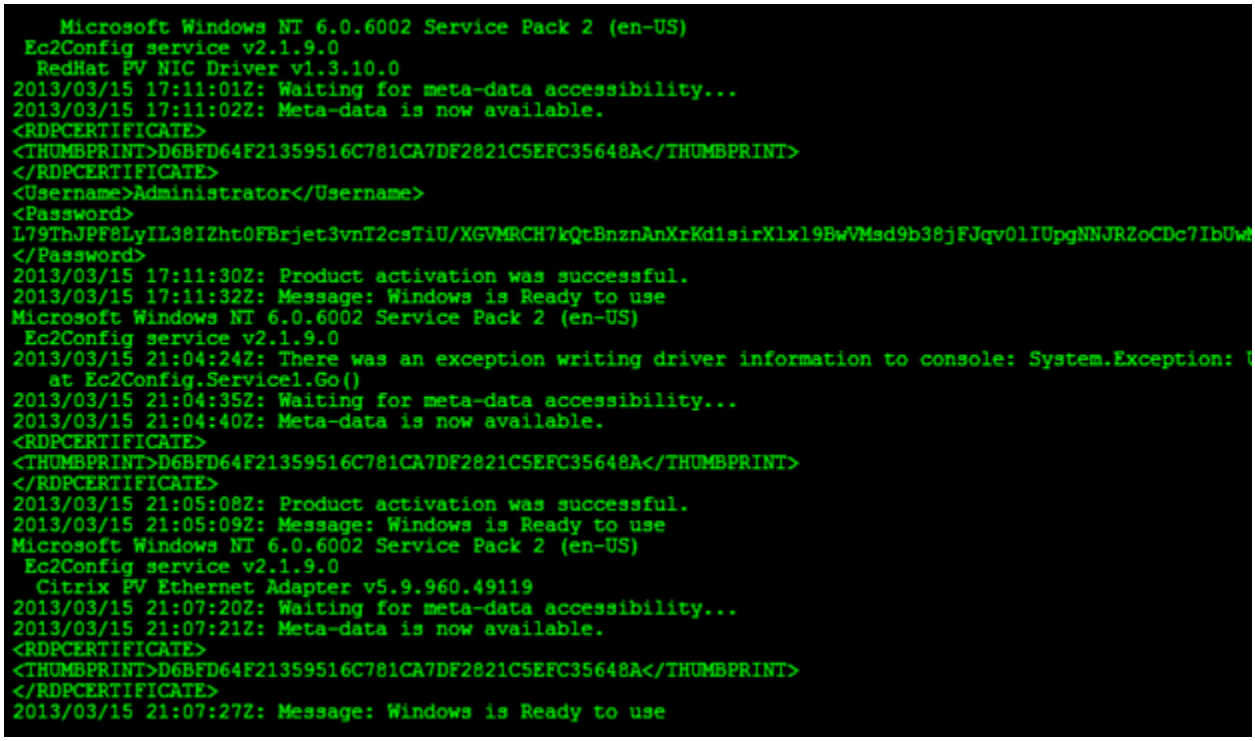
- Não execute a ferramenta Sysprep manualmente nem usando o serviço EC2Config.
- Defina o adaptador de Ethernet para obter um endereço IP usando automaticamente o DHCP. Para obter mais informações, consulte Definir as configurações de TCP/IP na Biblioteca do Microsoft TechNet.

Para atualizar drivers RedHat

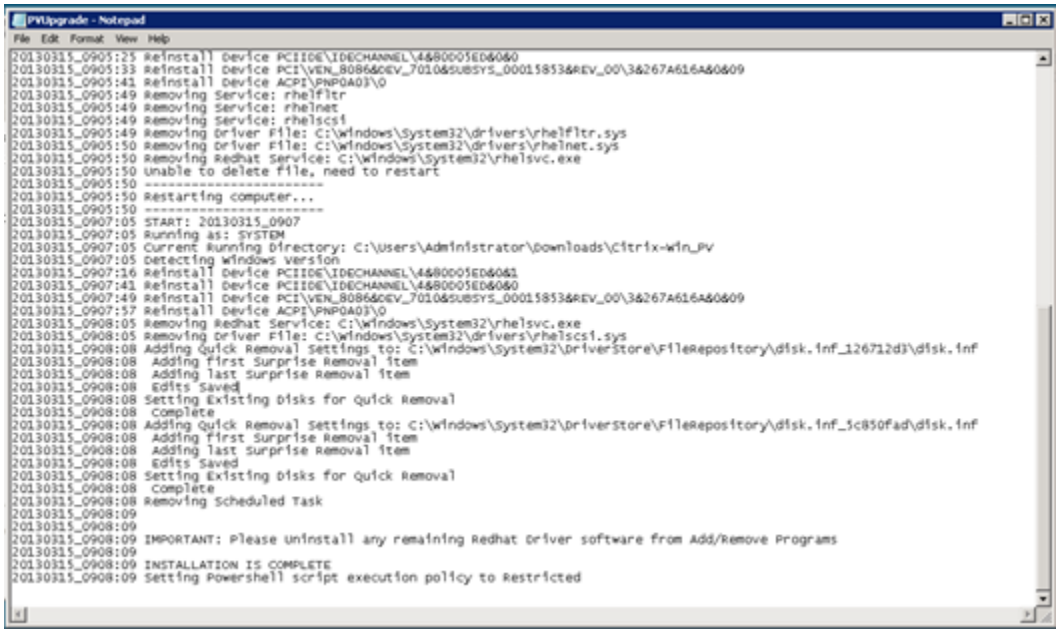
1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à sua instância do Windows do .
2. Em sua instância, faça download do pacote de atualização do Citrix PV.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.
4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Na caixa de diálogo Desinstalador dos drivers paravirtualizados Red Hat para Windows, selecione Sim para remover o software RedHat. Sua instância será recarregada.

> **Note**
>
> Se você não vir a caixa de diálogo do desinstalador, selecione Red Hat paravirtualizado na barra de tarefas do Windows.

7. Verifique se a instância foi reinicializada e está pronta para uso.
   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. Na página Instances (Instâncias), selecione Actions (Ações),Monitor and troubleshoot (Monitorar e solucionar problemas) e, em seguida, escolha Get system log (Obter log do sistema).
   c. As operações de atualização devem ter reiniciado o servidor 3 ou 4 vezes. É possível ver isso no arquivo de log pelo número de vezes em que `Windows is Ready to use` é exibido.



8. Conecte-se à instância e faça login como administrador local.
9. Feche a caixa de diálogo Desinstalador dos drivers Xen paravirtualizados Red Hat para Windows.
10. Verifique se a instalação foi concluída. Navegue até a pasta `Citrix-WIN_PV` que você extraiu anteriormente, abra o arquivo `PVUpgrade.log` e verifique o texto `INSTALLATION IS COMPLETE`.



Atualizar o serviço de agente convidado do Citrix Xen

Se você estiver usando drivers Citrix PV no Windows Server, será possível atualizar o serviço de agente de convidado do Citrix Xen. Esse serviço do Windows gerencia tarefas como eventos de desligamento e reinicialização a partir da API. É possível executar esse pacote de atualização em qualquer versão do Windows Server, desde que a instância esteja executando drivers Citrix PV.

> **Important**
>
> Para Windows Server 2008 R2 e posterior, recomendamos atualizar para drivers AWS PV que incluem a atualização do agente convidado.

Antes de começar a atualizar seus drivers, faça backup de suas informações importantes sobre a instância ou crie uma AMI a partir da instância. Para obter mais informações sobre a criação de uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

> **Tip**
>
> Em vez de criar a AMI no console do Amazon EC2, você poderá usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

Se você criar uma AMI, certifique-se de fazer o seguinte:

- Não habilite a ferramenta Sysprep no serviço EC2Config.
- Escreva sua senha.
- Defina o adaptador de Ethernet como DHCP.

Para atualizar seu serviço de agente convidado do Citrix Xen

1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à sua instância do Windows do .
2. Em sua instância, faça download do pacote de atualização do Citrix.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.

4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Quando a atualização estiver concluída, o arquivo `PVUpgrade.log` será aberto e conterá o texto `UPGRADE IS COMPLETE`.
7. Reinicie a instância.

Solução de problemas em drivers PV em instâncias do Windows

Veja a seguir soluções para problemas que podem ser encontrados com imagens do Amazon EC2 e drivers de PV mais antigos.

Tópicos

- O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância
- Descarregamento de TCP
- Sincronização de horário
- Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU

O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância

> **Important**
>
> Esse problema ocorre somente com AMIs disponibilizadas antes de setembro de 2014.

As Imagens de máquina da Amazon (AMIs) do Windows Server 2012 R2 disponibilizadas antes de 10 de setembro de 2014 podem perder conectividade de rede e armazenamento após a reinicialização da instância. O erro no log do sistema do AWS Management Console indica: "Dificuldade em detectar detalhes do driver PV para a saída do console". A perda de conectividade é causada pelo recurso Limpeza de plug and play. Esse recurso verifica e desabilita dispositivos inativos do sistema a cada 30 dias. O recurso identifica incorretamente o dispositivo de rede EC2

como inativo e o remove do sistema. Quando isso ocorre, a instância perde a conectividade de rede após uma reinicialização.

Para sistemas que você suspeita estar sendo afetados por esse problema, é possível fazer download e executar uma atualização de driver no local. Caso não seja possível executar a atualização de driver no local, é possível executar um script auxiliar. O script determina se sua instância foi afetada. Se ela tiver sido afetada, e o dispositivo de rede do Amazon EC2 não tiver sido removido, o script desabilitará a verificação da Limpeza de plug and play. Se o dispositivo de rede tiver sido removido, o script reparará o dispositivo, desabilitará a verificação do recurso Limpeza de plug and play e permitirá que sua instância seja reinicializada com a conectividade de rede habilitada.

Tópicos

- Escolher como corrigir problemas
- Método 1 – Redes aprimoradas
- Método 2 – Configuração do Registro
- Executar o script de correção

Escolher como corrigir problemas

Há dois métodos para restaurar a conectividade de rede e de armazenamento em uma instância afetada por esse problema. Escolha um dos seguintes métodos:

Método	Pré-requisitos	Visão geral do procedimento
Método 1 – Redes aprimoradas	As redes aprimoradas só estão disponíveis em uma nuvem privada virtual (VPC) que exija um tipo de instância C3. Se o servidor não usar atualmente o tipo de instância C3, altere-o temporariamente.	Você altera o tipo de instância do servidor em uma instância C3. Em seguida, as redes aprimoradas permitem a você se conectar à instância afetada e corrigir o problema. Depois de corrigir o problema, você altera a instância de volta para o tipo original. Esse método é geralmente mais rápido do que o método 2 e tem menos probabilidade de resultar em erro do usuário.

Método	Pré-requisitos	Visão geral do procedimento
		Haverá cobranças adicionais pelo período de execução da instância C3.
Método 2 – Configuração do Registro	Capacidade de criar ou acessar um segundo servidor. Capacidade de alterar as configurações do Registro.	Você desanexa o volume raiz da instância afetada, anexa-o a outra instância, conecta-se e faz alterações no Registro. Haverá cobranças adicionais pelo período de execução do servidor adicional. Esse método é mais lento do que o método 1, mas ele funcionou em situações nas quais o método 1 não resolveu o problema.

Método 1 – Redes aprimoradas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância e escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
5. Altere o tipo de instância para qualquer tipo de instância C3.
6. Inicie a instância.

7. Conecte-se à instância usando o Desktop Remoto e faça download do pacote de atualização de drivers AWS PV na instância.
8. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

   Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.
9. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para ter mais informações, consulte Histórico do pacote de drivers AWS PV.
10. Interrompa a instância e altere-a de volta para seu tipo original.
11. Inicie a instância e retome o uso normal.

Método 2 – Configuração do Registro

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância, escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

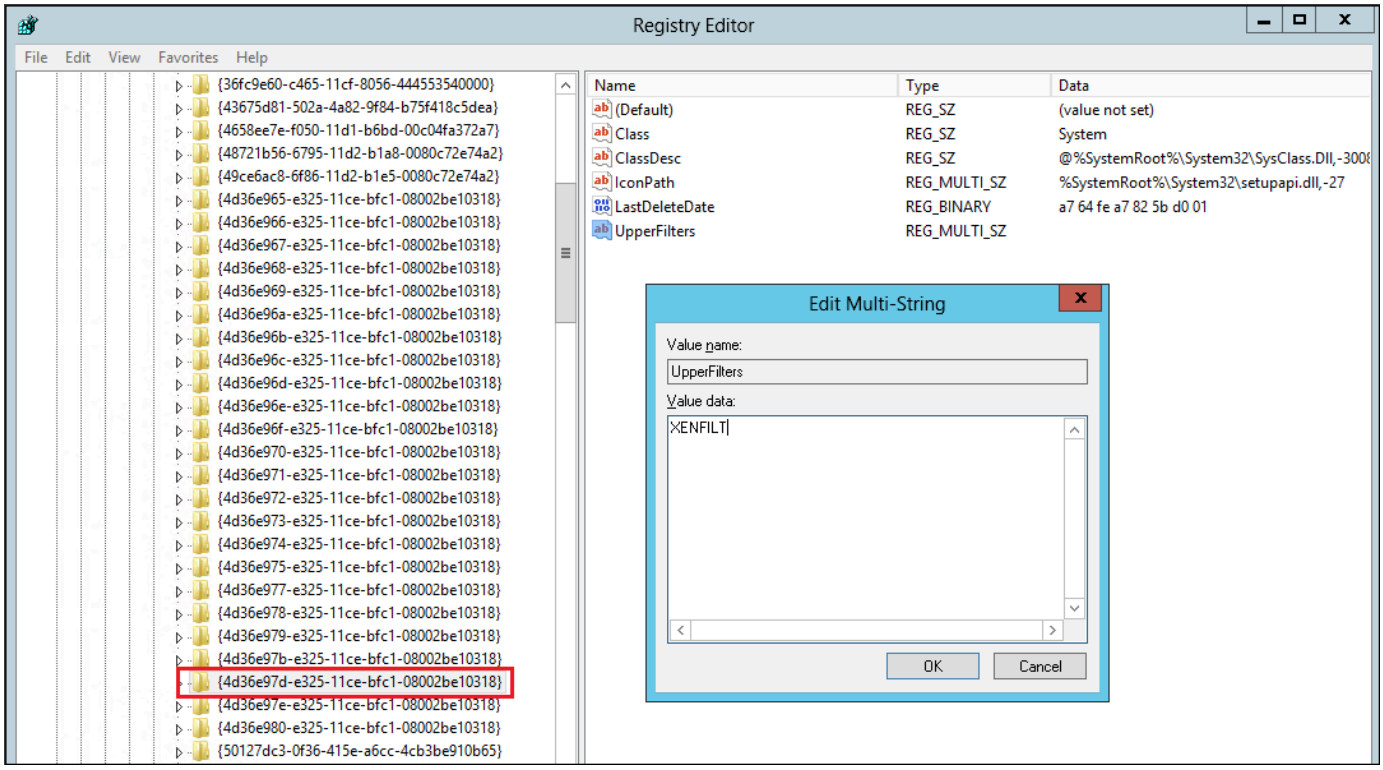
   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.
4. Escolha Launch instance (Executar instâncias) e crie uma instância temporária Windows Server 2008 ou Windows Server 2012 na mesma zona de disponibilidade que a instância afetada. Não crie uma instância do Windows Server 2012 R2.

> **Important**
>
> Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No painel de navegação, escolha Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Desanexe o volume e anexe o volume à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para se conectar à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.
8. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **`regedit`** e pressione Enter.
9. No painel de navegação do Editor de Registro, escolha HKEY_Local_Machine e no menu Arquivo escolha Carregar Hive.
10. Na caixa de diálogo Carregar Hive, navegue até Volume afetado\Windows\System32\config \System e digite um nome temporário na caixa de diálogo Nome da chave. Por exemplo, digite OldSys.
11. No painel de navegação do Editor de Registro, localize as seguintes chaves:

    HKEY_LOCAL_MACHINE***`your_temporary_key_name`**\ControlSet001\Control\Class \4d36e97d-e325-11ce-bfc1-08002be10318

    HKEY_LOCAL_MACHINE***`your_temporary_key_name`**\ControlSet001\Control\Class \4d36e96a-e325-11ce-bfc1-08002be10318
12. Para cada chave, clique duas vezes em UpperFilters, digite um valor de XENFILT e, em seguida, selecione OK.



13. Localize a seguinte chave:

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ControlSet001\Services\XENBUS\Parameters

14. Crie uma nova string (REG_SZ) com o nome ActiveDevice e o seguinte valor:

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Localize a seguinte chave:

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ControlSet001\Services\XENBUS

16. Altere a contagem de 0 para 1.

17. Localize e exclua as seguintes chaves:

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ControlSet001\Services\xenvbd\StartOverride

    HKEY_LOCAL_MACHINE ***your_temporary_key_name***\ControlSet001\Services\xenfilt\StartOverride

18. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.

19. No menu Arquivo, escolha Descarregar Hive.
20. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
21. No console do Amazon EC2, desanexe o volume afetado de instância temporária e reanexe-o à sua instância do Windows Server 2012 R2 com o nome de dispositivo /dev/sda1. Especifique o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
22. Inicie a instância.
23. Conecte-se à instância usando o Desktop Remoto e faça download do pacote de atualização de drivers AWS PV na instância.
24. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

    Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.
25. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para ter mais informações, consulte Histórico do pacote de drivers AWS PV.
26. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Executar o script de correção

Caso não seja possível executar uma atualização de driver no local nem migrar para uma instância mais nova, é possível executar o script de correção para corrigir os problemas causados pela tarefa da Limpeza de plug and play.

Para executar o script de correção

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Escolha a instância para a qual você deseja executar o script de correção. Escolha Instance State (Estado da instância) e, em seguida, escolha Stop Instance (Interromper instância).

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e, em seguida, escolha Create image (Criar imagem).
5. Escolha Instance state (Estado da instância) e, em seguida, escolha Start Instance (Iniciar instância).
6. Conecte-se à instância usando o Desktop Remoto e, em seguida, faça download da pasta RemediateDriverIssue.zip na instância.
7. Extraia o conteúdo da pasta.
8. Execute o script de correção de acordo com as instruções no arquivo Readme.txt. O arquivo está localizado na pasta onde você extraiu o RemediateDriverIssue.zip.

Descarregamento de TCP

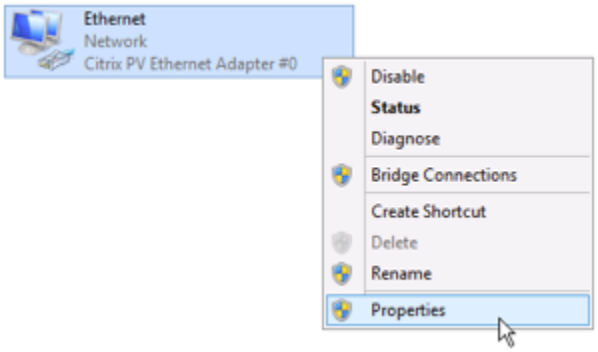
> **Important**
>
> Esse problema não se aplica a instâncias que executam drivers de rede AWS PV ou Intel.

Por padrão, o descarregamento TCP é habilitado para os drivers Citrix PV em AMIs do Windows. Se você encontrar erros no nível do transporte ou na transmissão de pacotes (conforme esteja visível no monitor de performance do Windows)—por exemplo, quando você estiver executando determinadas workloads do SQL—talvez seja necessário desabilitar esse recurso.

> **Warning**
>
> Desabilitar o descarregamento TCP pode reduzir a performance de rede de sua instância.

Para desabilitar o descarregamento TCP para Windows Server 2012 e 2008

1. Conecte-se à instância e faça login como administrador local.
2. Se você estiver usando o Windows Server 2012, pressione Ctrl+Esc para acessar a tela Iniciar e, em seguida, selecione Painel de controle. Se você estiver usando o Windows Server 2008, escolha Iniciar e selecione Painel de controle.
3. Escolha Rede e Internet e, em seguida, Central de Rede e Compartilhamento.
4. Selecione Alterar configurações de adaptador.
5. Clique com o botão direito do mouse em Adaptador de rede Citrix PV Ethernet nº 0 e selecione Propriedades.



6. Na caixa de diálogo Propriedades de conexão de área local, selecione Configurar para abrir a caixa de diálogo Propriedades do adaptador Citrix PV Ethernet nº 0.
7. Na guia Avançado, desabilite cada uma das propriedades, exceto Valor correto da soma de verificação TCP/UDP. Para desabilitar uma propriedade, seleciona-a em Propriedade e escolha Desabilitado em Valor.
8. Escolha OK.
9. Execute os comandos a seguir em uma janela do prompt de comando.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Reinicialize a instância.

Sincronização de horário

Antes da versão de 13/02/2013, a AMI do Windows, o agente convidado do Citrix Xen poderiam definir a hora do sistema incorretamente. Isso pode fazer com que seu locação de DHCP expire. Se você tiver problemas para se conectar à sua instância, talvez precise atualizar o agente.

Para determinar se você tem o agente convidado do Citrix Xen atualizado, verifique se a data do arquivo `C:\Program Files\Citrix\XenGuestAgent.exe` é a partir de março de 2013. Se a data nesse arquivo for anterior, atualize o serviço do agente convidado do Citrix Xen. Para ter mais informações, consulte Atualizar o serviço de agente convidado do Citrix Xen.

Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU

É possível ser afetado por esse problema se estiver usando instâncias do Windows que executam os drivers AWS PV que usam mais de 20.000 IOPS, e se você encontrar o código `0x9E: USER_MODE_HEALTH_MONITOR` de verificação de bugs.

As leituras e gravações de disco (E/S) nos drivers AWS PV ocorrem em duas fases: Preparação de E/S e Conclusão de E/S. Por padrão, a fase de preparação é executada em um único núcleo arbitrário. A fase de conclusão é executada no núcleo `0`. A quantidade de computação necessária para processar uma E/S varia de acordo com o tamanho e outras propriedades. Algumas E/S usam mais computação na fase de preparação, e outras na fase de conclusão. Quando uma instância gera mais de 20.000 IOPS, a fase de preparação ou conclusão pode resultar em um gargalo, em que a CPU na qual ela é executada está com 100% de capacidade. Se a fase de preparação ou conclusão se torna ou não um gargalo depende das propriedades de E/S usadas pela aplicação.

Começando nos drivers AWS PV 8.4.0, a carga da fase de preparação e de conclusão podem ser distribuídas por vários núcleos, eliminando gargalos. Cada aplicação usa diferentes propriedades de E/S. Portanto, a adoção de uma das configurações a seguir pode aumentar, reduzir ou não afetar a performance da aplicação. Depois de aplicar qualquer uma dessas configurações, monitore a aplicação para verificar se ela está proporcionando a performance desejada.

1. Pré-requisitos

   Antes de iniciar este procedimento de solução de problemas, verifique os seguintes pré-requisitos:

   - A instância usa drivers AWS PV versão 8.4.0 ou posterior. Para atualizar, consulte Atualizar drivers de PV em instâncias do Windows.

- Você tem acesso RDP à instância. Para conhecer as etapas para se conectar à instância baseada no Windows usando RDP, consulte Conexão com a instância do Windows usando um cliente RDP.
- Você tem acesso de administrador na instância.

2. Observe a carga da CPU na instância

   É possível usar o Gerenciador de Tarefas do Windows para visualizar a carga em cada CPU, a fim de determinar possíveis gargalos na E/S do disco.

   1. Verifique se a aplicação está executando e lidando com o tráfego semelhante à workload de produção.
   2. Conecte-se à sua instância usando RDP.
   3. Clique no menu Start (Iniciar) na sua instância.
   4. Insira `Task Manager` no menu Iniciar para abrir o Gerenciador de Tarefas.
   5. Se o Gerenciador de tarefas mostrar a exibição Summary (Resumo), clique em More details (Mais detalhes) para expandir a exibição detalhada.
   6. Escolha a guia Performance.
   7. Selecione a CPU no painel esquerdo.
   8. Clique com o botão direito do mouse no gráfico do painel principal e selecione Change graph to (Alterar gráfico para) > Logical processors (Processadores lógicos) para exibir cada núcleo individual.
   9. Dependendo de quantos núcleos estiverem na instância, com o passar do tempo será possível ver linhas exibindo a carga da CPU, ou poderá ver somente um número.
      - Se forem exibidos gráficos da carga ao longo do tempo, procure CPUs onde a caixa esteja quase totalmente sombreada.
      - Se um número for exibido em cada núcleo, procure por núcleos que consistentemente mostrem 95% ou mais.
   10. Observe se o núcleo `0` ou um núcleo diferente está experimentando uma carga pesada.

3. Escolha qual configuração aplicar

Nome da configuração	Quando aplicar esta configuração	Observações
Default configuration	A workload está gerando menos de 20.000 IOPS, ou outras configurações não melhoraram a performance ou a estabilidade.	Para essa configuração, a E/S ocorre em alguns núcleos, o que pode beneficiar workloads menores, aumentando a localidade do cache e reduzindo a comutação de contexto.
Allow driver to choose whether to distribute completion	A workload está gerando mais de 20.000 IOPS e uma carga moderada ou alta é observada no núcleo `0`.	Essa configuração é recomendada para todas as instâncias Xen que usam o PV 8.4.0 ou posterior, e que usam mais de 20.000 IOPS, independentemente de problemas serem encontrados ou não.
Distribute both preparation and completion	A workload está gerando mais de 20.000 IOPS. Ou a permissão para o driver escolher a distribuição não melhorou a performance, ou um núcleo diferente de `0` está experimentando uma alta carga.	Esta configuração permite a distribuição da preparação de E/S e da conclusão de E/S.

> **Note**
>
> Recomendamos que você não distribua a preparação de E/S sem também distribuir a conclusão de E/S (configuração `DpcRedirection` sem configuração

`NotifierDistributed`) porque a fase de conclusão é sensível à sobrecarga na fase de preparação, quando a fase de preparação estiver ocorrendo em paralelo.

Valores de chave do Registro

- NotifierDistributed

  Valor `0` ou não presente — A fase de conclusão será executada no núcleo `0`.

  Valor 1 — O driver escolhe executar a fase de conclusão, o núcleo `0` ou um núcleo adicional por disco conectado.

  Valor 2 — O driver executa a fase de conclusão em um núcleo adicional por disco conectado.
- DpcRedirection

  Valor `0` ou não presente — A fase de preparação será executada em um único núcleo arbitrário.

  Valor 1 — A fase de preparação é distribuída entre vários núcleos.

Configuração padrão

Aplique a configuração padrão com as versões de driver AWS PV anteriores à 8.4.0 ou se a degradação da performance ou da estabilidade for observada após a aplicação de uma das outras configurações nesta seção.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para remover as chaves de registro `NotifierDistributed` e `DpcRedirection`.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Reinicie a instância.

Permitir que o driver escolha se deseja distribuir a conclusão

Defina a chave de registro `NotiferDistributed` para permitir que o driver de armazenamento PV escolha se deve ou não distribuir a conclusão de E/S.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Use o comando a seguir para adicionar a chave de registro `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Reinicie a instância.

Distribuir a preparação e a conclusão

Defina as chaves de registro `NotifierDistributed` e `DpcRedirection` para sempre distribuir as fases de preparação e conclusão.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para definir as chaves de registro `NotifierDistributed` e `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Reinicie a instância.

Drivers AWS NVMe para instâncias do Windows

Os volumes do Amazon EBS e os volumes de armazenamento de instância são expostos como dispositivos de bloco NVMe em instâncias desenvolvidas no AWS Nitro System. Para utilizar totalmente o desempenho e as capacidades dos recursos do Amazon EBS para volumes expostos como dispositivos de blocos NVMe, a instância deve ter o driver AWS NVMe instalado. Todas as AMIs Windows AWS da geração atual vêm com o driver AWS NVMe instalado por padrão.

Para obter mais informações sobre o EBS e o NVMe, consulte Amazon EBS e NVMe no Guia do usuário do Amazon EBS. Para obter mais informações sobre armazenamento de instâncias em SSD e o NVMe, consulte Volumes de armazenamento de instâncias SSD.

Instalar ou atualizar drivers AWS NVMe usando o PowerShell

Se você não está usando as AMIs do Windows da AWS mais recentes fornecidas pela Amazon, use o procedimento a seguir para instalar o driver AWS NVMe atual. Execute essa atualização em um momento conveniente para reinicializar a instância. O script de instalação reiniciará sua instância ou você deverá reiniciá-la como a etapa final.

Pré-requisitos

PowerShell 3.0 ou posterior

Para fazer download e instalar o driver AWS NVMe mais recente

1. Recomendamos que você crie uma AMI como backup da seguinte forma, caso precise reverter suas alterações.

   a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
   b. No painel de navegação, escolha Instances (Instâncias).
   c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).
   d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).

e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

2. Conecte-se à instância e faça login como administrador local.
3. Faça download e extraia os drivers para sua instância usando uma das seguintes opções:
   - Usando um navegador:
     a. Faça download do pacote de drivers mais recente na instância.
     b. Extraia o arquivo zip.
   - Usando o PowerShell:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/
Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Instale o driver em sua instância executando o script do PowerShell `install.ps1` do diretório `nvme_driver` (`.\install.ps1`). Se você receber um erro, verifique se está usando o PowerShell 3.0 ou posterior.

   a. (Opcional) A partir da versão AWS NVMe`1.5.0`, as reservas persistentes Small Computer System Interface (SCSI) são suportadas para o Windows Server 2016 e versões posteriores. Esse recurso adiciona suporte ao Windows Server Failover Clustering com armazenamento compartilhado do Amazon EBS. Por padrão, esse recurso não está ativado durante a instalação.

   Você pode ativar o recurso ao executar o `install.ps1` script para instalar o driver especificando o `EnableSCSIPersistentReservations` parâmetro com um valor de`$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

Você pode desativar o recurso ao executar o `install.ps1` script para instalar o driver especificando o `EnableSCSIPersistentReservations` parâmetro com um valor de`$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. Começando com o AWS NVMe`1.5.0`, o `install.ps1` script sempre instala a `ebsnvme-id` ferramenta com o driver.

   (Opcional) Para as versões `1.4.0`1.4.1,`1.4.2`, e, o `install.ps1` script permite que você especifique se a `ebsnvme-id` ferramenta deve ser instalada com o driver.

   i. Para instalar a ferramenta `ebsnvme-id`, especifique `InstallEBSNVMeIdTool 'Yes'`.

   ii. Se você não quiser instalar a ferramenta, especifique `InstallEBSNVMeIdTool 'No'`.

   Se você não especificar `InstallEBSNVMeIdTool` e a ferramenta já está presente em `C:\ProgramData\Amazon\Tools`, o pacote atualizará a ferramenta por padrão. Se a ferramenta não estiver presente, o `install.ps1` não atualizará a ferramenta por padrão.

   Se você não quiser instalar a ferramenta como parte do pacote, e quiser instalá-la mais tarde, você pode encontrar a versão mais recente ou a ferramenta no pacote do driver. Como alternativa, você pode baixar a versão `1.0.0` do Amazon S3:

   Baixe a `ebsnvme-id` ferramenta.

5. Se o instalador não reinicializar sua instância, reinicie-a.

Instalar ou atualizar drivers NVMe da AWS com o distribuidor

É possível usar o distribuidor, um recurso do AWS Systems Manager, para instalar o pacote de drivers do NVMe uma vez ou com atualizações programadas.

1. Para obter instruções sobre como instalar o pacote de drivers do NVMe usando o distribuidor, consulte os procedimentos em Instalar ou atualizar pacotes no Guia do usuário do Amazon EC2 Systems Manager.
2. Em Tipo de instalação, escolha Desinstalar e reinstalar.
3. Em Nome, escolha AWSNVMe.
4. (Opcional) Em Argumentos adicionais, é possível personalizar a instalação especificando valores. Os valores devem ser formatados usando uma sintaxe JSON válida. Para obter exemplos de como passar argumentos adicionais para o pacote `aws configure`, consulte a documentação do Amazon EC2 Systems Manager.

   a. Começando com o AWS NVMe`1.5.0`, o driver oferece suporte a reservas persistentes SCSI para Windows Server 2016 e versões posteriores. Por padrão, esse recurso não está ativado durante a instalação.

      - Para habilitar esse recurso, especifique `{"SSM_EnableSCSIPersistentReservations": true}`.
      - Se você não quiser habilitar esse recurso, especifique `{"SSM_EnableSCSIPersistentReservations": false}`.

   b. Começando com o AWS NVMe`1.5.0`, o `install.ps1` script sempre instalará a `ebsnvme-id` ferramenta.

      (Opcional) Para as versões`1.4.0`,`1.4.1`, e`1.4.2`,, o `install.ps1` script permite que você especifique se a ferramenta ebsnvme-id deve ser instalada com o driver.

      - Para instalar a ferramenta ebsnvme-id, especifique `{"SSM_InstallEBSNVMeIdTool": "Yes"}`.
      - Se você não quiser instalar a ferramenta, especifique `{"SSM_InstallEBSNVMeIdTool": "No"}`.

        Se `SSM_InstallEBSNVMeIdTool` não for especificado em Additional Arguments (Argumentos adicionais) e a ferramenta já está presente em `C:\ProgramData\Amazon\Tools`, o pacote atualizará a ferramenta por padrão. Se a ferramenta não estiver presente, o pacote não atualizará a ferramenta por padrão.

        Se você não quiser instalar a ferramenta como parte do pacote, e quiser instalá-la mais tarde, você pode encontrar a versão mais recente da ferramenta no pacote do driver. Como alternativa, você pode baixar a versão `1.0.0` do Amazon S3:

Baixe a `ebsnvme-id` ferramenta.

5. Se o instalador não reinicializar sua instância, reinicie-a.

Configurar reservas persistentes SCSI

Depois que a versão do driver AWS NVMe `1.5.0` ou posterior for instalada, você poderá habilitar ou desabilitar as reservas persistentes de SCSI usando o registro do Windows para Windows Server 2016 e versões posteriores. Você deve reiniciar a instância de banco de dados antes que a alteração entre em vigor.

Você pode habilitar reservas persistentes de SCSI com o comando a seguir, que define `EnableSCSIPersistentReservations` o como um valor de`1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Você pode desativar as reservas persistentes de SCSI com o comando a seguir, que define `EnableSCSIPersistentReservations` o como um valor de`0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

Histórico da versão do driver AWS NVMe

A tabela a seguir descreve as versões lançadas do driver AWS NVMe.

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.5.1	1.5.0	Corrigido o script de instalação para criar uma pasta para a ferramenta ebsnvme-id se ela não estiver presente.	17 de novembro de 2023

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.5.0	1.5.0	Foi adicionado suporte para reservas persistentes da Small Computer System Interface (SCSI) para instâncias que executam o Windows Server 2016 e versões posteriores. A ferramenta ebsnvme-id (`ebsnvme-id.exe`) agora é instalada por padrão.	31 de agosto de 2023
1.4.2	1.4.2	Corrigido um erro em que o Driver do AWS NVMe não oferecia suporte a volumes de armazenamento em instâncias D3.	16 de março de 2023
1.4.1	1.4.1	Relatórios Namespace Preferred Write Granularity (NPGW) para volumes do EBS que suportem esse recurso de NVMe opcional. Para obter mais informações, consulte a seção 8.25, “Melhorando o desempenho por meio do tamanho da E/S e aderência ao alinhamento”, na Especificação básica do NVMe, versão 1.4.	20 de maio de 2022

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.4.0	1.4.0	• Adicionado suporte para IOCTLs, que permitem que as aplicações interajam com dispositivos NVMe. Esse suporte permite que as aplicações obtenham a lista de `IdentifyController` , `IdentifyNamespace` e `NameSpace` do dispositivo NVMe. Para obter mais informações, consulte Consultas específicas do protocolo na documentação da Microsoft. • A instalação do AWSNVMe 1.4.0 no Windows Server 2008 R2 falhará. O AWSNVMe versão 1.3.2 e anteriores são compatíveis com o Windows Server 2008 R2. • A versão 1.4.0 do driver e a ferramenta `ebsnvme-id` mais recente (`ebsnvme-id.exe`) são combinadas em um único pacote. Essa combinação permite instalar o driver e a ferramenta de um único pacote. Para obter mais detalhes, consulte Instalar ou atualizar drivers AWS NVMe usando o PowerShell. • Correções de bugs e aprimoramentos em confiabilidade.	23 de novembro de 2021
1.3.2	1.3.2	Corrigido o problema com a modificação de volumes do EBS processando a E/S ativamente, o que pode resultar em dados corrompidos. Os clientes que não modificam volumes do EBS online (por exemplo, redimensionando ou alterando o tipo) não são afetados.	10 de setembro de 2019

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.3.1	1.3.1	Melhorias de confiabilidade.	21 de maio de 2019
1.3.0	1.3.0	Melhorias de otimização do dispositivo.	31 de agosto de 2018
1.2.0	1.2.0	Melhorias na performance e confiabilidade para dispositivos NVMe da AWS em todas as instâncias compatíveis, incluindo instâncias bare metal.	13 de junho de 2018
1.0.0	1.0.0	Driver NVMe da AWS para tipos de instâncias compatíveis executando Windows Server.	12 de fevereiro de 2018

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Como assinar as notificações do EC2 no console

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:

    a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

    arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. Para Protocolo, selecione `Email`.

c. Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações.

d. Selecione Create subscription.

6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Subscriptions.
3. Marque a caixa de seleção da assinatura e, depois, selecione Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Para assinar as notificações do EC2 usando a AWS CLI

Para assinar as notificações do EC2 com a AWS CLI, use o comando a seguir.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Para assinar as notificações do EC2 usando o AWS Tools for Windows PowerShell

Para assinar as notificações do EC2 com AWS Tools for Windows PowerShell, use o comando a seguir.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configurar sua instância do Windows

Após iniciar uma instância do Windows, você poderá fazer login como administrador para executar configurações adicionais para agentes de inicialização e recursos específicos do Windows. Os tópicos apresentados a seguir se concentram na configuração da instância do Windows.

Conteúdo

- Definição das configurações de inicialização para instâncias do Windows do Amazon EC2
- Uso do EC2 Fast Launch para as instâncias do Windows
- Uso de aceleradores Amazon Elastic Graphics em instâncias do Windows
- Instale o WSL em sua instância do Windows

Definição das configurações de inicialização para instâncias do Windows do Amazon EC2

Os agentes de inicialização do Amazon EC2 executam tarefas durante a inicialização da instância e serão executados se uma instância for interrompida e, posteriormente, iniciada ou reiniciada. Para obter informações sobre um agente específico, consulte as páginas de detalhes na lista a seguir.

- Configurar uma instância do Windows usando o EC2Launch v2
- Configurar uma instância do Windows usando o EC2Launch
- Configuração de uma instância do Windows usando o serviço EC2Config (herdado)

Conteúdo

- Comparação entre os agentes de inicialização do Amazon EC2
- Configuração do sufixo DNS para agentes de inicialização do Windows

Comparação entre os agentes de inicialização do Amazon EC2

A tabela a seguir mostra as principais diferenças funcionais entre EC2Config, EC2Launch v1 e EC2Launch v2.

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Executar como	Windows Service	Scripts PowerShell	Windows Service
Suporte	Somente SO herdado	Windows 2016 Windows 2019 (LTSC e SAC)	Windows 2016 Windows 2019 (LTSC e SAC) Windows 2022
Arquivo de configuração	XML	XML	YAML
Definir nome de usuário do administrador	Não	Não	Sim
Tamanho dos dados do usuário	16 KB	16 KB	60 KB (compactado)
Dados de usuário local incorporados na AMI	Não	Não	Sim, configurável
Configuração de tarefa nos dados do usuário	Não	Não	Sim
Papel de parede configurável	Não	Não	Sim
Personalizar a ordem de execução de tarefas	Não	Não	Sim
Tarefas configuráveis	15	9	20 na execução

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Oferece suporte ao Visualizador de eventos do Windows	Sim	Não	Sim
Número dos tipos de eventos do Visualizador de eventos	2	0	30

> **Note**
>
> A documentação do EC2Config é fornecida somente para referência histórica. As versões do sistema operacional em que ele é executado não têm mais suporte pela Microsoft. É altamente recomendável atualizar para o serviço de execução mais recente.

Configuração do sufixo DNS para agentes de inicialização do Windows

Com os agentes de inicialização do Amazon EC2, é possível configurar uma lista de sufixos DNS que as instâncias do Windows usam para a resolução de nomes de domínio. Os agentes de inicialização substituem as configurações padrão do Windows na chave de registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` ao adicionar os seguintes valores à lista de pesquisa de sufixos DNS:

- O domínio da instância
- Os sufixos que resultam da devolução do domínio da instância
- O domínio NV
- Os domínios especificados por cada placa de interface de rede

Todos os agentes de inicialização são compatíveis com a configuração de sufixo DNS. Para obter mais informações, consulte a versão específica do seu agente de inicialização:

- Para obter informações sobre a tarefa `setDnsSuffix` e como configurar sufixos DNS no EC2Launch v2, consulte setDnsSuffix .

- Para obter informações sobre a configuração da lista de sufixos DNS e como habilitar ou desabilitar a devolução para o EC2Launch v1, consulte Configurar o EC2Launch.
- Para obter informações sobre a configuração da lista de sufixos DNS e como habilitar ou desabilitar a devolução para o EC2Config, consulte Arquivos de configurações do EC2Config.

Devolução de nome de domínio

A devolução de nome de domínio é um comportamento do Active Directory que permite que computadores em um domínio secundário acessem recursos no domínio principal sem a necessidade de usar um nome de domínio totalmente qualificado. Por padrão, a devolução de nome de domínio continua até que restem somente dois nós na progressão do nome de domínio.

Os agentes de inicialização executarão a devolução no nome de domínio se a instância estiver conectada a um domínio e adicionarão os resultados à lista de pesquisa de sufixos DNS mantida na chave do registro **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**. Os agentes usam as configurações das chaves de registro apresentadas a seguir para determinar o comportamento de devolução.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Quando não há definição, desabilita a devolução.
  - Quando está definida como `1`, habilita a devolução (padrão).
  - Quando está definida como `0`, desabilita a devolução.
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Quando não há definição, use o nível de 2 (padrão).
  - Quando está definida como `3` ou valores superiores, use o valor para definir o nível.

Quando você desabilita a devolução ou altera as configurações de devolução para um nível superior, a chave do registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` ainda contém os sufixos que foram adicionados anteriormente. Eles não são removidos automaticamente. É possível atualizar a lista de forma manual ou limpá-la e deixar seu agente executar o processo para configurar a nova lista.

> **Note**
>
> Para limpar a lista de sufixos DNS do registro, você pode executar o comando apresentado a seguir.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Exemplos de devolução

Os exemplos apresentados a seguir demonstram a progressão do nome de domínio por meio do processo de devolução.

`corp.example.com`

- Progride para `example.com`

`locale.region.corp.example.com`

1. Progride para `region.corp.example.com`
2. Progride para `corp.example.com`
3. Progride para `example.com`

`locale.region.corp.example.com` com uma configuração de `DomainNameDevolutionLevel=3`

1. Progride para `region.corp.example.com`
2. Progride para `corp.example.com` A progressão é interrompida aqui devido à configuração do nível.

Configurar uma instância do Windows usando o EC2Launch v2

Todas as instâncias compatíveis do Amazon EC2 que executam o Windows Server 2022 incluem o agente de execução EC2Launch v2 (`EC2Launch.exe`) por padrão. Também fornecemos AMIs do Windows Server 2016 e 2019 com o EC2Launch v2 instalado como o agente padrão de

execução. Essas AMIs são fornecidas além das AMIs do Windows Server 2016 e 2019 que incluem o EC2Launch v1. É possível procurar por AMIs do Windows que incluam o EC2Launch v2 por padrão inserindo o seguinte prefixo em sua pesquisa na página AMIs no console do Amazon EC2: `EC2LaunchV2-Windows_Server-*`.

O EC2Launch v2 executa tarefas durante o startup da instância e é executado se uma instância for interrompida e iniciada posteriormente, ou reiniciada. O EC2Launch v2 também pode executar tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. O serviço EC2Launch v2 é compatível com todos os recursos EC2Config e EC2Launch.

Esse serviço usa um arquivo de configuração para controlar sua operação. É possível atualizar o arquivo de configuração usando uma ferramenta gráfica ou editando-o diretamente como único arquivo .yml (`agent-config.yml`). Os binários de serviço ficam localizados no diretório `%ProgramFiles%\Amazon\EC2Launch`.

O EC2Launch v2 publica logs de eventos do Windows para ajudá-lo a solucionar erros e definir gatilhos. Para ter mais informações, consulte Logs de eventos do Windows.

Sistemas operacionais compatíveis

- Windows Server 2022
- Windows Server 2019 (canal de manutenção de longo prazo e canal semestral)
- Windows Server 2016

Conteúdos da seção EC2Launch v2

- Visão geral do EC2Launch v2
- Instalar a versão mais recente do EC2Launch v2
- Migrar para o EC2Launch v2
- Interromper, reiniciar, excluir ou desinstalar o EC2Launch v2
- Assinar notificações do serviço EC2Launch v2
- Configurações do EC2Launch v2
- Solucionar problemas do EC2Launch v2
- Históricos de versões do EC2Launch v2

Visão geral do EC2Launch v2

O EC2Launch v2 é um serviço que executa tarefas durante o startup da instância e é executado se uma instância for interrompida e iniciada posteriormente, ou reiniciada.

Tópicos de visão geral

- Conceitos do EC2Launch v2
- Tarefas do EC2Launch v2
- Telemetria

Para comparar os recursos da versão do agente de inicialização, consulte Comparação entre os agentes de inicialização do Amazon EC2.

Conceitos do EC2Launch v2

É útil entender os conceitos a seguir ao considerar o EC2Launch v2.

Tarefa

É possível invocar uma tarefa para realizar uma ação em uma instância. É possível configurar tarefas no arquivo `agent-config.yml` ou por meio de dados do usuário. Para obter uma lista das tarefas disponíveis no EC2Launch v2, consulte Tarefas do EC2Launch v2. Para obter o esquema e os detalhes de configuração da tarefa, consulte Configuração de tarefas do EC2Launch v2.

Estágio

Um estágio é um agrupamento lógico de tarefas que o agente EC2Launch v2 executa. Algumas tarefas podem ser executadas apenas em um estágio específico. Outras podem ser executadas em vários estágios. Ao usar `agent-config.yml`, você deve especificar uma lista de estágios e uma lista das tarefas de cada estágio.

O serviço executa as etapas nesta ordem:

Etapa 1: Boot

Etapa 2: Network

Etapa 3: PreReady

O Windows está pronto

Após a conclusão do estágio PreReady, o serviço envia a mensagem `Windows is ready` para o console do Amazon EC2.

Etapa 4: PostReady

Os dados do usuário são executados durante o estágio PostReady. Algumas versões de script são executadas antes do estágio PostReady do arquivo `agent-config.yml` e outras depois, da seguinte forma:

Antes do `agent-config.yml`

- Dados de usuário em YAML versão 1.1
- Dados de usuário em XML

Depois de `agent-config.yml`

- Dados do usuário em YAML versão 1.0 (versão antiga para compatibilidade com versões anteriores)

Para obter exemplos dos estágios e das tarefas, consulte Exemplo: `agent-config.yml`.

Ao usar dados do usuário, você deve especificar uma lista de tarefas para o agente de inicialização executar. O estágio está implícito. Para obter exemplos de tarefas, consulte Exemplo: dados do usuário.

O EC2Launch v2 executa a lista de tarefas na ordem especificada em `agent-config.yml` e nos dados do usuário. Os estágios são executados sequencialmente. O próximo estágio começa após a conclusão do estágio anterior. As tarefas também são executadas sequencialmente.

Frequência

A frequência da tarefa determina quando as tarefas devem ser executadas, dependendo do contexto de inicialização. A maioria das tarefas tem apenas uma frequência permitida. Você pode especificar uma frequência para as tarefas `executeScript`.

Você verá as seguintes frequências no Configuração de tarefas do EC2Launch v2.

- Uma vez — a tarefa é executada uma vez, mediante a inicialização da AMI pela primeira vez (Sysprep concluído).
- Sempre: a tarefa é executada toda vez que o agente de inicialização é executado. O agente de inicialização é executado quando:

- uma instância inicia ou reinicia
- o serviço EC2Launch é executado
- O `EC2Launch.exe run` é invocado

agent-config

O `agent-config` é um arquivo localizado na pasta de configuração do EC2Launch v2. Ele inclui a configuração para os estágios de inicialização, rede, PreReady e PostReady. Este arquivo é usado para especificar a configuração de uma instância para tarefas que devem ser executadas quando a AMI é inicializada pela primeira vez ou em ocasiões posteriores.

Por padrão, a instalação do EC2Launch v2 instala um arquivo `agent-config` que inclui configurações recomendadas usadas nas AMIs padrão do Amazon Windows. É possível atualizar o arquivo de configuração de modo a alterar a experiência de inicialização padrão para sua AMI especificada pelo EC2Launch v2.

Dados do usuário

Os dados do usuário são dados que podem ser configurados ao iniciar uma instância. É possível atualizar os dados do usuário para alterar de maneira dinâmica como as AMIs personalizadas ou AMIs de início rápido são configuradas. O EC2Launch v2 suporta 60 kB de comprimento de entrada de dados do usuário. Os dados do usuário incluem apenas o estágio do UserData e, portanto, são executados após o arquivo `agent-config`. É possível inserir dados do usuário ao executar uma instância usando o assistente de execução de instância ou pode modificar os dados do usuário no console do EC2. Para obter mais informações sobre como trabalhar com dados do usuário, consulteComo o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

Tarefas do EC2Launch v2

O EC2Launch v2 pode executar as seguintes tarefas em cada inicialização:

- Configurar papel de parede novo e opcionalmente personalizado que renderiza informações sobre a instância.
- Definir os atributos para a conta de administrador criada na máquina local.
- Adicionar sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista.
- Definir letras de unidade para quaisquer volumes adicionais e estendê-las para usar o espaço disponível.

- Gravar arquivos da configuração no disco.
- Executar scripts especificados no arquivo de configuração do EC2Launch v2 ou de `user-data`. Os scripts de `user-data` podem ser em texto simples ou compactados e fornecidos no formato base64.
- Executar um programa com os argumentos fornecidos.
- Definir o nome do computador.
- Enviar informações de instância para o console do Amazon EC2.
- Enviar a impressão digital do certificado RDP ao console do Amazon EC2.
- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Executar dados do usuário. Para obter mais informações sobre como especificar os dados do usuário, consulte Configuração de tarefas do EC2Launch v2.
- Defina rotas estáticas não persistentes para alcançar o serviço de metadados e os servidores AWS KMS.
- Definir partições que não sejam de inicialização como `mbr` ou `gpt`.
- Iniciar o serviço Systems Manager após o Sysprep.
- Otimizar as configurações do ENA.
- Ativar o OpenSSH para versões posteriores do Windows.
- Ativar os frames jumbo.
- Defina o Sysprep para execução com o EC2Launch v2.
- Publicar logs de eventos do Windows.

Telemetria

Telemetria é informação adicional que ajuda a AWS a entender melhor suas necessidades, diagnosticar problemas e fornecer recursos para melhorar sua experiência com os Serviços da AWS.

EC2Launch versão v2 `2.0.592` e, posteriormente, coletar telemetria, como métricas de uso e erros. Esses dados são coletados da instância do Amazon EC2 na qual o EC2Launch v2 é executado. Isso inclui todas as AMIs do Windows de propriedade da AWS.

Os seguintes tipos de telemetria são coletados pelo EC2Launch v2:

- Informações de uso: comandos do agente, método de instalação e frequência de execução programada.

- Erros e informações de diagnóstico: códigos de erro da instalação do agente, códigos de erro de execução e pilhas de chamada como erro.

Exemplos de dados coletados pelo:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

A telemetria está habilitada por padrão. É possível desativar a coleta de telemetria a qualquer momento. Se a telemetria estiver ativada, o EC2Launch v2 enviará dados de telemetria sem notificações adicionais do cliente.

Visibilidade de telemetria

Quando a telemetria está habilitada, ela aparece na saída do console do Amazon EC2 da seguinte maneira:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desativar telemetria em uma instância

Para desativar a telemetria para uma única instância, é possível definir uma variável de ambiente do sistema ou usar o MSI para modificar a instalação.

Para desabilitar a telemetria definindo uma variável de ambiente do sistema, execute o seguinte comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desabilitar a telemetria usando o MSI, execute o comando a seguir depois de baixar o MSI,

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Instalar a versão mais recente do EC2Launch v2

É possível usar um dos seguintes métodos para instalar o agente EC2Launch v2 em sua instância do EC2:

- Fazer download do agente do Amazon S3 e instalá-lo com o Windows PowerShell. Para URLs de downloads, consulte Downloads do EC2Launch v2 no Amazon S3.
- Instalar com o SSM Distributor.
- Instalar como um componente do EC2 Image Builder.
- Iniciar sua instância de uma AMI que tenha o EC2Launch v2 pré-instalado.

> **Warning**
>
> O AmazonEC2Launch.msi desinstala versões anteriores dos serviços de execução do EC2, como EC2Launch (v1) ou EC2Config.

Para as etapas de instalação, selecione a guia que corresponde ao seu método preferido.

Windows PowerShell

Para instalar a versão mais recente do agente do EC2Launch v2 com o Windows PowerShell, siga estas etapas.

1. Crie um diretório local.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Defina o URL do seu local de download. Execute o comando a seguir com o URL do Amazon S3 que será usado. Para URLs de downloads, consulte Downloads do EC2Launch v2 no Amazon S3.

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Use o comando a seguir para fazer download do agente e executar a instalação

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
```

```
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Para verificar a instalação, certifique-se de que o arquivo msi exista no diretório EC2Launch v2 em sua instância (`C:\ProgramData\Amazon\EC2Launch`).

AWS Systems Manager Distributor

Para configurar atualizações automáticas para o EC2Launch v2 com a Configuração rápida do AWS Systems Manager, consulte Instalar e atualizar automaticamente com o Distributor Quick Setup.

Você também pode realizar uma instalação única do pacote `AWSEC2Launch-Agent` a partir do Distribuidor do AWS Systems Manager. Para obter instruções sobre como instalar um pacote com o Systems Manager Distributor, consulte Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager SSM.

EC2 Image Builder component

É possível instalar o componente `ec2launch-v2-windows` ao criar uma imagem personalizada com o EC2 Image Builder. Para instruções sobre como criar uma imagem personalizada com o EC2 Image Builder, consulte Create an image pipeline using the EC2 Image Builder console wizard no Guia do usuário do EC2 Image Builder.

AMI

O EC2Launch v2 é fornecido pré-instalado por padrão nas seguintes AMIs do Windows Server 2022 e UEFI:

- Windows_Server-2022-English-Full-Base

- Windows_Server-2022-English-Core-Base
- AMIs do Windows Server 2022 com todos os outros idiomas
- AMIs do Windows Server 2022 com SQL instalado
- Windows_Server-2022-English-Core-EKS_Optimized

O EC2Launch v2 também vem pré-instalado nas AMIs do Windows Server a seguir. Essas AMIs podem ser encontradas no console do Amazon EC2. Também é possível usar o seguinte prefixo de pesquisa: `EC2LaunchV2-` na AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_R2_RTM-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_RTM-English-Full-Base

Instalar e atualizar o EC2Launch v2 automaticamente com o AWS Systems Manager Distributor Quick Setup

Com o AWS Systems Manager Distributor Quick Setup, você pode configurar atualizações automáticas para o EC2Launch v2. O processo a seguir configura uma Associação do Systems Manager na sua instância que atualiza automaticamente o agente EC2Launch v2 em uma frequência que você especifica. A associação criada pelo Distributor Quick Setup pode incluir instâncias dentro de uma região e Conta da AWS ou instâncias dentro de uma Organização da AWS. Para obter mais informações sobre como configurar uma organização, consulte Tutorial: Criar e configurar uma organização, no Guia do usuário do AWS Organizations.

Antes de começar, certifique-se de que as suas instâncias atendam a todos os pré-requisitos.

Pré-requisitos

Para configurar atualizações automáticas com o Distributor Quick Setup, suas instâncias devem atender aos seguintes pré-requisitos.

- Você tem pelo menos uma instância em execução que oferece suporte ao EC2Launch v2. Consulte os sistemas operacionais compatíveis com o EC2Launch v2.

- Você executou as tarefas de configuração do Systems Manager nas suas instâncias. Para obter mais informações, consulte Configurar o Systems Manager, no Guia do usuário do AWS Systems Manager.
- O EC2Launch v2 deve ser o único agente de inicialização instalado na sua instância. Se você tiver mais de um agente de inicialização instalado, sua configuração do Distributor Quick Setup falhará. Antes de configurar o EC2Launch v2 com o Distributor Quick Setup, desinstale os agentes de inicialização EC2Config ou EC2Launch v1, se existirem.

Configurar o Distributor Quick Setup para o EC2Launch v2

Para criar uma configuração para o EC2Launch v2 com o Distributor Quick Setup, use as seguintes configurações ao concluir as etapas de Implantação do pacote do Distributor:

- Pacotes de software: agente Amazon EC2Launch v2.
- Frequência de atualização: selecione uma frequência na lista.
- Destinos: escolha entre as opções de implantação disponíveis.

Para verificar o status da sua configuração, navegue até a guia Configurações do Systems Manager Quick Setup no AWS Management Console.

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Configuração rápida.
3. Na guia Configurações, selecione a linha associada à configuração que você criou. A guia Configurações lista suas configurações e inclui um resumo dos principais detalhes, como Região, Status da implantação e Status da associação.

   > **Note**
   >
   > O nome da associação para cada configuração do EC2Launch v2 Distributor começa com o seguinte prefixo: `AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Para visualizar detalhes, selecione a configuração e escolha Visualizar detalhes.

Para obter mais informações e etapas para a solução de problemas, consulte Solução de problemas com resultados do Quick Setup, no Guia do usuário do AWS Systems Manager.

Downloads do EC2Launch v2 no Amazon S3

Para instalar a versão mais recente do EC2Launch v2, baixe o instalador dos seguintes locais:

> **Note**
>
> O link de instalação de 32 bits será descontinuado. Recomendamos utilizar o link de instalação de 64 bits para instalar o EC2Launch v2. Se você precisar de um agente de inicialização de 32 bits, use EC2Config.

- 64 bits — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi
- 32 bits — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi

Configurar opções de instalação

Ao instalar ou atualizar o EC2Launch v2, você poderá configurar as opções de instalação com a caixa de diálogo de instalação do EC2Launch v2 ou com o comando msiexec em um shell de linha de comando.

Na primeira vez que o instalador do EC2Launch v2 é executado em uma instância, ele inicializa as configurações do agente de execução em sua instância da seguinte forma:

- Ele cria o caminho local e grava nele o arquivo do agente de execução. Algumas vezes, isso é chamado de instalação limpa.
- Ele cria a variável de ambiente `EC2LAUNCH_TELEMETRY`, se ela ainda não existir, e a define com base na sua configuração.

Para obter detalhes de configuração, selecione a guia que corresponde ao método de configuração que você usará.

Amazon EC2Launch Setup dialog

Ao instalar ou atualizar o EC2Launch v2, você poderá configurar as opções de instalação a seguir na caixa de diálogo de instalação do EC2Launch v2.

Opções de Instalação básica

Enviar telemetria

Quando você inclui esse recurso na caixa de diálogo de configuração, o instalador define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`. Se você desabilitar a opção Enviar telemetria, o instalador definirá a variável de ambiente com um valor de `0`.

Quando o agente EC2Launch v2 é executado, ele lê a variável de ambiente `EC2LAUNCH_TELEMETRY` para determinar se os dados de telemetria devem ser carregados. Se o valor for igual a `1`, ele carregará os dados. Caso contrário, os dados não serão carregados.

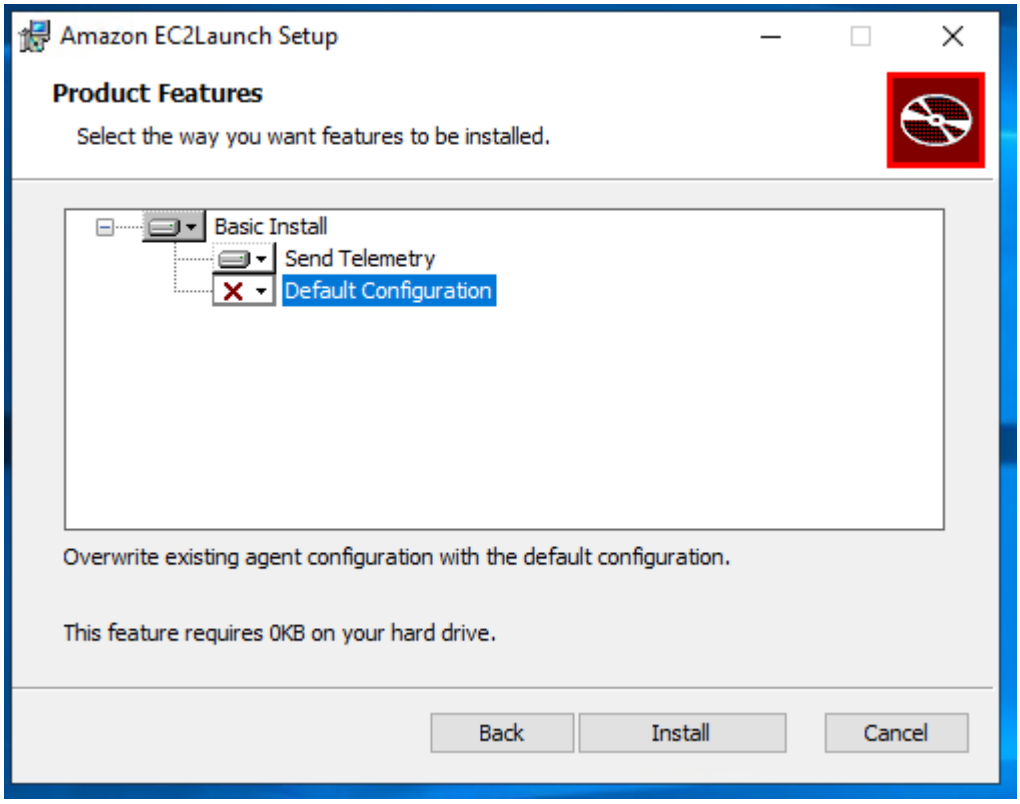
Configuração padrão

A configuração padrão do EC2Launch v2 é sobrescrever o agente de inicialização local, caso ele já exista. Na primeira vez que você executa uma instalação em uma instância, a configuração padrão realiza uma instalação limpa. Se a configuração padrão for desabilitada na instalação inicial, a instalação falhará.

Se você executar a instalação novamente na instância, poderá desabilitar a configuração padrão para realizar uma atualização que não substitua o arquivo `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Exemplo: atualizar o EC2Launch v2 com telemetria

O exemplo a seguir mostra a caixa de diálogo de configuração do EC2Launch v2 configurada para atualizar a instalação atual e habilitar a telemetria. Essa configuração realiza uma instalação sem substituir o arquivo de configuração do agente e define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`.



Command line

Ao instalar ou atualizar o EC2Launch v2, você poderá configurar as seguintes opções de instalação com o comando msiexec em um shell de linha de comando.

Valores do parâmetro **`ADDLOCAL`**

Básico (obrigatório)

Instale o agente de execução. Se esse valor não estiver presente no parâmetro `ADDLOCAL`, a instalação terminará.

Limpa

Quando o valor `Clean` é incluído no parâmetro `ADDLOCAL`, o instalador grava o arquivo de configuração do agente no seguinte local: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Se o arquivo de configuração do agente já existir, ele sobrescreverá o arquivo.

Quando o valor `Clean` é deixado de fora do parâmetro `ADDLOCAL`, o instalador executa uma atualização que não substitui o arquivo de configuração do agente.

Telemetria

Quando o valor `Telemetry` é incluído no parâmetro `ADDLOCAL`, o instalador define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`.

Quando o valor `Telemetry` é deixado de fora do parâmetro `ADDLOCAL`, o instalador define a variável de ambiente para o valor `0`.

Quando o agente EC2Launch v2 é executado, ele lê a variável de ambiente `EC2LAUNCH_TELEMETRY` para determinar se os dados de telemetria devem ser carregados. Se o valor for igual a `1`, ele carregará os dados. Caso contrário, os dados não serão carregados.

Exemplo: instalar o EC2Launch v2 com telemetria

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verificar a versão do EC2Launch v2

Use o procedimento a seguir para verificar a versão do EC2Launch v2 que está instalada nas suas instâncias.

Windows PowerShell

Verifique a versão instalada do EC2Launch v2 com o Windows PowerShell.

1. Execute uma instância pela AMI e conecte-se a ela.
2. Execute o comando a seguir no Windows PowerShell a seguir para verificar a versão instalada do EC2Launch v2.

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Verifique a versão instalada do EC2Launch v2 no Painel de Controle do Windows conforme descrito a seguir.

1. Execute uma instância pela AMI e conecte-se a ela.
2. Abra o Painel de Controle do Windows e selecione Programas e Recursos.
3. Procure `Amazon EC2Launch` na lista de programas instalados. O número da versão aparece na coluna Versão.

Para ver as atualizações mais recentes das AMIs do AWS Windows, consulte o histórico de versões da AMI do Windows na Referência da AMI do AWS Windows.

Para obter a versão mais recente do EC2Launch v2, consulte Histórico de versões do EC2Launch v2.

Para obter a versão mais recente da ferramenta de migração do EC2Launch v2, consulte Histórico de versões da ferramenta de migração do EC2Launch v2.

É possível receber notificações quando novas versões do serviço EC2Launch v2 forem liberadas. Para ter mais informações, consulte Assinar notificações do serviço EC2Launch v2.

Migrar para o EC2Launch v2

A ferramenta de migração do EC2Launch atualiza o agente de inicialização instalado (EC2Config e EC2Launch v1) ao desinstalá-lo e ao instalar o EC2Launch v2. As configurações aplicáveis dos serviços de inicialização anteriores são migradas automaticamente para o novo serviço. A ferramenta de migração não detecta qualquer tarefa agendada vinculada aos scripts do EC2Launch v1; portanto, ela não configura automaticamente essas tarefas no EC2Launch v2. Para configurar essas tarefas, edite o arquivo `agent-config.yml` ou use a caixa de diálogo de configurações do EC2Launch v2. Por exemplo, se uma instância tiver uma tarefa agendada que executa `InitializeDisks.ps1`, depois de executar a ferramenta de migração, você deverá especificar os volumes que deseja inicializar na caixa de diálogo de configurações do EC2Launch v2. Consulte a Etapa 6 do procedimento para Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2.

É possível baixar a ferramenta de migração ou instalar com um documento SSM RunCommand.

É possível fazer download da ferramenta nos seguintes locais.

> **Note**
>
> O link da ferramenta de migração de 32 bits será descontinuado. Recomendamos utilizar o link de 64 bits para migrar para o EC2Launch v2. Se você precisar de um agente de inicialização de 32 bits, use EC2Config.

- 64 bits — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/amd64/latest/EC2LaunchMigrationTool.zip
- 32 bits — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/386/latest/EC2LaunchMigrationTool.zip

> **Note**
>
> É necessário executar a ferramenta de migração do EC2Launch v2 como administrador. O EC2Launch v2 é instalado como um serviço depois da execução da ferramenta de migração. Ele não é executado imediatamente. Por padrão, ele é executado durante o startup da instância e é executado se uma instância for interrompida e posteriormente iniciada ou reiniciada.

Use o documento do SSM do `AWSEC2Launch-RunMigration` para migrar para a versão mais recente do EC2Launch v2 com o Run Command do SSM. O documento não requer parâmetros. Para obter mais informações sobre como usar o Run Command do SSM, consulte Run Command do AWS Systems Manager.

A ferramenta de migração aplica as configurações a seguir do EC2Config ao EC2Launch v2.

- Se `Ec2DynamicBootVolumeSize` for definido como `false`, o EC2Launch v2 será removido da etapa `boot`
- Se `Ec2SetPassword` for definido como `Enabled`, o tipo de senha do EC2Launch v2 será definido como `random`
- Se `Ec2SetPassword` for definido como `Disabled`, o tipo de senha do EC2Launch v2 será definido como `donothing`
- Se `SetDnsSuffixList` for definido como `false`, o EC2Launch v2 será removido da tarefa `setDnsSuffix`

- Se `EC2SetComputerName` for definido como verdadeiro, a tarefa `setHostName` do EC2Launch v2 será adicionada à configuração do `yaml`

A ferramenta de migração aplica as configurações a seguir do EC2Launch v1 ao EC2Launch v2.

- Se `ExtendBootVolumeSize` for definido como `false`, o EC2Launch v2 será removido da etapa `boot`
- Se `AdminPasswordType` for definido como `Random`, o tipo de senha do EC2Launch v2 será definido como `random`
- Se `AdminPasswordType` for definido como `Specify`, o tipo de senha do EC2Launch v2 será definido como `static` e os dados da senha como a senha especificada em `AdminPassword`
- Se `SetWallpaper` for definido como `false`, o EC2Launch v2 será removido da tarefa `setWallpaper`
- Se `AddDnsSuffixList` for definido como `false`, o EC2Launch v2 será removido da tarefa `setDnsSuffix`
- Se `SetComputerName` for definido como `true`, a tarefa `setHostName` do EC2Launch v2 será adicionada

Interromper, reiniciar, excluir ou desinstalar o EC2Launch v2

É possível gerenciar o serviço EC2Launch v2 da mesma forma como qualquer outro serviço do Windows.

O EC2Launch v2 é executado uma vez na inicialização executa todas as tarefas configuradas. Depois de executar as tarefas, o serviço entra no estado interrompido. Quando você reinicia o serviço, ele executa todas as tarefas configuradas novamente e retorna ao estado interrompido.

Para aplicar as configurações atualizadas à sua instância, interrompa e reinicie o serviço. Se estiver instalando manualmente o EC2Launch v2, você deverá interromper o serviço primeiro.

Para interromper o serviço EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e abra Serviços.
3. Na lista de serviços, clique com o botão direito sobre Amazon EC2Launch e selecione Parar.

Para reiniciar o serviço EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e abra Serviços.
3. Na lista de serviços, clique com o botão direito sobre Amazon EC2Launch e selecione Reiniciar.

Se não precisar atualizar as configurações, ao criar sua própria AMI ou usar o AWS Systems Manager, será possível excluir e desinstalar de serviço. A exclusão de um serviço remove a subchave do registro. Desinstalar um serviço elimina os arquivos, as subchaves do registro e todos os atalhos do serviço.

Para excluir o serviço EC2Launch v2

1. Inicie uma janela do prompt de comando.
2. Execute o seguinte comando:

```
sc delete EC2Launch
```

Para desinstalar o EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Start (Iniciar), selecione Control Panel (Painel de Controle).
3. Abra Programs (Programas) e, em seguida, Programs and Features (Programas e recursos).
4. Na lista de programas, escolha Amazon EC2Launch. Para confirmar que você está escolhendo a v2, marque a coluna Version (Versão).
5. Clique em Desinstalar.

Assinar notificações do serviço EC2Launch v2

O Amazon SNS pode notificá-lo quando novas versões do serviço EC2Launch v2 forem liberadas. Use o procedimento a seguir para se inscrever nessas notificações.

Assinar notificações do EC2Launch v2

1. Faça login no AWS Management Console e abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.

2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
    a. Para ARN do tópico, use o seguinte Nome de recurso da Amazon (ARN): arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2.
    b. Em Protocol (Protocolo), escolha Email.
    c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.
    d. Selecione Create subscription.
6. Você receberá um e-mail solicitando a confirmação de sua assinatura. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que uma nova versão do serviço EC2Launch v2 for liberada, nós enviaremos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

1. Abra o console do Amazon SNS.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a assinatura e escolha Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Configurações do EC2Launch v2

Esta seção contém informações sobre como definir configurações para o EC2Launch v2.

Os tópicos incluem:

- Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2
- Estrutura de diretório do EC2Launch v2
- Configurar o EC2Launch v2 com a CLI
- Configuração de tarefas do EC2Launch v2
- Códigos de saída e reinicializações do EC2Launch v2

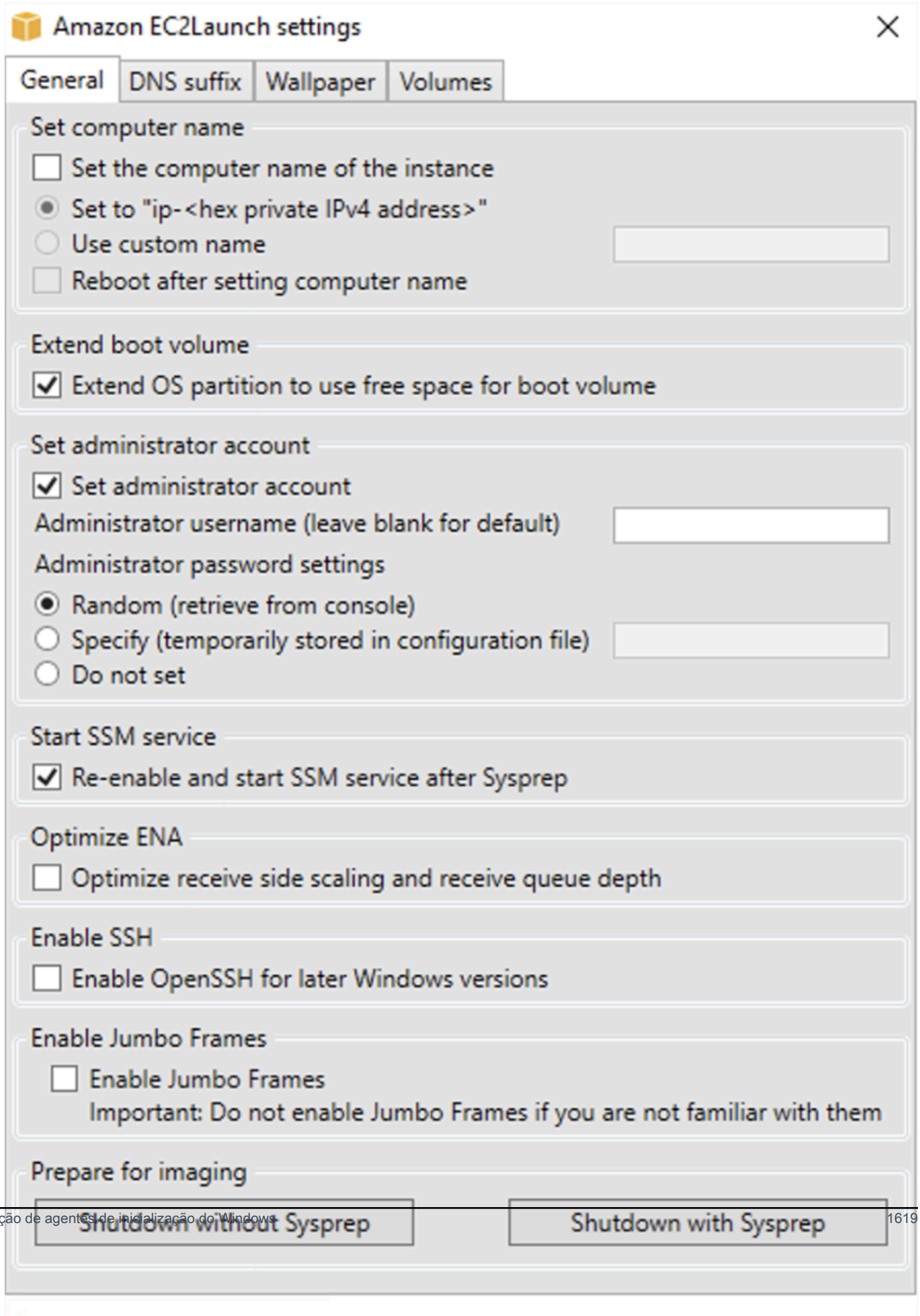
- EC2Launch v2 e Sysprep

Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2

O procedimento a seguir descreve como usar a caixa de diálogo de configurações do EC2Launch v2 para habilitar ou desabilitar configurações.

> **Note**
>
> Se você configurar de forma imprópria tarefas personalizadas no arquivo agent-config.yml e tentar abrir a caixa de diálogo de configurações Amazon EC2Launch, receberá um erro. Por obter um exemplo de esquema, consulte Exemplo: `agent-config.yml`.

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, escolha Todos os programas e navegue até as Configurações do EC2Launch.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Na guia Geral da caixa de diálogo Configurações do EC2Launch, é possível habilitar ou desabilitar as configurações a seguir.

   a. Definir o nome do computador

      Se essa configuração estiver habilitada (por padrão, ela fica desabilitada), o nome do host atual será comparado com o nome de host desejado em cada inicialização. Se os nomes de host não corresponderem, o nome do host será redefinido e o sistema, opcionalmente, reinicializa para ficar com o novo nome de host. Se um nome de host personalizado não for especificado, ele será gerado usando o endereço IPv4 privado formatado hexadecimal, por exemplo, `ip-AC1F4E6`. Para impedir a modificação de um nome de host existente, não habilite essa configuração.

   b. Estender o volume de inicialização

      Essa configuração amplia dinamicamente o `Disk 0`/`Volume 0` para incluir qualquer espaço não particionado. Isso pode ser útil quando a instância for inicializada a partir de um volume do dispositivo raiz com tamanho personalizado.

   c. Definir a conta do administrador

      Quando habilitado, é possível definir os atributos de nome de usuário e senha para a conta de administrador criada em sua máquina local. Se esse recurso não estiver habilitado, uma conta de administrador não será criada no sistema após o Sysprep. Forneça uma senha em `adminPassword` somente se `adminPasswordtype` for `Specify`.

      Os tipos de senha são definidos da seguinte maneira:

      i. `Random`

         O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

      ii. `Specify`

         O EC2Launch usa a senha especificada em `adminPassword`. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em `agent-config.yml` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

iii. `Do not set`

O EC2Launch usa a senha especificada no arquivo unattend.xml. Se você não especificar uma senha em unattend.xml, a conta de administrador será desativada.

d. Iniciar o serviço SSM

Quando selecionado, o serviço Systems Manager é habilitado para começar após o Sysprep. O EC2Launch v2 executa todas as tarefas descritas anteriormente e o SSM Agent processa recursos do Systems Manager, como Run Command e State Manager.

É possível usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço do EC2Launch v2 e do SSM Agent. Para obter mais informações, consulte Atualizar o SSM Agent usando o Run Command no Guia do usuário do AWS Systems Manager.

e. Otimizar ENA

Quando selecionadas, as configurações do ENA são definidas para garantir que as configurações Receive Side Scaling (Receber dimensionamento lateral) e Receive Queue Depth (Receber profundidade da fila) sejam otimizadas para a AWS. Para ter mais informações, consulte Configurar afinidade de CPU RSS.

f. Habilitar SSH

Essa configuração habilita o OpenSSH para versões posteriores do Windows a fim de permitir a administração remota do sistema.

g. Ativar os frames jumbo

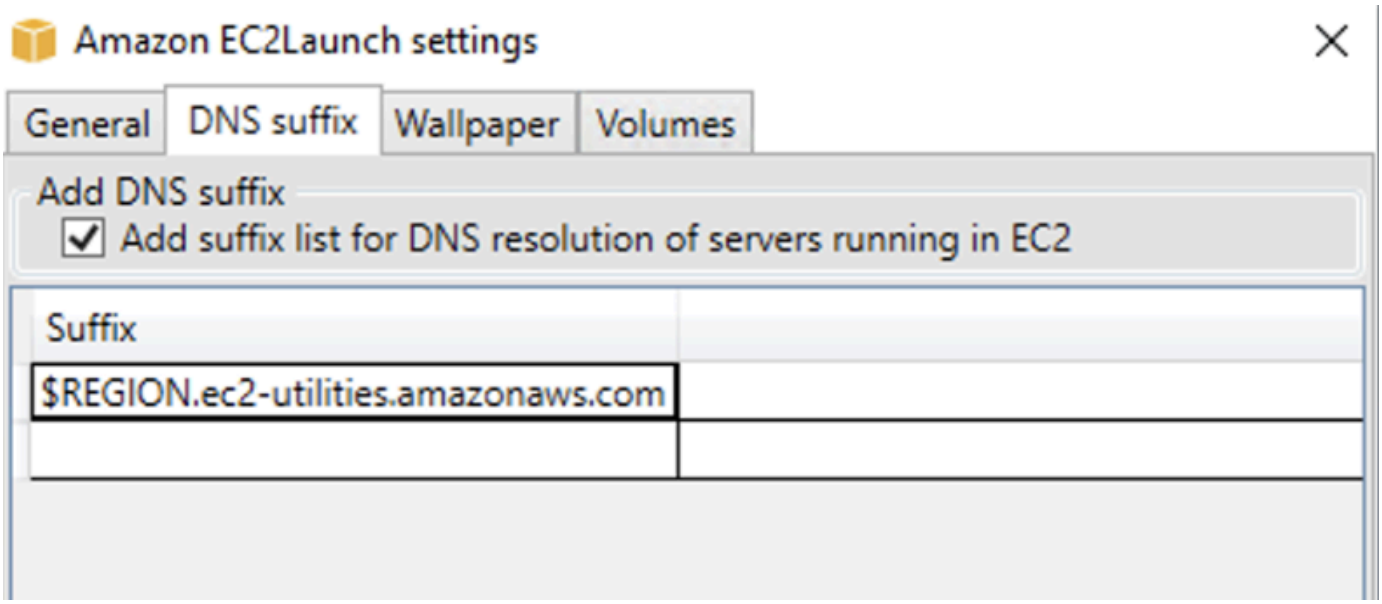
Selecione para ativar frames jumbo. Os frames jumbo podem ter efeitos não intencionais sobre suas comunicações de rede, portanto, certifique-se de entender como eles afetarão seu sistema antes de ativá-los. Para obter mais informações sobre os frames jumbo, consulte Frames jumbo (9001 MTU).

h. Preparar para imagens

Selecione se deseja que sua instância do EC2 seja desligada com ou sem Sysprep. Quando quiser executar o Sysprep com o EC2Launch v2, escolha Shutdown with Sysprep (Desligar com Sysprep).

4. Na guia Sufixo DNS, é possível selecionar se deseja adicionar uma lista de sufixos DNS para resolução DNS de servidores em execução no EC2, sem fornecer o nome de domínio totalmente

qualificado. Os sufixos DNS podem conter as variáveis `$REGION` e `$AZ`. Somente sufixos que ainda não existem serão adicionados à lista.

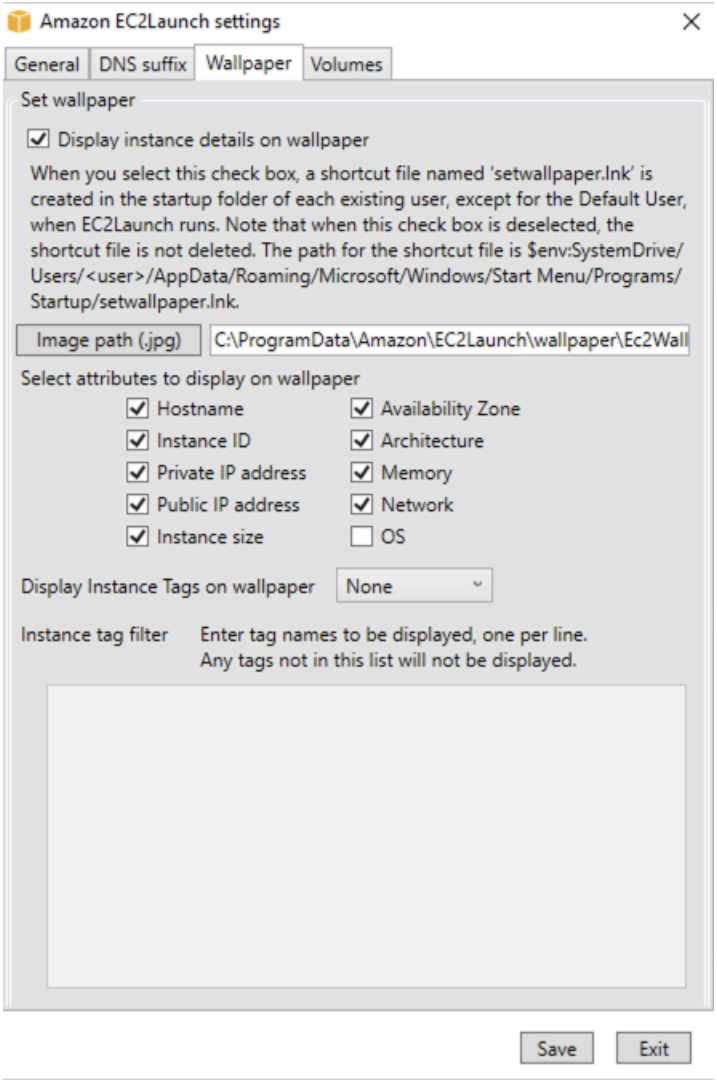


5. Na guia Papel de parede, você pode configurar o papel de parede da instância com uma imagem de fundo e especificar os detalhes da instância a serem exibidos no papel de parede. O Amazon EC2 gera os detalhes toda vez que você faz login.

   Você pode configurar o papel de parede com os seguintes controles.

   - Exibir detalhes da instância no papel de parede: essa caixa de seleção ativa ou desativa a exibição de detalhes da instância no papel de parede.
   - Caminho da imagem (.jpg): especifique o caminho até a imagem a ser usada como plano de fundo do papel de parede.
   - Selecionar atributos a serem exibidos no papel de parede: marque as caixas de seleção dos detalhes da instância que você deseja que apareçam no papel de parede. Desmarque as caixas de seleção dos detalhes da instância selecionados anteriormente que você deseja remover do papel de parede.
   - Exibir tags de instância no papel de parede: selecione uma das seguintes configurações para exibir tags de instância no papel de parede:
     - Nenhuma: não exiba nenhuma tag de instância no papel de parede.
     - Mostrar todas: exiba todas as tags de instância no papel de parede.
     - Mostrar filtradas: exibe as tags de instância especificadas no papel de parede. Quando você selecionar essa configuração, será possível adicionar tags de instância que você deseje exibir no seu papel de parede na caixa Filtro de tag de instância.

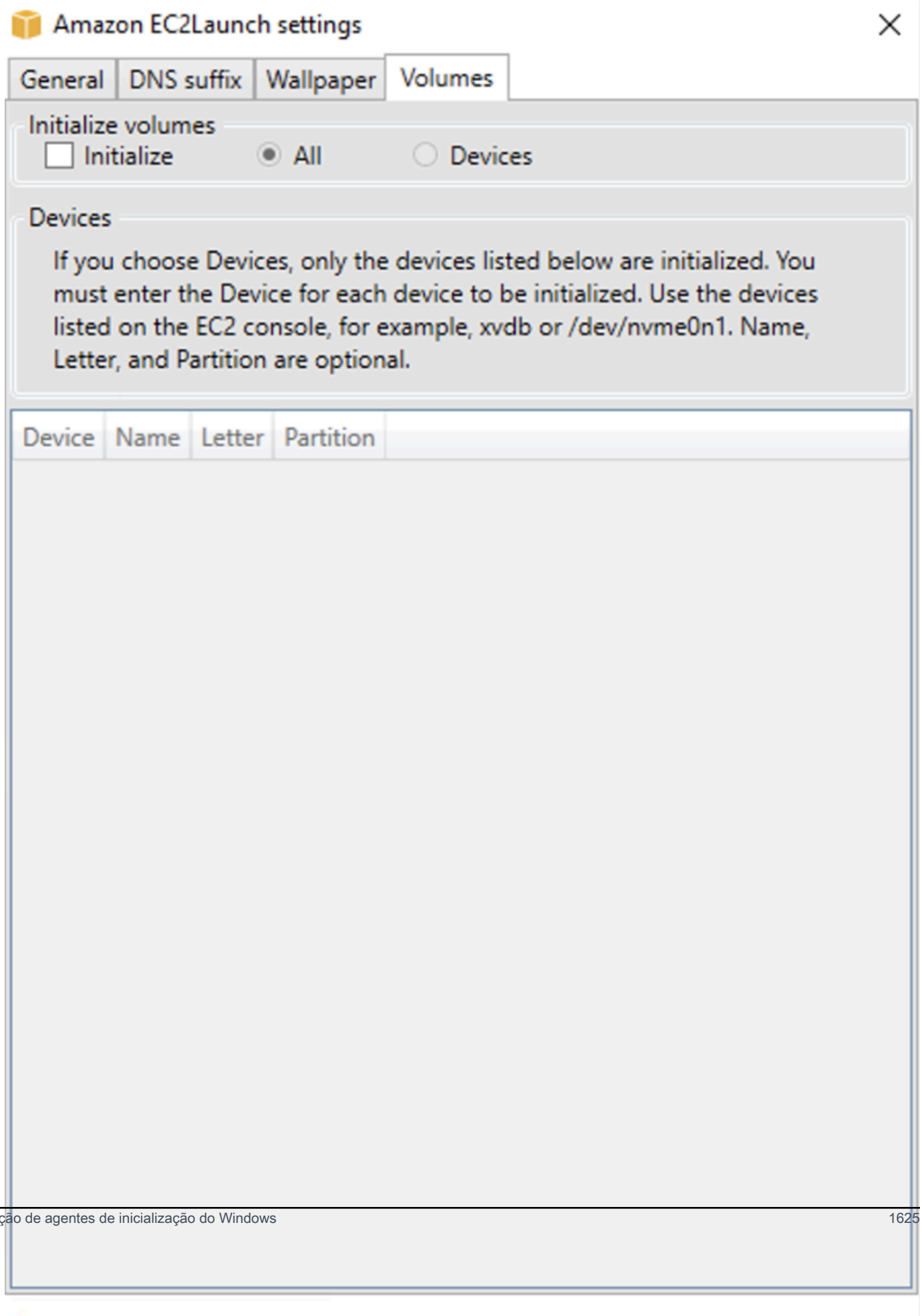
> **Note**
>
> Você deve habilitar as tags nos metadados para mostrá-las no papel de parede. Para obter mais informações sobre tags e metadados da instância, consulte Trabalho com tags de instância em metadados de instância.



6. Na guia Volumes, selecione se deseja inicializar os volumes anexados à instância. A ativação define letras de unidade para quaisquer volumes adicionais e estende-as para usar o espaço disponível. Se você selecionar Todos, todos os volumes de armazenamento serão inicializados. Se você selecionar Dispositivos, somente os dispositivos especificados na lista serão inicializados. É preciso inserir cada dispositivo a ser inicializado. Use os dispositivos listados no console do EC2, por exemplo, `xvdb` ou `/dev/nvme0n1`. A lista suspensa exibe os volumes

de armazenamento anexados à instância. Para inserir um dispositivo que não está anexado à instância, insira-o no campo de texto.

Nome, Letra e Partição são campos opcionais. Se nenhum valor for especificado para Partição, os volumes de armazenamento com mais de 2 TB serão inicializados com o tipo de partição `gpt` e os com menos de 2 TB serão inicializados com o tipo de partição `mbr`. Se os dispositivos estiverem configurados e um dispositivo não NTFS contiver uma tabela de partição ou os primeiros 4 KB do disco contiverem dados, o disco será ignorado e a ação será registrada.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Veja a seguir um exemplo de arquivo de configuração YAML criado a partir das configurações inseridas no diálogo EC2Launch.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Estrutura de diretório do EC2Launch v2

O EC2Launch v2 deve ser instalado nos seguintes diretórios:

- Binários de serviço: `%ProgramFiles%\Amazon\EC2Launch`
- Dados de serviço (configurações, arquivos de log e arquivos de estado): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e arquivos do EC2Launch v2, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório `%ProgramFiles%\Amazon\EC2Launch` contém binários e bibliotecas compatíveis. Ele inclui os seguintes subdiretórios:

- `settings`
  - `EC2LaunchSettingsUI.exe` — interface de usuário para modificar o arquivo `agent-config.yml`
  - `YamlDotNet.dll` — DLL para oferecer suporte a algumas operações na interface do usuário
- `tools`
  - `ebsnvme-id.exe` — ferramenta para examinar os metadados dos volumes do EBS na instância
  - `AWSAcpiSpcrReader.exe` — ferramenta para determinar a porta COM correta a ser usada
  - `EC2LaunchEventMessage.dll` — DLL para oferecer suporte ao registro de eventos do Windows para o EC2Launch.
- `service`
  - `EC2LaunchService.exe` — Serviço do Windows executável que é iniciado quando o agente de inicialização é executado como um serviço.
- `EC2Launch.exe` — executável principal do EC2Launch
- `EC2LaunchAgentAttribution.txt` — atribuição para código usado dentro do EC2 Launch

O diretório `%ProgramData%\Amazon\EC2Launch` contém os seguintes subdiretórios. Todos os dados produzidos pelo serviço, incluindo logs, configuração e estado, são armazenados neste diretório.

- `config`: configuração

  O arquivo de configuração do serviço é armazenado neste diretório como `agent-config.yml`. Esse arquivo pode ser atualizado de modo a modificar, adicionar ou remover tarefas padrão executadas pelo serviço. A permissão para criar arquivos neste diretório é restrita à conta de administrador para evitar o escalonamento de privilégios.
- `log`: logs de instância

  Os logs do serviço (`agent.log`), o console (`console.log`), a performance (`bench.log`), os erros (`err.log`) e a telemetria (`telemetry.log`) são armazenados neste diretório. Os arquivos de log são anexados a execuções subsequentes do serviço.
- `state`: dados de estado do serviço

  O estado usado pelo serviço para determinar quais tarefas devem ser executadas é armazenado aqui. Há um arquivo `.run-once` que indica se o serviço já foi executado após Sysprep (portanto, as tarefas com frequência de uma vez serão ignoradas na próxima execução). Esse subdiretório inclui `state.json` e `previous-state.json` para rastrear o status de cada tarefa.
- `sysprep`: Sysprep

  Esse diretório contém arquivos usados para determinar quais operações executar pelo Sysprep ao criar uma AMI do Windows personalizada que pode ser reutilizada.
- `wallpaper`: papel de parede

  As imagens de papel de parede são armazenadas nesse diretório.

Configurar o EC2Launch v2 com a CLI

É possível usar a Interface de Linhas de Comando (CLI) para definir suas configurações do EC2Launch e gerenciar o serviço. A seção a seguir contém descrições e informações de uso dos comandos da CLI que podem ser usados para gerenciamento do EC2Launch v2.

Comandos

- collect-logs
- get-agent-config
- list-volumes
- reset
- run

- status
- sysprep
- validar
- versão
- wallpaper

collect-logs

Coleta arquivos de log para o EC2Launch, compacta os arquivos e os coloca em um diretório especificado.

Exemplo

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Uso

`ec2launch collect-logs [flags]`

Sinalizadores

`-h`, `--help`

ajuda para `collect-logs`

`-o`, `--output string`

caminho para arquivos de log de saída compactados

get-agent-config

Imprime `agent-config.yml` no formato especificado (JSON ou YAML). Se nenhum formato for especificado, `agent-config.yml` será impresso no formato especificado anteriormente.

Exemplo

```
ec2launch get-agent-config -f json
```

Exemplo 2

Os seguintes comandos do PowerShell mostram como editar e salvar o arquivo `agent-config` no formato JSON.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
 ConvertFrom-Json
$jumboFrame =@"
{
   "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Uso

`ec2launch get-agent-config [flags]`

Sinalizadores

`-h`, `--help`

ajuda para `get-agent-config`

`-f`, `--format string`

formato de saída do arquivo `agent-config`: `json`, `yaml`

list-volumes

Lista todos os volumes de armazenamento anexados à instância, incluindo volumes temporários e do EBS.

Exemplo

```
ec2launch list-volumes
```

Uso

`ec2launch list-volumes`

Sinalizadores

`-h, --help`

ajuda para `list-volumes`

reset

O objetivo principal dessa tarefa é redefinir o agente para a próxima vez que ele for executado. Para fazer isso, o comando reset exclui todos os dados de estado do agente do EC2Launch v2 do `EC2Launch` diretório local (consulte Estrutura de diretório do EC2Launch v2). Opcionalmente, a redefinição exclui os logs do serviço e do Sysprep.

O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Exemplo

```
ec2launch reset -c
```

Uso

`ec2launch reset [flags]`

Sinalizadores

`-c`, `--clean`

limpa os logs da instância antes de `reset`

`-h`, `--help`

ajuda para `reset`

run

Executa o EC2Launch v2.

Exemplo

```
ec2launch run
```

Uso

`ec2launch run [flags]`

Sinalizadores

`-h`, `--help`

ajuda para `run`

status

Obtém o status do agente EC2Launch v2. Opcionalmente, bloqueia o processo até que o agente seja concluído. O código de saída do processo determina o estado do agente:

- `0`: o agente foi executado de forma bem-sucedida.

- 1: o agente foi executado e apresentou falha.
- 2: o agente ainda está em execução.
- 3: o agente está em um estado desconhecido. O estado do agente é não está em execução ou foi interrompido.
- 4: ocorreu um erro ao tentar recuperar o estado do agente.
- 5: o agente não está em execução e o status da última execução conhecida é desconhecido. Isso pode significar uma das seguintes opções:
  - tanto o `state.json` quanto o `previous-state.json` foram excluídos.
  - o `previous-state.json` está corrompido.

  Este é o estado do agente após executar o comando `reset`.

Exemplo:

```
ec2launch status -b
```

Uso

`ec2launch status [flags]`

Sinalizadores

`-b,--block`

bloqueia o processo até que o agente conclua a execução

`-h,--help`

ajuda para `status`

sysprep

O objetivo principal dessa tarefa é redefinir o agente para a próxima vez que ele for executado. Para fazer isso, o comando sysprep redefine o estado do agente, atualiza o arquivo `unattend.xml`, desabilita o RDP e executa o Sysprep.

O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Exemplo:

```
ec2launch sysprep
```

Uso

`ec2launch sysprep [flags]`

Sinalizadores

`-c,--clean`

limpa os logs da instância antes de `sysprep`

`-h,--help`

ajuda para Sysprep

`-s,--shutdown`

desliga a instância após `sysprep`

validar

Valida o arquivo `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Exemplo

```
ec2launch validate
```

Uso

`ec2launch validate [flags]`

Sinalizadores

`-h , --help`

ajuda para `validate`

versão

Obtém a versão executável.

Exemplo

```
ec2launch version
```

Uso

`ec2launch version [flags]`

Sinalizadores

`-h, --help`

ajuda para `version`

wallpaper

Define o novo papel de parede para o caminho de papel de parede fornecido (arquivo .jpg) e exibe os detalhes da instância selecionada.

Sintaxe

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Entradas

Parâmetros

--allowed-tags [***`tag-name-1`***, ***`tag-name-n`***]

(Opcional) Matriz JSON codificada em Base64 de nomes de tags de instância para exibição no papel de parede. Você pode usar essa tag ou `--all-tags`, mas não ambas.

--attributes ***`attribute-string-1`***, ***`attribute-string-n`***

(Opcional) uma lista separada por vírgulas de strings de atributo `wallpaper` para aplicar configurações ao papel de parede.

[--path | -p] ***`path-string`***

(Obrigatório) Especifica o caminho do arquivo da imagem do plano de fundo do `wallpaper`.

Sinalizadores

--all-tags

(Opcional) Exibe todas as tags de instância no papel de parede. Você pode usar essa tag ou `--allowed-tags`, mas não ambas.

[--help | -h]

Exibe a ajuda referente ao comando wallpaper.

Configuração de tarefas do EC2Launch v2

Esta seção inclui o esquema, tarefas, detalhes e exemplos de configuração para `agent-config.yml` e dados do usuário.

Tarefas e exemplos

- Esquema: agent-config.yml
- Esquema: dados do usuário
- Definições de tarefa

Esquema: **`agent-config.yml`**

Veja a estrutura do arquivo `agent-config.yml` abaixo. Não é possível repetir uma tarefa na mesma etapa. Para obter as propriedades da tarefa, consulte as descrições da tarefa a seguir.

Estrutura do documento: agent-config.yml

JSON

```
{
 "version": "1.0",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
```

```
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Exemplo: **`agent-config.yml`**

O exemplo a seguir mostra as configurações do arquivo de configuração `agent-config.yml`.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
```

```
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

Esquema: dados do usuário

Os exemplos de JSON e YAML a seguir mostram a estrutura do documento para dados do usuário. O Amazon EC2 analisa cada tarefa nomeada na matriz `tasks` que você especifica no documento. Cada tarefa tem seu próprio conjunto de propriedades e requisitos. Para obter detalhes, consulte Definições de tarefa.

> **Note**
>
> Uma tarefa só deve aparecer uma vez na matriz de tarefas de dados do usuário.

Estrutura do documento: dados do usuário

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Exemplo: dados do usuário

Para obter mais informações sobre as funções de usuário, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

O exemplo de documento YAML a seguir mostra um script do PowerShell que o EC2Launch v2 executa como dados do usuário para criar um arquivo.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

É possível usar um formato XML para os dados do usuário que seja compatível com as versões anteriores do agente de inicialização. O EC2Launch v2 executa o script como uma tarefa `executeScript` no estágio `UserData`. Para atender ao comportamento do EC2Launch v1 e do EC2Config, o script de dados do usuário é executado por padrão como um processo anexado/em linha.

Você pode adicionar tags opcionais para personalizar a execução do seu script. Por exemplo, para executar o script de dados do usuário quando a instância é reinicializada, além de uma vez quando a instância é iniciada, é possível usar a seguinte tag:

`<persist>true</persist>`

Exemplo:

```
<powershell>
```

```
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

É possível especificar um ou mais argumentos do PowerShell com tag `<powershellArguments>`. Se nenhum argumento for passado, o EC2Launch v2 adicionará o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

Exemplo:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Para executar um script de dados de usuário XML como um processo separado, adicione a seguinte tag aos dados do usuário.

`<detach>true</detach>`

Exemplo:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> A tag de desanexação não é compatível com agentes de inicialização anteriores.

Log de alterações: dados do usuário

A tabela a seguir lista as alterações nos dados do usuário e as faz referência cruzada à versão do agente EC2Launch v2 aplicável.

Versão de dados do usuário	Detalhes	Introduzida em
1.1	• As tarefas de dados do usuário são executadas antes do estágio `PostReady` no arquivo de configuração do agente. • Executa dados do usuário antes de iniciar o Systems Manager Agent (mesmo comportamento do EC2Launch v1 e do EC2Config).*	EC2Launch v2 versão 2.0.1245
1,0	• Será descontinuada. • As tarefas de dados do usuário são executadas depois do estágio `PostReady` no arquivo de configuração do agente. Isso não é compatível com versões anteriores do EC2Launch v1. • Impactado por uma condição de corrida entre o início do Systems Manager Agent e as tarefas de dados do usuário.	EC2Launch v2 versão 2.0.0

* Quando usado com o arquivo `agent-config.yml` padrão.

Definições de tarefa

Cada tarefa tem seu próprio conjunto de propriedades e requisitos. Para obter detalhes, consulte as tarefas individuais que você deseja incluir no documento.

Tarefas

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition

- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Ativa o Windows em relação a um conjunto de servidores de AWS KMS. A ativação será ignorada se a instância for detectada como traga a sua própria licença (BYOL).

Frequência — uma vez

AllowedStages — `[PreReady]`

Entradas —

`activation`: (mapa)

`type`: (string) tipo de ativação a usar, defina como `amazon`

Exemplo

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Habilita frames jumbo, que aumentam a MTU (unidade de transmissão máxima) do adaptador de rede. Para ter mais informações, consulte Frames jumbo (9001 MTU).

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo

```
task: enableJumboFrames
```

enableOpenSsh

Habilita o Windows OpenSSH e adiciona a chave pública da instância à pasta de chaves autorizadas.

Frequência — uma vez

AllowedStages — `[PreReady, UserData]`

Entradas — nenhuma

Exemplo

O exemplo a seguir mostra como habilitar o OpenSSH em uma instância e adicionar a chave pública da instância à pasta de chaves autorizadas. Essa configuração funciona somente em instâncias que executam o Windows Server 2019 e versões posteriores.

```
task: enableOpenSsh
```

executeProgram

Executa um programa com argumentos opcionais e uma frequência especificada.

Estágios: você pode executar a tarefa `executeProgram` durante os estágios `PreReady`, `PostReady` e `UserData`.

Frequência: configurável. Consulte Entradas.

Entradas

Você pode configurar os parâmetros de runtime seguinte forma:

frequência (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `once`
- `always`

caminho (string)

(Obrigatório) O caminho do arquivo para que o executável seja executado.

argumentos (lista de strings)

(Opcional) Uma lista de argumentos separados por vírgula para fornecer ao programa como entrada.

runAs (string)

(Obrigatório) Deve ser definido como `localSystem`

Saída

Todas as tarefas gravam entradas do arquivo de log no arquivo `agent.log`. A saída adicional da tarefa `executeProgram` é armazenada separadamente em uma pasta com nome dinâmico, da seguinte forma:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

O caminho exato para os arquivos de saída está incluído no arquivo `agent.log`, por exemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Arquivos de saída para a tarefa **`executeProgram`**

`ExecuteProgramInputs.tmp`

Contém o caminho para o executável e todos os parâmetros de entrada que a tarefa `executeProgram` transmite para ele quando é executada.

`Output.tmp`

Contém a saída de runtime do programa que a tarefa `executeProgram` executa.

`Err.tmp`

Contém as mensagens de erro de runtime do programa que a tarefa `executeProgram` executa.

Exemplos

Os exemplos a seguir mostram como executar um arquivo executável de um diretório local em uma instância com a tarefa `executeProgram`.

Exemplo 1: configurar executável com um argumento

Este exemplo mostra uma tarefa `executeProgram` que executa um executável de configuração no modo silencioso.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Exemplo 2: VLC executável com dois argumentos

Este exemplo mostra uma tarefa `executeProgram` que executa um arquivo VLC executável com dois argumentos transmitidos como parâmetros de entrada.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
  arguments: ['/L=1033','/S']
  runAs: localSystem
```

executeScript

Executa um script com argumentos opcionais e uma frequência especificada. O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Estágios: você pode executar a tarefa `executeScript` durante os estágios `PreReady`, `PostReady` e `UserData`.

Frequência: configurável. Consulte Entradas.

Entradas

Você pode configurar os parâmetros de runtime seguinte forma:

frequência (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `once`

- `always`

tipo (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `batch`
- `powershell`

argumentos (lista de strings)

(Opcional) Uma lista de argumentos de string a serem transmitidos ao shell. Esse parâmetro não é compatível com `type: batch`. Se nenhum argumento for passado, o EC2Launch v2 adicionará o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

conteúdo (string)

(Obrigatório) Conteúdo de script

runAs (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `admin`
- `localSystem`

desanexar (booleano)

(Opcional) O agente do EC2Launch v2 assume como padrão a execução de um script por vez (`detach: false`). Para executar o script simultaneamente com outras tarefas, defina o valor como `true` (`detach: true`).

> **Note**
>
> Os códigos de saída de script (incluindo `3010`) não têm efeito quando `detach` é definido como `true`.

Saída

Todas as tarefas gravam entradas do arquivo de log no arquivo `agent.log`. A saída adicional do script que a tarefa `executeScript` executa é armazenada separadamente em uma pasta com nome dinâmico, da seguinte forma:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.ext`*

O caminho exato para os arquivos de saída está incluído no arquivo `agent.log`, por exemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Arquivos de saída para a tarefa **`executeScript`**

`UserScript.`*`ext`*

Contém o script que a tarefa `executeScript` executou. A extensão do arquivo depende do tipo de script especificado no parâmetro `type` da tarefa `executeScript`, da seguinte forma:

- Se o tipo for `batch`, então a extensão do arquivo será `.bat`.
- Se o tipo for `powershell`, então a extensão do arquivo será `.ps1`.

`Output.tmp`

Contém a saída de runtime do script que a tarefa `executeScript` executa.

`Err.tmp`

Contém as mensagens de erro de runtime do script que a tarefa `executeScript` executa.

Exemplos

Os exemplos a seguir mostram como executar um script em linha com a tarefa `executeScript`.

Exemplo 1: arquivo de texto de saída Hello world

Este exemplo mostra uma tarefa `executeScript` que executa um script do PowerShell para criar um arquivo de texto "Hello world" na unidade `C:`.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |-
    New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
    Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Exemplo 2: execução de dois scripts

Este exemplo mostra que a tarefa `executeScript` pode executar mais de um script, e o tipo de script não precisa necessariamente corresponder.

O primeiro script (`type: powershell`) grava um resumo dos processos atualmente em execução na instância em um arquivo de texto localizado na unidade `C:`.

O segundo script (`batch`) grava as informações do sistema no arquivo `Output.tmp`.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath C:\Process.txt
  runAs: localSystem
- frequency: always
  type: batch
  content: |
    systeminfo
```

Exemplo 3: configuração do sistema idempotente com reinicializações

Este exemplo mostra uma tarefa `executeScript` que executa um script idempotente para realizar a seguinte configuração do sistema com uma reinicialização entre cada etapa:

- Renomear o computador.
- Juntar o computador ao domínio.
- Habilitar Telnet.

O script garante que cada operação seja executada apenas uma vez. Isso evita um loop de reinicialização e torna o script idempotente.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  content: |-
    $name = $env:ComputerName
     if ($name -ne $desiredName) {
       Rename-Computer -NewName $desiredName
```

```
    exit 3010
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
    Add-Computer -DomainName $desiredDomain
    exit 3010
  }
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
{
  Install-WindowsFeature -Name "Telnet-Client"
  exit 3010
}
```

extendRootPartition

Estende o volume raiz para usar todo o espaço disponível no disco.

Frequência — uma vez

AllowedStages — `[Boot]`

Entradas — nenhuma

Exemplo

```
task: extendRootPartition
```

initializeVolume

Inicializa volumes vazios que estão anexados à instância para que eles sejam ativados e particionados. O agente de inicialização ignorará a inicialização se detectar que o volume não está vazio. Um volume será considerado vazio se os primeiros 4 KiB estiverem vazios ou se o volume não tiver um layout de unidade reconhecível pelo Windows.

O parâmetro de entrada `letter` sempre é aplicado quando essa tarefa é executada, quer a unidade tenha sido inicializada ou não.

A tarefa `initializeVolume` realiza as ações a seguir.

- Defina os atributos de disco `offline` e `readonly` como falsos.

- Crie uma partição. Se nenhum tipo de partição for especificado no parâmetro de entrada `partition`, os seguintes padrões serão aplicados:
  - Se o tamanho do disco for menor do que 2 TB, defina o tipo de partição com `mbr`.
  - Se o tamanho do disco for 2 TB ou mais, defina o tipo de partição com `gpt`.
- Formate o volume como NTFS.
- Defina o rótulo do volume como se segue:
  - Use o valor `name` do parâmetro de entrada, se especificado.
  - Se o volume for efêmero e nenhum nome estiver especificado, defina o rótulo do volume como `Temporary Storage Z`.
- Se o volume for efêmero (SSD ou HDD, não Amazon EBS), crie um arquivo `Important.txt` na raiz do volume com o seguinte conteúdo:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Armazenamento de instâncias do Amazon EC2.
```

- Defina a letra da unidade como o valor especificado no parâmetro de entrada `letter`.

Estágios: você pode executar a tarefa `initializeVolume` durante os estágios `PostReady` e `UserData`.

Frequência: sempre.

Entradas

Você pode configurar os parâmetros de runtime seguinte forma:

dispositivos (lista de mapas)

(Condicional) Configuração de cada dispositivo iniciado pelo agente de inicialização. É obrigatório quando o parâmetro de entrada `initialize` está definido como `devices`.

- dispositivo (string, obrigatório): identifica o dispositivo durante a criação da instância. Por exemplo, `xvdb`, `xvdf` ou `\dev\nvme0n1`.

- letra (string, opcional): um caractere. A letra de unidade a ser atribuída.
- nome (string, opcional): o nome do volume a ser atribuído.
- partição (string, opcional): especifique um dos seguintes valores para o tipo de partição a ser criada ou deixe o agente de inicialização usar o padrão de acordo com o tamanho do volume:
  - mbr
  - gpt

inicializar (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `all`
- `devices`

Exemplos

Os exemplos a seguir mostram exemplos de configurações de entrada para a tarefa `initializeVolume`.

Exemplo 1: inicializar dois volumes em uma instância

Este exemplo mostra uma tarefa `initializeVolume` que inicializa dois volumes secundários em uma instância. O dispositivo denominado `DataVolume2` no exemplo é efêmero.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Exemplo 2: inicializar volumes do EBS anexados a uma instância

Este exemplo mostra uma tarefa `initializeVolume` que inicializa todos os volumes vazios do EBS que estão conectados à instância.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Otimiza as configurações do ENA com base no tipo de instância atual; pode reinicializar a instância.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo

```
task: optimizeEna
```

setAdminAccount

Define atributos para a conta de administrador padrão criada na máquina local.

Frequência — uma vez

AllowedStages — `[PreReady]`

Entradas —

`name`: (string) nome da conta de administrador

`password`: (mapa)

`type`: (string) estratégia para definir a senha como `static`, `random` ou `doNothing`

`data`: (string) armazena dados se o campo `type` for estático

Exemplo

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
```

```
    type: random
```

setDnsSuffix

Adiciona sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configuração do sufixo DNS para agentes de inicialização do Windows.

Frequência — sempre

AllowedStages — `[PreReady]`

Entradas —

`suffixes`: (lista de strings) lista de um ou mais sufixos DNS válidos; variáveis de substituição válidas são `$REGION` e `$AZ`

Exemplo

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Define o nome do host do computador como uma string personalizada ou, se o `hostName` não for especificado, o endereço IPv4 privado.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas —

`hostName`: (string) nome do host opcional, que deve ser formatado conforme o seguinte.

- Ele deve ter 15 caracteres ou menos
- Ele deve conter apenas caracteres alfanuméricos (a-z, A-Z, 0-9) e hífen (-).
- Ele não deve consistir inteiramente em caracteres numéricos.

`reboot`: (booliano) indica se uma reinicialização é permitida quando o nome de host é alterado

Exemplo

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Cria o arquivo de atalho `setwallpaper.lnk` na pasta de startup de cada usuário existente, exceto para `Default User`. Esse arquivo de atalho é executado quando o usuário faz login pela primeira vez após a inicialização da instância. Ele configura a instância com um papel de parede personalizado que exibe os atributos da instância.

O caminho de arquivo de atalho é:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Quando você remover a tarefa `setWallpaper`, não exclua esse arquivo de atalho. Para ter mais informações, consulte A tarefa `setWallpaper` não está ativada, mas o papel de parede é redefinido na reinicialização.

Estágios: é possível configurar o papel de parede durante os estágios `PreReady` e `UserData`.

Frequência: `always`

Configuração do papel de parede

Você pode usar as definições a seguir para configurar o papel de parede.

Entradas

Parâmetros de entrada que você fornece e atributos que você pode definir para configurar o papel de parede:

atributos (lista de strings)

(Opcional) Você pode adicionar um ou mais dos seguintes atributos ao papel de parede:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Opcional) Você pode usar exatamente uma das seguintes opções para essa configuração.

- AllTags (string): adicione todas as tags de instância ao papel de parede.

```
instanceTags: AllTags
```

- InstanceTags (lista de strings): especifique uma lista de nomes de tags de instância para adicionar ao papel de parede. Por exemplo:

```
instanceTags:
  - Tag 1
  - Tag 2
```

caminho (string)

(Obrigatório) O caminho do nome do arquivo da imagem local no formato .jpg a ser usada como imagem do papel de parede.

Exemplo

O exemplo a seguir mostra as entradas da configuração do papel de parede que definem o caminho do arquivo da imagem de fundo do papel de parede, junto com as tags de instância denominadas `Tag 1` e `Tag 2`, e os atributos que incluem o nome do host, o ID da instância e os endereços IP públicos e privados da instância.

```
task: setWallpaper
inputs:
```

```
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Você deve habilitar as tags nos metadados para mostrá-las no papel de parede. Para obter mais informações sobre tags e metadados da instância, consulte Trabalho com tags de instância em metadados de instância.

startSsm

Iniciar o serviço Systems Manager (SSM) após o Sysprep.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo

```
task: startSsm
```

sysprep

Redefine o estado do serviço, atualiza `unattend.xml`, desativa o RDP e executa Sysprep. Esta tarefa só é executada depois que todas as outras tarefas forem concluídas

Frequência — uma vez

AllowedStages — `[UserData]`

Entradas —

`clean`: (booliano) limpa os logs de instância antes de executar o Sysprep

`shutdown`: (booliano) desliga a instância depois de executar o Sysprep

Exemplo

```
task: sysprep
inputs:
  clean: true
  shutdown: true
```

writeFile

Grava um arquivo em um destino.

Frequência — visualizar Entradas

AllowedStages — `[PostReady, UserData]`

Entradas —

`frequency`: (string) `once` ou `always`

`destination`: (string) caminho no qual gravar o conteúdo

`content`: (string) texto a gravar no destino

Exemplo

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Códigos de saída e reinicializações do EC2Launch v2

É possível usar EC2Launch v2 para definir como os códigos de saída são manipulados por seus scripts. Por padrão, o código de saída do último comando executado em um script é relatado como o código de saída de todo o script. Por exemplo, se um script incluir três comandos e o primeiro comando falhar, mas os seguintes forem bem-sucedidos, o status de execução será relatado como `success` porque o comando final foi bem-sucedido.

Se quiser que um script reinicialize uma instância, você deverá especificar `exit 3010` em seu script, mesmo quando a reinicialização for a última etapa do script. O `exit 3010` instrui o

EC2Launch v2 a reiniciar a instância e chamar o script novamente até que ele retorne um código de saída que não seja `3010` ou até que a contagem máxima de reinicializações seja atingida. O EC2Launch v2 permite um máximo de 5 reinicializações por tarefa. Se você tentar reiniciar uma instância a partir de um script usando um mecanismo diferente, como `Restart-Computer`, o status de execução do script será inconsistente. Por exemplo, ele pode ficar preso em um loop de reinicialização ou não executar a reinicialização.

Se você estiver usando um formato de dados de usuário XML compatível com agentes mais antigos, os dados do usuário poderão ser executados mais vezes do que o pretendido. Para obter mais informações, consulte O serviço executa dados do usuário mais de uma vez na seção Solução de problemas.

EC2Launch v2 e Sysprep

O serviço EC2Launch v2 executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Launch v2 acessa o Sysprep, ela usa os arquivos em `%ProgramData%\Amazon\EC2Launch` para determinar quais operações devem ser executadas. É possível editar esses arquivos indiretamente usando a caixa de diálogo Configurações do EC2Launch ou diretamente usando um editor de YAML ou um editor de texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Configurações do EC2Launch, portanto, é necessário editar as entradas diretamente.

Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

Solucionar problemas do EC2Launch v2

Esta seção mostra cenários comuns de solução de problemas para o EC2Launch v2, informações sobre como visualizar logs de eventos do Windows e saída e mensagens do log do console.

Tópicos de solução de problemas

- Cenários comuns de solução de problemas
- Logs de eventos do Windows
- Saída do log do console do EC2Launch v2

Cenários comuns de solução de problemas

Esta seção mostra cenários comuns de solução de problemas e etapas para resolução.

Cenários

- Falha no serviço ao definir o papel de parede
- Falha no serviço ao executar dados do usuário
- O serviço executa uma tarefa apenas uma vez
- Falha no serviço ao executar uma tarefa
- O serviço executa dados do usuário mais de uma vez
- As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2
- O serviço inicializa um volume do EBS que não está vazio
- A tarefa setWallpaper não está ativada, mas o papel de parede é redefinido na reinicialização
- Serviço preso no status em execução
- Um agent-config.yml inválido impede a abertura da caixa de diálogo de configurações do EC2Launch v2
- task:executeScript should be unique and only invoked once

Falha no serviço ao definir o papel de parede

Resolução

1. Verifique se `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` existe.
2. Verifique `%ProgramData%\Amazon\EC2Launch\log\agent.log` para saber se ocorreram erros.

Falha no serviço ao executar dados do usuário

Causa possível: a falha no serviço pode ter ocorrido antes da execução dos dados do usuário.

Resolução

1. Verifique `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Veja se `boot`, `network`, `preReady` e `postReadyLocalData` foram todos marcados como sucesso.
3. Se um dos estágios falhar, verifique se há erros específicos `%ProgramData%\Amazon\EC2Launch\log\agent.log`.

O serviço executa uma tarefa apenas uma vez

Resolução

1. Verifique a frequência da tarefa.
2. Se o serviço já tiver sido executado após Sysprep e a frequência da tarefa estiver definida como `once`, a tarefa não será executada novamente.
3. Defina a frequência da tarefa como `always` se você quiser que ela execute a tarefa sempre que o EC2Launch v2 for executado.

Falha no serviço ao executar uma tarefa

Resolução

1. Verifique as entradas mais recentes em `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Se não ocorrerem erros, tente executar o serviço manualmente a partir de `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` para ver se as tarefas foram bem-sucedidas.

O serviço executa dados do usuário mais de uma vez

Resolução

Os dados do usuário são tratados de forma diferente entre o EC2Launch v1 e o EC2Launch v2. O EC2Launch v1 executa dados do usuário como uma tarefa programada na instância quando `persist` for definido como `true`. Se `persist` estiver definido como `false`, a tarefa não será programada mesmo quando ela sair com uma reinicialização ou for interrompida durante a execução.

EC2Launch v2 executa dados do usuário como uma tarefa de agente e rastreia seu estado de execução. Se os dados do usuário emitirem uma reinicialização do computador ou se os dados do usuário tiverem sido interrompidos durante a execução, o estado de execução persistirá `pending` e os dados do usuário serão executados novamente na próxima inicialização da instância. Se você quiser impedir que o script de dados do usuário seja executado mais de uma vez, torne o script idempotente.

O exemplo a seguir de script idempotente define o nome do computador e se junta a um domínio.

```
<powershell>
```

```
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2

Resolução

A ferramenta de migração não detecta qualquer tarefa agendada vinculada aos scripts do EC2Launch v1; portanto, ela não configura automaticamente essas tarefas no EC2Launch v2. Para configurar essas tarefas, edite o arquivo `agent-config.yml` ou use a caixa de diálogo de configurações do EC2Launch v2. Por exemplo, se uma instância tiver uma tarefa agendada que executa `InitializeDisks.ps1`, depois de executar a ferramenta de migração, você deverá especificar os volumes que deseja inicializar na caixa de diálogo de configurações do EC2Launch v2. Consulte a Etapa 6 do procedimento para Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2.

O serviço inicializa um volume do EBS que não está vazio

Resolução

Antes de inicializar um volume, o EC2Launch v2 tenta detectar se ele está vazio. Se um volume não estiver vazio, ele ignorará a inicialização. Quaisquer volumes detectados como não vazios não são inicializados. Um volume é considerado vazio se seus primeiros 4 KiB estiverem vazios ou se o volume não tiver um layout de unidade reconhecível pelo Windows. Um volume que foi inicializado e formatado em um sistema Linux não tem um layout de unidade reconhecível pelo Windows, por exemplo MBR ou GPT. Portanto, ele será considerado vazio e será inicializado. Se você quiser

preservar esses dados, não confie na detecção de unidade vazia do EC2Launch v2. Em vez disso, especifique os volumes que você gostaria de inicializar na caixa de diálogo de configurações do EC2Launch v2 (consulte a etapa 6) ou no `agent-config.yml`.

A tarefa **`setWallpaper`** não está ativada, mas o papel de parede é redefinido na reinicialização

A tarefa `setWallpaper` cria o arquivo de atalho `setwallpaper.lnk` na pasta de startup de cada usuário existente, exceto para `Default User`. Esse arquivo de atalho é executado quando o usuário faz login pela primeira vez após a inicialização da instância. Ele configura a instância com um papel de parede personalizado que exibe os atributos da instância. Remover a tarefa `setWallpaper` não exclui esse arquivo de atalho. Exclua esse arquivo manualmente ou excluí-lo usando um script.

O caminho do atalho é:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Resolução

Exclua esse arquivo manualmente ou exclua-o usando um script.

Exemplo de script PowerShell para excluir arquivo de atalho

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Serviço preso no status em execução

Descrição

O EC2Launch v2 é bloqueado com mensagens de log (`agent.log`) semelhantes às seguintes:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Possível causa

O SAC está habilitado e usando a porta serial. Para mais informações, consulte Use SAC to troubleshoot your Windows instance (Usar o SAC para solucionar problemas de instâncias do Windows).

Resolução

Tente as seguintes etapas para resolver esse problema:

- Desative o serviço que está usando a porta serial.
- Se quiser que o serviço continue usando a porta serial, crie scripts personalizados para executar tarefas do agente de execução e invoque-os como tarefas agendadas.

Um **`agent-config.yml`** inválido impede a abertura da caixa de diálogo de configurações do EC2Launch v2

Descrição

As configurações do EC2Launch v2 tentam analisar o arquivo `agent-config.yml` antes de abrir a caixa de diálogo. Se o arquivo de configuração YAML não seguir o esquema compatível, a caixa de diálogo exibirá o seguinte erro:

`Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.`

Resolução

1. Verifique se o arquivo de configuração segue o esquema compatível.

2. Para começar do zero, copie o arquivo de configuração padrão no `agent-config.yml`. Você pode usar o exemplo `agent-config.yml` fornecido na seção Configuração da tarefa.
3. Também é possível recomeçar excluindo o `agent-config.yml`. As configurações do EC2Launch v2 geram um arquivo de configuração vazio.

`task:executeScript should be unique and only invoked once`

Descrição

Não é possível repetir uma tarefa na mesma etapa.

Resolução

Algumas tarefas devem ser inseridas como uma matriz, como executeScript e executeProgram. Para obter um exemplo de como escrever o script como uma matriz, consulte executeScript.

Logs de eventos do Windows

O EC2Launch v2 publica logs de eventos do Windows para eventos importantes, como a inicialização do serviço, o Windows pronto, e o sucesso e a falha da tarefa. Identificadores de eventos identificam exclusivamente um evento específico. Cada evento contém informações de estágio, tarefa e nível e uma descrição. É possível definir gatilhos para eventos específicos usando o identificador de eventos.

Os IDs de evento fornecem informações sobre um evento e identificam alguns eventos de forma exclusiva. O dígito menos significativo de um ID de evento indica a gravidade de um evento.

Evento	Dígito menos significativo
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Os eventos relacionados ao serviço, gerados quando o serviço é iniciado ou interrompido, incluem um identificador de evento de um dígito.

Evento	Identificador de um dígito
`Success`	`0`
`Informational`	`1`
`Warning`	`2`
`Error`	`3`

As mensagens de evento para eventos do `EC2LaunchService.exe` começam com `Service:`. As mensagens de evento para eventos do `EC2Launch.exe` não começam com `Service:`.

Os IDs de evento de quatro dígitos incluem informações sobre o estado, a tarefa e a gravidade de um evento.

Tópicos

- Formato de ID do evento
- Exemplos de ID de evento
- Esquema de log de eventos do Windows

Formato de ID do evento

A tabela a seguir mostra o formato de um identificador de eventos do EC2Launch v2.

3	2 1	0
S	T	L

As letras e números na tabela representam o tipo de evento e as definições a seguir.

Tipo de evento	Definição
S (Estágio)	0 - Mensagem de nível de serviço

Tipo de evento	Definição
	1 - Inicialização 2 - Rede 3 - PreReady 5 - O Windows está pronto 6 - PostReady 7 - Dados do usuário
T (Tarefa)	As tarefas representadas pelos dois valores correspondentes são diferentes para cada estágio. Para visualizar a lista completa de eventos, consulte Esquema de log de eventos do Windows.
L (Nível do evento)	0 - Êxito 1 - Informativo 2 - Aviso 3 - Erro

Exemplos de ID de evento

Veja a seguir alguns exemplos de IDs de evento.

- `5000` - o Windows está pronto para ser usado
- `3010` - êxito ao ativar a tarefa do Windows no estágio PreReady
- `6013` - A tarefa Definir papel de parede no estágio PostReady Local Data encontrou um erro

Esquema de log de eventos do Windows

MessageId/ID do evento	Mensagem do evento
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition

MessageId/ID do evento	Mensagem do evento
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule

MessageId/ID do evento	Mensagem do evento
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Saída do log do console do EC2Launch v2

Esta seção contém uma saída de log do console de exemplo para EC2Launch v2 e lista todas as mensagens de erro de log do console do EC2Launch v2 para ajudar você a solucionar problemas. Para obter mais informações sobre a saída do console da instância e como acessá-la, consulte the section called “Saída do console da instância”.

Outputs

- Saída do log do console do EC2Launch v2

- Mensagens de log do console do EC2Launch v2

Saída do log do console do EC2Launch v2

Veja a seguir um exemplo de saída de log do console para EC2Launch v2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
 EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-SO1T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
 1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
```

```
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

Mensagens de log do console do EC2Launch v2

Veja a seguir uma lista de todas as mensagens de log do console do EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
 Error setting up EC2Launch agent folders
 See instance logs for detail
 Error stopping service
 Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
Message: Windows sysprep configuration complete
```

```
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
User data format: {format}
```

Históricos de versões do EC2Launch v2

Históricos de versões

- Histórico de versões do EC2Launch v2
- Histórico de versões da ferramenta de migração do EC2Launch v2

Histórico de versões do EC2Launch v2

A tabela a seguir descreve as versões liberadas do EC2Launch v2.

Versão	Detalhes	Data de lançamento
2.0.1924	• Atualização da interface do usuário de configurações do EC2Launch. • Atualização do comando da CLI para o papel de parede. • Atualização do instalador do EC2Launch.	10 de junho de 2024
2.0.1914	• Adição de rotas com endereços de gateway não especific ados (`0.0.0.0` para IPv4 ou`::` para IPv6). • Sempre realize a adição tanto da rota IPv4 quanto da rota IPv6. • Correção de um problema em que o nome de usuário `Administrator` era adicionado ao arquivo `agent-con fig.yml` quando não estava especificado.	5 de junho de 2024

Versão	Detalhes	Data de lançamento
	• Modificação das permissões do EC2Launch v2.	
2.0.1881	• Adicionada uma opção de senha criptografada à tarefa `setAdminAccount` . • Adicionado o comando da CLI para criptografar senha estática em agent-config.yml. • Corrigido um problema em que os dados de usuário do XML não adicionavam argumentos do PowerShell quando executados com permissões de administrador. Para obter mais detalhes, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows. • Ajustados os argumentos do PowerShell para a tarefa `executeScript` e os scripts de dados de usuário quando executados com permissões `LocalSystem` . Quando os argumentos estão vazios, o agente usa o seguinte valor padrão: `-ExecutionPolicy Unrestricted` . • Evitada a impressão de versões duplicadas do driver no log do console.	8 de maio de 2024

Versão	Detalhes	Data de lançamento
2.0.1815	• Ajuste do tratamento de erros para gerar uma falha em problemas críticos de configuração antes da execução de sysprep. • Corrigido um problema em que tarefas de papel de parede e nome de host podiam usar um endereço IP incorreto em instâncias com vários endereços IP atribuídos à interface de rede primária. • As tarefas de papel de parede e nome de host foram alteradas para obter primeiro o IP privado do IMDS e, em seguida, retornar ao WMI se o IMDS estiver desativado. • Corrigido um problema com a tarefa `initializeVolume` em que os volumes `sc1` não eram inicializados devido a um erro transitório.	6 de março de 2024
2.0.1739	• Correção de um problema que impedia a captura de códigos de saída por tarefas `executeScript` executadas como o usuário Administrador do Windows.	17 de janeiro de 2024

Versão	Detalhes	Data de lançamento
2.0.1702	• Permissões `Telemetry.log` restritas para `read-execute` somente para usuários padrão. • Configurado o serviço EC2Launch Windows para reiniciar em caso de falha na inicialização. • Falhas `add-routes` tornadas acionáveis ao registrar em log a saída `route.exe stderr`. • Corrigido um problema que ocorre quando as métricas de rota estão fora do intervalo [1, 9999]. • Adicionado suporte a papéis de parede para vários novos tipos de instâncias. • Corrigido um problema causado por scripts de dados do usuário executados como usuário administrador do Windows e que enviam a saída para `stderr`.	4 de janeiro de 2024

Versão	Detalhes	Data de lançamento
2.0.1643	• Atualização da ferramenta `ebsnvme-id.exe` para a versão 1.1.0.7. • Correção de um problema com o Receive Side Scaling (RSS) e as configurações de profundidade da fila de recebimento em tipos de instância de metal que começam com 'metal-*', como metal-48x1. • Remoção de evento de telemetria que relata comandos de dados de usuários em XML que bloqueiam o agente. • Atualização da tarefa `setDnsSuffix` para limitar a devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Inclusão de uma tarefa pública e uma CLI que adiciona rotas de rede. • Observação: essa é a última versão a oferecer suporte oficial ao Windows Server 2012. • Observação: essa é a última versão a oferecer suporte oficial a sistemas operacionais de 32 bits.	4 de outubro de 2023
2.0.1580	• Alterou a forma como o agente de inicialização lida com erros quando você modifica as permissões do arquivo de log. • Foi adicionado um tempo limite para conexão com a porta serial. O tempo limite permite que o agente de lançamento continue em execução se a porta serial estiver em uso.	5 de setembro de 2023

Versão	Detalhes	Data de lançamento

2.0.1521	• A sinalização –`block` dos comandos `EC2Launch .exe` , reset e sysprep foi descontinuada.
	• Atualização de `EC2Launch.exe` para detectar e lidar com os comandos reset e sysprep usados em tarefas `executeScript` em linha. Esses comandos fazem com que o agente pare de ser executado depois que a tarefa `executeScript` os executa.
	• Scripts de dados de usuário em XML atualizados para serem executados em linha por padrão.
	• Permita que scripts XML de dados de usuário sejam executados separadamente com a nova tag `detach`. Para obter mais detalhes, consulte Scripts de dados do usuário.
	• As alterações a seguir foram implementadas no log do agente.
	  • Mensagens de log do agente atualizadas.
	  • Conteúdo de `executeScript` e saída removidos do log do agente.
	  • Argumentos de `executeProgram` e saída removidos do log do agente.
	• As alterações a seguir foram implementadas no log do console.
	  • Valor `EnableSCSIPersistentReservations` adicionado ao log do console.
		3 de julho de 2023

Versão	Detalhes	Data de lançamento
2.0.1303	• Foram acrescentadas linhas adicionais de tratamento de erros e de logs ao acrescentar rotas de rede. • Tarefas `executeScript` e `executeProgram` permitidas no estágio PreReady. • Tarefa `executeProgram` atualizada para gerar arquivos de saída semelhantes à saída da tarefa executeScript. Para ter mais informações, consulte executeProgram. • Foi adicionada a telemetria para monitorar o uso dos comandos do agente de bloqueio nos dados de usuário XML.	3 de maio de 2023
2.0.1245	• Maior visibilidade de falhas registrando em log pilhas de chamadas de falha em texto não criptografado. • Foi adicionado o serviço EventLog como uma dependência de startup para corrigir uma falha quando o serviço Amazon EC2Launch é iniciado mais rápido do que o serviço EventLog. • Foi feito com que os dados do usuário XML fossem executados antes do estágio PostReady a partir do arquivo de configuração do agente (como EC2Launch v1 e EC2Config). • Foram adicionados dados do usuário YAML versão 1.1 para fazer com que os dados do usuário sejam executados antes do estágio PostReady a partir do arquivo de configuração do agente (os dados do usuário YAML versão 1.0 são executados após o estágio PostReady a partir do arquivo de configuração do agente).	8 de março de 2023

Versão	Detalhes	Data de lançamento
2.0.1173	• Adiciona um recurso opcional para exibir tags de instância no papel de parede. Para ter mais informações, consulte setWallpaper . • Adiciona o tratamento de erros quando o grupo de segurança do Elastic Graphics não está configurado corretamente. • Corrige um tempo limite quando o Instance Metadata Service não está habilitado.	6 de fevereiro de 2023
2.0.1121	• Corrige um problema em que um erro 404 é impresso no papel de parede quando nenhum endereço IPv4 público é atribuído. • Corrige um problema em que o sistema de arquivos do volume é formatado como `RAW` em vez de `NTFS` quando a letra da unidade do dispositivo está definida como `D`. • Corrige um problema em que os volumes de SSD NVMe são identificados incorretamente como volumes do EBS. • Corrige um erro ao ativar o Windows quando o IMDS está desativado.	4 de janeiro de 2023

Versão	Detalhes	Data de lançamento
2.0.1082	• Corrige um problema em que o campo `setWallpaper` : `privateIpAddress` : fica em branco quando o IMDS é desabiltado. • Corrige um problema com a configuração de hostname para o endereço IPv4 privado quando o IMDS está desabilitado. • Corrige um problema com a inicialização de volumes no Windows Server 2012. • Corrige um problema com a configuração de frames jumbo. • Corrige um erro quando nenhuma chave SSH é especificada na inicialização da instância. • Corrige um erro no Windows Server 2012 quando o Windows não tem uma chave de registro “ReleaseId”.	7 de dezembro de 2022
2.0.1011	• Corrige a lógica para encontrar o adaptador de rede quando o PnPDeviceID está vazio.	11 de novembro de 2022
2.0.1009	• Usa informações do segmento PCI para selecionar a porta do console.	8 de novembro de 2022

Versão	Detalhes	Data de lançamento
2.0.982	• Adiciona lógica de nova tentativa para obtenção de informaçõ es de RDP. • Corrige erros durante a inicialização do volume em instâncias `d2.8xlarge` . • Corrige um problema que permite selecionar um adaptador de rede incorreto após uma reinicialização. • Remove a mensagem de erro de alarme falso quando o ACPI SPCR não está disponível.	31 de outubro de 2022
2.0.863	• Atualiza a lógica de espera IMDS para fazer somente solicitaç ões IMDSv2. • Adiciona lógica para atribuir a letra da unidade a volumes que já foram inicializados, mas não montados. • Imprime uma mensagem de erro mais específica quando não há suporte ao tipo do par de chaves. • Corrige o erro do código de reinicialização 3010. • Adiciona a verificação de dados do usuário com codificação base64 inválida.	6 de julho de 2022
2.0.698	• Corrige o erro de digitação na saída do log ao executar scripts.	30 de janeiro de 2022

Versão	Detalhes	Data de lançamento
2.0.674	• A telemetria carrega o controle de privacidade habilitado/desabilitado. • Corrige o bug `index out of bounds`. • Remove atalhos de papel de parede durante `sysprep`.	15 de novembro de 2021
2.0.651	• Adiciona lógica para desinstalar agentes herdados durante a instalação do EC2Launch v2. • Corrige o problema de CLI `list-volume` quando o volume raiz não está listado como volume 0.	7 de outubro de 2021
2.0.592	• Corrige o bug para relatar corretamente o status do estágio. • Remove alarmes falsos de mensagens de erro quando os arquivos de log são fechados. • Adiciona telemetria.	31 de agosto de 2021
2.0.548	• Adiciona zeros à esquerda para nome de host IP hexadecimal. • Corrige permissões de arquivo para a tarefa `enableOpenSsh`. • Corrige a falha no comando sysprep.	4 de agosto de 2021

Versão	Detalhes	Data de lançamento
2.0.470	• Corrige o erro na etapa de rede para esperar que o DHCP atribua um IP à instância. • Correções de erros com `setDnsSuffix` quando a chave de registro `SearchList` não existe. • Corrige o bug na lógica de devolução de DNS em `setDnsSuffix` . • Adiciona roteamentos de rede após reinicializações intermediárias. • Permite que `initializeVolume` volte a escrever volumes existentes. • Remove informações adicionais do subcomando da versão.	20 de julho de 2021
2.0.285	• Adiciona opção de executar scripts de usuário em um processo desanexado. • Os dados de usuário herdados (dados de usuário XML) agora são executados em um processo desvinculado, que é um comportamento semelhante ao agente de inicialização anterior. • Adiciona o sinalizador CLI ao `sysprep` e aos comandos `reset`, o que os permite bloquear até que o serviço pare. • Restringe as permissões da pasta de configuração.	8 de março de 2021

Versão	Detalhes	Data de lançamento
2.0.207	• Adiciona o campo `hostName` opcional à tarefa `setHostName` . • Corrige bugs de reinicialização. As tarefas de reinicialização `executeScript` e `executeProgram` serão marcadas como em execução. • Adiciona mais códigos de retorno ao comando de status. • Adiciona o serviço de bootstrap para corrigir problema de startup ao executar no tipo de instância `t2.nano`. • Corrige o modo de instalação limpa para remover arquivos não rastreados pelo instalador.	2 de fevereiro de 2021
2.0.160	• Corrige o comando `validate` para detectar nomes de estágios inválidos. • Adiciona o comando `w32tm resync` na tarefa `addroutes` . • Corrige o problema com a alteração da ordem de pesquisa de sufixos DNS. • Adiciona condições de verificação para relatar melhor dados inválidos do usuário.	4 de dezembro de 2020
2.0.153	Adiciona a funcionalidade Sysprep em UserData.	3 de novembro de 2020

Versão	Detalhes	Data de lançamento
2.0.146	• Corrige o problema com RootExtend em AMIs em outros idiomas. • Concede permissão de gravação ao grupo de usuários para os arquivos de log. • Cria partição MS Reserved para volumes GPT. • Adiciona o comando list-volumes e o menu suspenso de volume nas configurações do Amazon EC2Launch. • Adiciona comando get-agent-config para imprimir o arquivo agent-config.yml no formato yaml ou json. • Apaga a senha estática se nenhuma chave pública for detectada.	6 de outubro de 2020
2.0.124	• Adiciona a opção para exibir a versão do SO no papel de parede. • Inicializa volumes criptografados do EBS. • Adiciona rotas para VPCs sem nome DNS local.	10 de setembro de 2020
2.0.104	• Cria a lista de pesquisa de sufixos DNS, se ela não existir. • Ignora a hibernação se não for solicitado.	12 de agosto de 2020
2.0.0	Versão inicial.	30 de junho de 2020

Histórico de versões da ferramenta de migração do EC2Launch v2

A tabela a seguir descreve as versões lançadas da ferramenta de migração do EC2Launch v2.

Versão	Detalhes	Data de lançamento
1.0.396	• Atualização da ferramenta de migração para a versão mais recente do agente do EC2Launch v2: 2.0.1924.	11 de junho de 2024
1.0.394	• Atualização da ferramenta de migração para a versão mais recente do agente do EC2Launch v2: 2.0.1914.	6 de junho de 2024
1.0.384	• Atualizada a ferramenta de migração com a versão mais recente do agente do EC2Launch v2 agent: 2.0.1881.	8 de maio de 2024
1.0.358	• Atualização da ferramenta de migração com a versão mais recente do agente EC2Launch v2: 2.0.1815.	8 de março de 2024
1.0.345	• Atualização da ferramenta de migração com a versão mais recente do agente EC2Launch v2 2.0.1739.	18 de janeiro de 2024
1.0.342	• Atualização da ferramenta de migração com a versão mais recente do agente EC2Launch v2: 2.0.1702.	5 de janeiro de 2024
1.0.331	• Atualizar a ferramenta de migração com a versão mais recente do agente EC2Launch v2: 2.0.1643 • Correção de um erro que ocorre durante a execução `.Install.ps1 -DryRun` . • Correção de um problema em que a configuração da senha é definida incorretamente como `random` durante a migração do EC2Config. •	3 de novembro de 2023

Versão	Detalhes	Data de lançamento
	Correção de um erro que ocorre se `setWallpaper` for definido como `False` durante a migração do EC2Launch.	
1.0.303	Atualização da ferramenta de migração com a versão mais recente do agente do EC2Launch v2: 2.0.1580.	14 de setembro de 2023
1.0.286	Atualização da ferramenta de migração com a versão mais recente do agente do EC2Launch v2: 2.0.1521.	14 de julho de 2023
1.0.272	Atualização da ferramenta de migração com a versão mais recente do agente do EC2Launch v2: 2.0.1303.	3 de maio de 2023
1.0.262	Atualização da ferramenta de migração com a versão mais recente do agente do EC2Launch v2: 2.0.1245.	9 de março de 2023
1.0.241	Incremento do número da versão do agente do EC2Launch v2 para 2.0.1011.	7 de dezembro de 2022
1.0.218	• Valida o valor da região recuperado dos metadados da instância. • Corrige o erro de falha de migração em pacotes de idiomas. • Incremento do número da versão do agente do EC2Launch v2 para 2.0.863.	3 de setembro de 2022
1.0.162	• Move a lógica para remover agentes herdados para o MSI do EC2Launch v2. • Incremento do número da versão do agente do EC2Launch v2 para 2.0.698.	18 de março de 2022
1.0.136	Incremento do número da versão do agente do EC2Launch v2 para 2.0.651.	13 de outubro de 2021

Versão	Detalhes	Data de lançamento
1.0.130	Incremento do número da versão do agente do EC2Launch v2 para 2.0.548.	5 de agosto de 2021
1.0.113	Usa IMDSv2 em vez de IMDSv1.	04 de junho de 2021
1.0.101	Incremento do número da versão do agente do EC2Launch v2 para 2.0.285.	12 de março de 2021
1.0.86	Incremento do número da versão do agente do EC2Launch v2 para 2.0.207.	3 de fevereiro de 2021
1.0.76	Incremento do número da versão do agente do EC2Launch v2 para 2.0.160.	4 de dezembro de 2020
1.0.69	Incremento do número da versão do agente do EC2Launch v2 para 2.0.153.	5 de novembro de 2020
1.0.65	Incremento do número da versão do agente do EC2Launch v2 para 2.0.146.	9 de outubro de 2020
1.0.60	Incremento do número da versão do agente do EC2Launch v2 para 2.0.124.	10 de setembro de 2020
1.0.54	• Instala o EC2Launch v2 se nenhum agente estiver instalado. • Incremento do número da versão do agente do EC2Launch v2 para 2.0.104. • Desacopla o SSM Agent.	12 de agosto de 2020

Versão	Detalhes	Data de lançamento
1.0.50	Remove a dependência do NuGet.	10 de agosto de 2020
1.0.0	Versão inicial.	30 de junho de 2020

Configurar uma instância do Windows usando o EC2Launch

O EC2Launch é um conjunto de scripts do Windows PowerShell que substitui o serviço do EC2Config nas AMIs do Windows Server 2016 e 2019. Muitas dessas AMIs ainda estão disponíveis. O EC2Launch v2 é o agente de inicialização mais recente para todas as versões compatíveis do Windows, substituindo o EC2Config e o EC2Launch. Para ter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch v2.

> **Note**
>
> Para usar o EC2Launch com IMDSv2, a versão deve ser a 1.3.2002730 ou posterior.

Conteúdo

- Tarefas do EC2Launch
- Telemetria
- Instalar a versão mais recente do EC2Launch
- Verificar a versão do EC2Launch
- Estrutura de diretório do EC2Launch
- Configurar o EC2Launch
- Histórico de versões do EC2Launch

Tarefas do EC2Launch

Por padrão, o EC2Launch executa as seguintes tarefas durante a primeira inicialização da instância:

- Configura novo papel de parede que produz informações sobre a instância.

- Define o nome do computador para o endereço IPv4 privado da instância.
- Envia informações da instância ao console do Amazon EC2.
- Envia a impressão digital do certificado RDP ao console do EC2.
- Define uma senha aleatória para a conta do administrador.
- Adiciona sufixos DNS.
- Estende dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Executa dados do usuário (se especificado). Para obter mais informações sobre como especificar os dados do usuário, consulte Trabalhar com dados do usuário da instância.
- Define rotas estáticas persistentes para alcançar o serviço de metadados e os servidores AWS KMS.

> **Important**
>
> Se uma AMI personalizada for criada a partir dessa instância, essas rotas serão capturadas como parte da configuração do sistema operacional e quaisquer novas instâncias iniciadas a partir da AMI manterão as mesmas rotas, independentemente do posicionamento da sub-rede. Para atualizar as rotas, consulte Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada.

As seguintes tarefas ajudam a manter a compatibilidade com versões anteriores do serviço do EC2Config. Também é possível configurar o EC2Launch para executar essas tarefas durante o startup:

- Inicializar volumes de EBS secundários.
- Enviar logs de eventos do Windows aos logs do console do EC2.
- Enviar a mensagem O Windows está pronto para uso ao console do EC2.

Para obter mais informações sobre o Windows Server 2019, consulte Comparar recursos nas versões do Windows Server em Microsoft.com.

Telemetria

Telemetria é informação adicional que ajuda o AWS a entender melhor suas necessidades, diagnosticar problemas e fornecer recursos para melhorar sua experiência com os serviços da AWS.

O EC2Launch versão `1.3.2003498` e posteriores coleta telemetria, como métricas de uso e erros. Esses dados são coletados na instância do Amazon EC2 na qual o EC2Launch é executado. Isso inclui todas as AMIs do Windows de propriedade da AWS.

Os seguintes tipos de telemetria são coletados pelo EC2Launch:

- Informações de uso: comandos do agente, método de instalação e frequência de execução programada.
- Erros e informações de diagnóstico: instalação do agente e execução dos códigos de erro.

Exemplos de dados coletados pelo:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

A telemetria está habilitada por padrão. É possível desativar a coleta de telemetria a qualquer momento. Se a telemetria estiver habilitada, o EC2Launch enviará dados de telemetria sem notificações adicionais do cliente.

Sua escolha de habilitar ou desabilitar a telemetria é coletada.

É possível optar por habilitar ou desabilitar a coleta de telemetria. Sua seleção de optar por habilitar ou desabilitar telemetria é coletada para garantir que atenderemos à sua opção de telemetria.

Visibilidade de telemetria

Quando a telemetria é ativada, ela aparece na saída do console do Amazon EC2 da seguinte maneira:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desativar telemetria em uma instância

Para desativar a telemetria definindo uma variável de ambiente do sistema, execute o seguinte comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desabilitar a telemetria durante a instalação, execute `install.ps1` da seguinte forma:

```
. .\install.ps1 -EnableTelemetry:$false
```

Instalar a versão mais recente do EC2Launch

Use o seguinte procedimento para baixar e instalar a versão mais recente do EC2Launch em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Faça download do EC2-Windows-Launch.zip em um diretório na instância.
3. Faça download do install.ps1 no mesmo diretório onde você baixou o `EC2-Windows-Launch.zip`.
4. Executar `install.ps1`
5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para baixar e instalar a versão mais recente do EC2Launch usando o PowerShell

Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para instalar a versão mais recente do EC2Launch usando o PowerShell, execute os seguintes comandos em uma janela do PowerShell

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
```

```
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifique a instalação conferindo `C:\ProgramData\Amazon\EC2-Windows\Launch`.

Verificar a versão do EC2Launch

Use o comando do Windows PowerShell a seguir para verificar a versão instalada do EC2Launch.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

Estrutura de diretório do EC2Launch

Por padrão, o EC2Launch é instalado nas AMIs do Windows Server 2016 e posterior no diretório raiz `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e arquivos do EC2Launch, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório `Launch` contém os seguintes subdiretórios.

- `Scripts` — contém os scripts do PowerShell que compõem o EC2Launch.
- `Module` — contém o módulo para compilação dos scripts relacionados ao Amazon EC2.
- `Config` — contém arquivos script de configuração que é possível personalizar.
- `Sysprep` — contém recursos de Sysprep.
- `Settings`: contém uma aplicação para a interface gráfica do usuário do Sysprep.
- `Library` – Contém bibliotecas compartilhadas para agentes de inicialização do EC2.
- `Logs` — Contém arquivos de log gerados por scripts.

EC2Launch versão **`1.3.2004592`** e posterior

Os usuários do grupo `Administrators` têm permissões `Full control` para todos os diretórios do EC2Launch. Os usuários que não estiverem no grupo Administradores terão permissões `Read & execute` para todos os diretórios do EC2Launch, exceto `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Config`. O diretório `Config` é restrito aos usuários que forem membros do grupo `Administrators`.

EC2Launch versão **`1.3.2004491`** e anterior

Todos os diretórios do EC2Launch herdam suas permissões de `C:\ProgramData`, com exceção de `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Scripts`. Ao ser criada, essa pasta herda todas as permissões iniciais de `C:\ProgramData`, mas remove o acesso a `CreateFiles` para usuários normais no diretório.

Configurar o EC2Launch

Quando a instância tiver sido inicializada pela primeira vez, é possível configurar o EC2Launch para iniciar novamente e executar diferentes tarefas de startup.

Tarefas

- Configurar as tarefas de inicialização
- Programar o EC2Launch para ser executado em cada inicialização
- Inicializar unidades e mapear as letras de unidades
- Enviar logs de eventos do Windows ao console do EC2
- Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida

Configurar as tarefas de inicialização

Especifique as configurações no arquivo `LaunchConfig.json` para ativar ou desativar as seguintes tarefas de inicialização:

- Defina o nome do computador para o endereço IPv4 privado da instância.
- Defina o monitor para ficar sempre ligado.
- Configurar novo papel de parede.
- Adicionar a lista de sufixos DNS.

> **Note**
>
> Isso adiciona uma pesquisa de sufixo DNS para o domínio apresentado a seguir e configura outros sufixos padrão. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configuração do sufixo DNS para agentes de inicialização do Windows.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Estender o tamanho do volume de inicialização.
- Defina a senha de administrador.

Para definir as configurações de inicialização

1. Na instância a ser configurada, abra o seguinte arquivo em um editor de texto: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Atualize as seguintes configurações conforme necessário e salve suas alterações. Forneça uma senha em `adminPassword` somente se `adminPasswordtype` for `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
```

```
}
```

Os tipos de senha são definidos da seguinte maneira:

`Random`

O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

`Specify`

O EC2Launch usa a senha que você especifica `adminPassword`. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

`DoNothing`

O EC2Launch usa a senha que você especifica o arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.

3. No Windows PowerShell, execute o seguinte comando para programar a execução do script como uma tarefa agendada do Windows. O script é executado uma vez durante a próxima inicialização e desativa essas tarefas para que não sejam executadas novamente.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Programar o EC2Launch para ser executado em cada inicialização

É possível programar o EC2Launch para ser executado em cada inicialização e não apenas na inicialização inicial.

Para programar o EC2Launch para ser executado em cada inicialização:

1. Abra o Windows PowerShell e execute o seguinte comando:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Ou execute o executável com o seguinte comando:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Em seguida, selecione `Run EC2Launch on every boot`. É possível especificar que sua instância do EC2 seja `Shutdown without Sysprep` ou `Shutdown with Sysprep`.

> **Note**
>
> Quando você habilita o EC2Launch para ser executado em cada inicialização, acontecerá o seguinte na próxima vez que o EC2Launch for executado:
>
> - Se o `AdminPasswordType` ainda estiver definido como `Random`, o EC2Launch gerará uma nova senha na próxima inicialização. Após a reinicialização, o `AdminPasswordType` é automaticamente definido como `DoNothing`para impedir que o EC2Launch gere novas senhas em inicializações subsequentes. Para evitar que o EC2Launch gere uma nova senha na primeira inicialização, defina manualmente o `AdminPasswordType` como `DoNothing` antes de reiniciar.
> - `HandleUserData` será redefinido como `false` a menos que os dados do usuário tenham `persist` definido como `true`. Para ter mais informações, consulte the section called “Scripts de dados do usuário”.

Inicializar unidades e mapear as letras de unidades

Especifique as configurações no arquivo `DriveLetterMappingConfig.json` para mapear letras de unidades para volumes na instância do EC2. O script inicializa drives que ainda não foram inicializados e particionados. Para obter mais informações sobre como obter detalhes do volume no Windows, consulte Get-Volume na documentação da Microsoft.

Para mapear letras de unidade a volumes

1. Abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` em um editor de textos.
2. Especifique as seguintes configurações de volume e salve suas alterações:

```
{
 "driveLetterMapping": [
```

```
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch que inicializa os discos:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador `-Schedule` da seguinte forma:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Enviar logs de eventos do Windows ao console do EC2

Especifique configurações no arquivo `EventLogConfig.json` para enviar logs de eventos do Windows aos logs do console do EC2.

Para definir as configurações para enviar logs de eventos do Windows

1. Na instância, abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` em um editor de texto.
2. Configure as seguintes configurações de log e salve suas alterações:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. No Windows PowerShell, execute o seguinte comando para que o sistema agende o script para execução como uma tarefa agendada do Windows sempre que a instância for inicializada.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -
Schedule
```

   Os logs podem demorar três minutos ou mais para aparecerem no console do EC2.

Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida

O serviço de EC2Config envia a mensagem “O Windows está pronto” ao console do EC2 após cada inicialização. O EC2Launch envia essa mensagem somente após a primeira inicialização. Para compatibilidade com versões anteriores do serviço de EC2Config, é possível agendar o EC2Launch para enviar essa mensagem após cada inicialização. Na instância, abra o Windows PowerShell e execute o seguinte comando. O sistema agenda o script para ser executado como uma tarefa agendada do Windows.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -
Schedule
```

Histórico de versões do EC2Launch

As AMIs do Windows que são inicializadas com o Windows Server 2016 incluem um conjunto de scripts Windows Powershell chamados EC2Launch. O EC2Launch executa tarefas durante a inicialização inicial da instância. Para obter informações sobre as versões do EC2Launch incluídas nas AMIs do Windows na AWS, consulte AWS Windows AMI version history.

Para fazer download e instalar a versão mais recente do EC2Launch, consulte Instalar a versão mais recente do EC2Launch.

A tabela a seguir descreve as versões liberadas do EC2Launch. Observe que o formato da versão foi alterado após a versão 1.3.610.

Versão	Detalhes	Data de lançamento
1.3.2004891	• Corrigido um problema em que `HandleUserData` não estava definido como `false` conforme o esperado.	31 de maio de 2024

Versão	Detalhes	Data de lançamento
	• Adicionou uma opção de senha `Encrypted` a `LaunchConfig.json`. • Comportamento de `Settings UI` alterado para criptografar a senha especificada pelo usuário por padrão. • Adicionado `SetAdminPasswordConfig.ps1` para converter a opção de senha `Specify` para a opção de senha `Encrypted` no arquivo de configuração do agente.	
1.3.2004617	• Correção de um erro ao definir o papel de parede.	15 de janeiro de 2024

Versão	Detalhes	Data de lançamento
1.3.2004592	• Atualizadas permissões de acesso definidas por install.ps1 para `%ProgramData%\Amazon\EC2-Windows\Launch` . • Restringido o acesso a pastas/arquivos do EC2Launch para leitura e execução somente para contas de usuário padrão. • Alterado o agente para parar de esperar que o serviço de metadados de instância (IMDS) inicialize se o IMDS não estiver habilitado para a instância. • Adicionado um tempo limite de cinco minutos ao ser aguardada a inicialização do IMDS. • Alterado o agente para gravar a telemetria no log do console da instância antes da mensagem `Windows is Ready`, em vez de depois. • Adicionado suporte a papéis de parede para vários novos tipos de instâncias. Para obter mais informações sobre as permissões de acesso e as permissões de conta de usuário dos diretórios do EC2Launch, consulte the section called “Estrutura de diretório do EC2Launch”.	2 de janeiro de 2024
1.3.2004491	• Adicionada telemetria para monitorar o uso da opção Especificar senha do administrador.	9 de novembro de 2023
1.3.2004462	• Adicionada uma descarga após cada gravação no console de série.	18 de outubro de 2023

Versão	Detalhes	Data de lançamento
1.3.2004438	• Limitação da devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Limitação das permissões `UserdataExecution.log` apenas para `Administrators` . • Mensagens de erro adicionadas no log de eventos do Windows quando ocorre falha na inicialização.	4 de outubro de 2023
1.3.2004256	• Valor `EnableSCSIPersistentReservations` adicionado ao log do console. • Adição da capacidade de realização de novas tentativas a Get-ConsolePort.	7 de julho de 2023
1.3.2004052	• Corrigido um erro que ocorria quando nenhuma chave SSH era especificada na inicialização da instância. • Atualizado para tentar iniciar novamente o serviço AmazonSSMAgent Windows em caso de falha. • Atualizado para falhar SysprepInstance.ps1 se BeforeSysprep.cmd falhar com um código de saída diferente de zero.	8 de março de 2023
1.3.2003975	• Foi corrigido o problema que afetava as compilações do Packer AMI, em que `SysprepInstance.ps1` retorna um `$LastErrorCode` de 1.	24 de dezembro de 2022

Versão	Detalhes	Data de lançamento
1.3.2003961	• Foi corrigido um problema em que senhas de administrador especificadas explicitamente eram substituídas por uma senha aleatória em instâncias de inicialização rápida. • Foi corrigido um problema em que o SSM Agent apresentava falha ao iniciar em tipos de instância menores. • Foi corrigido um problema em que o log do console da instância continha `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000` em vez de um valor de impressão digital válido do certificado RDP.	6 de dezembro de 2022
1.3.2003923	• Corrige a lógica para encontrar o adaptador de rede quando o PnPDeviceID está vazio.	9 de novembro de 2022
1.3.2003919	• Atualizado Get-ConsolePort para usar as informações do segmento PCI. • Corrigido um problema que permite selecionar um adaptador de rede incorreto após a reinicialização. • Corrigida a lógica de tempo limite do Start-SSM-Agent. • Corrigida a compatibilidade com versões anteriores do alias da função Send-AdminCredentials.	8 de novembro de 2022
1.3.2003857	• Prioriza adaptadores com um gateway padrão quando o adaptador da rede primária é selecionado. • Criptografia de senha na memória estendida.	3 de outubro de 2022

Versão	Detalhes	Data de lançamento
1.3.2003824	• Foi corrigido o erro durante `setComputerName` . • Foi adicionada a lógica para ignorar a ativação do Windows quando um código de faturamento BYOL for detectado. • Foi adicionada criptografia de senha na memória. • Foi corrigido o erro durante a inicialização do volume em `m6id.4xlarge` .	30 de agosto de 2022
1.3.2003691	• Atualizada a lógica de espera IMDS para fazer somente solicitações IMDSv2. • Correção de bug que afeta a instalação da eGPU.	21 de junho de 2022
1.3.2003639	• Adicionada a lógica de espera do adaptador de rede para impedir o uso antes da inicialização. • Problemas secundários corrigidos.	10 de maio de 2022
1.3.2003498	• Telemetria adicionada. • Atalho adicionado à UI de Configurações. • Scripts PowerShell formatados. • Corrigido o problema de desligamento antes da conclusão do Beforesysprep.cmd.	31 de janeiro de 2022
1.3.2003411	Alterou-se a lógica de geração de senha para excluir senhas com baixa complexidade.	4 de agosto de 2021
1.3.2003364	Install-EGPumanager atualizado com suporte a IMDSv2.	7 de junho de 2021

Versão	Detalhes	Data de lançamento
1.3.2003312	• Linhas de log adicionadas antes e depois da configuração de `setMonitorAlwaysOn` . • Incluída a versão do pacote do AWS Nitro Enclaves no log do console.	04 de maio de 2021
1.3.2003284	Modelo de permissão aprimorado com atualização do local para armazenar dados do usuário em `LocalAppData` .	23 de março de 2021
1.3.2003236	• Método atualizado para definir a senha do usuário em `Set-AdminAccount` e `Randomize-LocalAdminPassword` . • `InitializeDisks` fixos para verificar se o disco está definido como somente leitura antes de configurá-lo para gravável.	11 de fevereiro de 2021
1.3.2003210	Correção de localização para `install.ps1` .	7 de janeiro de 2021
1.3.2003205	Correção de segurança do `install.ps1` para atualizar permissões no diretório `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 de dezembro de 2020
1.3.2003189	Adição do `w32tm resync` depois de adicionar rotas.	4 de dezembro de 2020
1.3.2003155	Informações de tipo de instância atualizadas.	25 de agosto de 2020
1.3.2003150	`OsCurrentBuild` e `OsReleaseId` adicionados à saída do console.	22 de abril de 2020
1.3.2003040	Lógica de fallback de versão 1 IMDS corrigida.	7 de abril de 2020

Versão	Detalhes	Data de lançamento
1.3.2002730	Suporte adicionado para IMDS V2.	3 de março de 2020
1.3.2002240	Problemas secundários corrigidos.	31 de outubro de 2019
1.3.2001660	Corrigido o problema de login automático para usuários sem a senha depois da primeira execução do Sysprep.	2 de julho de 2019
1.3.2001360	Problemas secundários corrigidos.	27 de março de 2019
1.3.2001220	Todos os scripts do PowerShell assinados.	28 de fevereiro de 2019
1.3.2001200	Corrigido o problema com InitializeDisks.ps1 em que a execução do script em um nó em um Cluster de Failover do Windows Server formaria unidades em nós remotos cuja letra da unidade correspondesse à letra da unidade local.	27 de fevereiro de 2019
1.3.2001160	Corrigido o papel de parede ausente no Windows 2019.	22 de fevereiro de 2019
1.3.2001040	• Plugin adicionado para configurar o monitor para nunca desligar para corrigir problemas de ACPI. • Edição e versão do SQL Server gravadas no console.	21 de janeiro de 2019
1.3.2000930	Correção para adição de rotas a metadados em ENIs habilitadas para IPv6.	2 de janeiro de 2019
1.3.2000760	• Configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA adicionadas • Hibernação desabilitada durante Sysprep.	5 de dezembro de 2018

Versão	Detalhes	Data de lançamento
1.3.2000630	• Adição da rota 169.254.169.253/32 para servidor DNS. • Adicionado filtro de configuração de usuário administrador. • Melhorias feitas na hibernação de instâncias. • Adicionada opção para programar o EC2Launch para ser executado em cada inicialização.	9 de novembro de 2018
1.3.2000430.0	• Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN. • Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID. • Adicionado tempo limite de 25 segundos ao tentar iniciar o Systems Manager.	19 de setembro de 2018
1.3.200039.0	• Corrigida a letra incorreta de unidade para volumes EBS NVME. • Adicionado log adicional para versões do driver NVME.	15 de agosto de 2018
1.3.2000080	Problemas secundários corrigidos.	
1.3.610	Problema corrigido com redirecionamento de saída e erros para os arquivos de dados do usuário.	
1.3.590	• Tipos de instâncias ausentes adicionadas ao papel de parede. • Problema corrigido com mapeamento de letra de unidade e instalação de disco.	
1.3.580	• `Get-Metadata` corrigido para usar as configurações do proxy do sistema padrão para solicitações da web. • Adicionou um argumento especial para NVMe na inicialização do disco. • Problemas secundários corrigidos.	

Versão	Detalhes	Data de lançamento
1.3.550	Adicionou uma opção `-NoShutdown` para ativar o Sysprep sem desligamento.	
1.3.540	Problemas secundários corrigidos.	
1.3.530	Problemas secundários corrigidos.	
1.3.521	Problemas secundários corrigidos.	
1.3.0	• Problema de tamanho de hexadecimal corrigido para alteração de nome do computador. • Possível loop de reinicialização corrigido para alteração de nome do computador. • Problema de configuração de papel de parede corrigido.	
1.2.0	• Atualização para exibir informações sobre o sistema operacional (SO) instalado no log do sistema do EC2. • Atualização para exibir a versão do EC2Launch e do SSM Agent no log do sistema do EC2. • Problemas secundários corrigidos.	

Versão	Detalhes	Data de lançamento
1.1.2	• Atualização para exibir informações do driver de ENA no log do sistema do EC2. • Atualização para excluir o Hyper-V da lógica primária do filtro NIC. • O servidor e a porta do AWS KMS foram adicionados à chave do registro para ativação do KMS. • Configuração de papel de parede aprimorada para vários usuários. • Atualização para limpar rotas no armazenamento persistente. • Atualização para remover o z da zona de disponibilidade na lista de sufixos DNS. • Atualização para resolver um problema com a tag <runAsLocalSystem> nos dados do usuário.	
1.1.1	Versão inicial.	

Configuração de uma instância do Windows usando o serviço EC2Config (herdado)

> **Note**
>
> A documentação do EC2Config é fornecida somente para referência histórica. As versões do sistema operacional em que ele é executado não têm mais suporte pela Microsoft. É altamente recomendável atualizar para o serviço de execução mais recente.
> O serviço de inicialização mais recente para todas o Windows Server 2022 é o EC2Launch v2, que substitui o EC2Config e o EC2Launch.

As AMIs do Windows para versões do Windows Server anteriores ao Windows Server 2016 incluem um serviço opcional: EC2Config (`EC2Config.exe`). O EC2Config é iniciado quando a instância inicia e executa tarefas durante o startup e sempre você iniciar ou para iniciar a instância. O EC2Config também executa tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. Embora opcional, esse serviço dá acesso a recursos avançados que não estariam disponíveis de outra forma. Esse serviço é executado na conta LocalSystem.

> **Note**
>
> O EC2Launch substituiu o EC2Config nas AMIs do Windows para o Windows Server 2016 e 2019. Para ter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch. O serviço de inicialização mais recente para todas as versões compatíveis do Windows Server é EC2Launch v2, que substitui o EC2Config e o EC2Launch.

O EC2Config usa arquivos de configurações para controlar sua operação. É possível atualizar esses arquivos de configurações usando uma ferramenta gráfica ou editando diretamente arquivos XML. Os arquivos binários de serviço e adicionais estão contidos no diretório `%ProgramFiles%\Amazon\EC2ConfigService`.

Tópicos

- Tarefas do EC2Config
- Instalar a versão mais recente do EC2Config
- Interromper, reiniciar, excluir ou desinstalar o EC2Config
- EC2Config e AWS Systems Manager
- EC2Config e Sysprep
- Propriedades do serviço do EC2
- Arquivos de configurações do EC2Config
- Configure as definições de proxy para o serviço do EC2Config
- Histórico de versões do EC2Config
- Solucionar problemas com o serviço do EC2Config

Tarefas do EC2Config

O EC2Config executa tarefas de startup iniciais quando a instância é iniciada pela primeira vez; depois, as desabilita. Para executar novamente essas tarefas, é necessário explicitamente habilitá-las antes de fechar a instância ou executar manualmente o Sysprep. Essas tarefas são as seguintes:

- Defina uma senha aleatória e criptografada para a conta do administrador.
- Gerencie e instale o certificado do host usado para abrir a Conexão de Desktop Remoto.
- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Execute os dados de usuário especificado (e Cloud-Init, se instalado). Para obter mais informações sobre como especificar os dados do usuário, consulte Trabalhar com dados do usuário da instância.

O EC2Config executa as tarefas a seguir sempre que a instância for iniciada:

- Altere o nome do host para corresponder ao endereço IP privado na notação Hex (essa tarefa está desabilitada por padrão e deverá ser ativada para execução no início da instância).
- Configure o servidor de gerenciamento de chaves (AWS KMS), verifique o status de ativação do Windows e ative o Windows, conforme necessário.
- Monte todos os volumes do Amazon EBS e volumes de armazenamento de instâncias e mapeie os nomes dos volumes para as letras de unidade.
- Grave entradas do log de eventos no console para ajudar a solucionar problemas (essa tarefa fica desabilitada por padrão e deve ser ativada para execução no início da instância).
- Escreva para o console que o Windows está pronto.
- Adicione uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando uma única NIC ou várias NICs estiverem conectadas: `169.254.169.250`, `169.254.169.251` e `169.254.169.254`. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.

> **Note**
>
> Se o sistema operacional Windows estiver configurado para usar IPv4, esses endereços locais de link IPv4 poderão ser usados. Se o sistema operacional Windows tiver a pilha de protocolos de rede IPv4 desabilitada e usar IPv6 em seu lugar, adicione

`[fd00:ec2::240]` em vez de `169.254.169.250` e `169.254.169.251`. Depois, adicione `[fd00:ec2::254]` em vez de `169.254.169.254`.

O EC2Config executa a tarefa a seguir sempre que um usuário faz login:

- Exibe informações do papel de parede do segundo plano do desktop.

Enquanto a instância estiver sendo executada, é possível solicitar que o EC2Config execute a seguinte tarefa sob demanda:

- Execute Sysprep e feche a instância, de modo que você possa criar as AMIs a partir dela. Para ter mais informações, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.

Instalar a versão mais recente do EC2Config

Por padrão, o serviço EC2Config está incluído em AMIs anteriores ao Windows Server 2016. Quando o serviço EC2Config for atualizado, as novas AMIs do Windows da AWS incluirão a versão mais recente do serviço. Contudo, você precisa atualizar suas próprias instâncias e AMIs do Windows com a versão mais recente do EC2Config.

> **Note**
>
> O EC2Launch substitui o EC2Config nas AMIs do Windows Server 2016 e 2019. Para ter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch. O serviço de inicialização mais recente para todas as versões compatíveis do Windows Server é EC2Launch v2, que substitui o EC2Config e o EC2Launch.

Para obter informações sobre como receber notificações para atualizações do EC2Config, consulte Assinar as notificações de serviço do EC2Config. Para obter informações sobre alterações em cada versão, consulte Histórico de versões do EC2Config.

Antes de começar

- Verifique que você tem .NET framework 3.5 SP1 ou posterior.
- Por padrão, a configuração substitui os arquivos de configuração durante a instalação e reinicia o serviço EC2Config quando a instalação é concluída. Se você tiver alterado as configurações

do serviço EC2Config, copie o arquivo `config.xml` do diretório `%Program Files%\Amazon \Ec2ConfigService\Settings`. Após atualizar o serviço EC2Config, será possível restaurar esse arquivo para reter as alterações nas configurações.

- Se a sua versão do EC2Config for anterior à versão 2.1.19 e você estiver instalando a versão 2.2.12 ou anterior, é necessário instalar a versão 2.1.19 primeiro. Para instalar a versão 2.1.19, faça download de EC2Install_2.1.19.zip, descompacte o arquivo e execute `EC2Install.exe`.

> **Note**
>
> Se a sua versão do EC2Config for anterior à versão 2.1.19 e você estiver instalando a versão 2.3.313 ou posterior, é possível instalá-la diretamente sem instalar a versão 2.1.19 primeiro.

Verificar a versão do EC2Config

Use o procedimento a seguir para verificar a versão do EC2Config que está instalada em suas instâncias.

Para verificar a versão instalada do EC2Config

1. Execute uma instância pela AMI e conecte-se a ela.
2. No Painel de Controle, selecione Programas e Recursos.
3. Na lista de programas instalados, procure `Ec2ConfigService`. O número da versão aparece na coluna Versão.

Atualizar o EC2Config

Use o seguinte procedimento para fazer download e instalar a versão mais recente do EC2Config em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Config

1. Faça download e descompacte o instalador do EC2Config.
2. Execute `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

> **Important**
>
> Para manter as configurações personalizadas do arquivo `config.xml` que você salvou, execute `EC2Install` com a opção `/norestart`, restaure as configurações e reinicie o serviço EC2Config manualmente.

3. Se você estiver executando o EC2Config versão 4.0 ou superior, reinicie o SSM Agent na instância do snap-in do Microsoft Services.

> **Note**
>
> As informações da versão atualizada do EC2Config não serão exibidas no log do sistema da instância ou na verificação do Trusted Advisor até que você reinicialize ou interrompa e inicie a instância.

Para baixar e instalar a versão mais recente do EC2Config usando o PowerShell

Para baixar, descompactar e instalar a versão mais recente do EC2Config usando o PowerShell, execute os seguintes comandos em uma janela do PowerShell:

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Verifique a instalação conferindo `C:\Program Files\Amazon\` para o diretório do `Ec2ConfigService`.

Interromper, reiniciar, excluir ou desinstalar o EC2Config

É possível gerenciar o serviço EC2Config da mesma forma como qualquer outro serviço.

Para aplicar as configurações atualizadas à sua instância, interrompa e reinicie o serviço. Se você estiver instalando manualmente o EC2Config, deverá primeiro interromper o serviço.

Para interromper o serviço EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e clique em Serviços.
3. Na lista de serviços, clique com o botão direito sobre EC2Config e selecione Parar.

Para reiniciar o serviço EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e clique em Serviços.
3. Na lista de serviços, clique com o botão direito sobre EC2Config e selecione Reiniciar.

Se você não precisar atualizar as configurações, ao criar sua própria AMI ou usar o AWS Systems Manager, poderá excluir e desinstalar de serviço. A exclusão de um serviço remove a subchave do registro. Desinstalar um serviço elimina os arquivos, a subchave do registro e todos os atalhos do serviço.

Para excluir o serviço EC2Config

1. Inicie uma janela do prompt de comando.
2. Execute o seguinte comando:

```
sc delete ec2config
```

Para desinstalar o EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, clique em Painel de Controle.
3. Clique duas vezes em Programas e Recursos.
4. Na lista de programas, selecione EC2ConfigService e clique em Desinstalar.

EC2Config e AWS Systems Manager

O serviço EC2Config processa solicitações de Systems Manager nas instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016 que foram publicadas antes de novembro de 2016.

Instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016, publicadas depois de novembro de 2016 incluem o serviço EC2Config e SSM Agent. O EC2Config executa todas as tarefas descritas anteriormente e o SSM Agent processa recursos do Systems Manager, como Run Command e o State Manager.

É possível usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço EC2Config e do SSM Agent. Para obter mais informações, consulte Atualizar o SSM Agent usando o Run Command no Manual do usuário do AWS Systems Manager.

EC2Config e Sysprep

O serviço EC2Config executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Config acessa o Sysprep, ela usa os arquivos em `%ProgramFiles%\Amazon\EC2ConfigService\Settings` para determinar quais operações devem ser executadas. É possível editar esses arquivos indiretamente usando a caixa de diálogo EC2 Service Properties (Propriedades do EC2 Service ou diretamente usando um editor de XML ou texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Propriedades do serviço Ec2; portanto, é necessário editar as entradas diretamente.

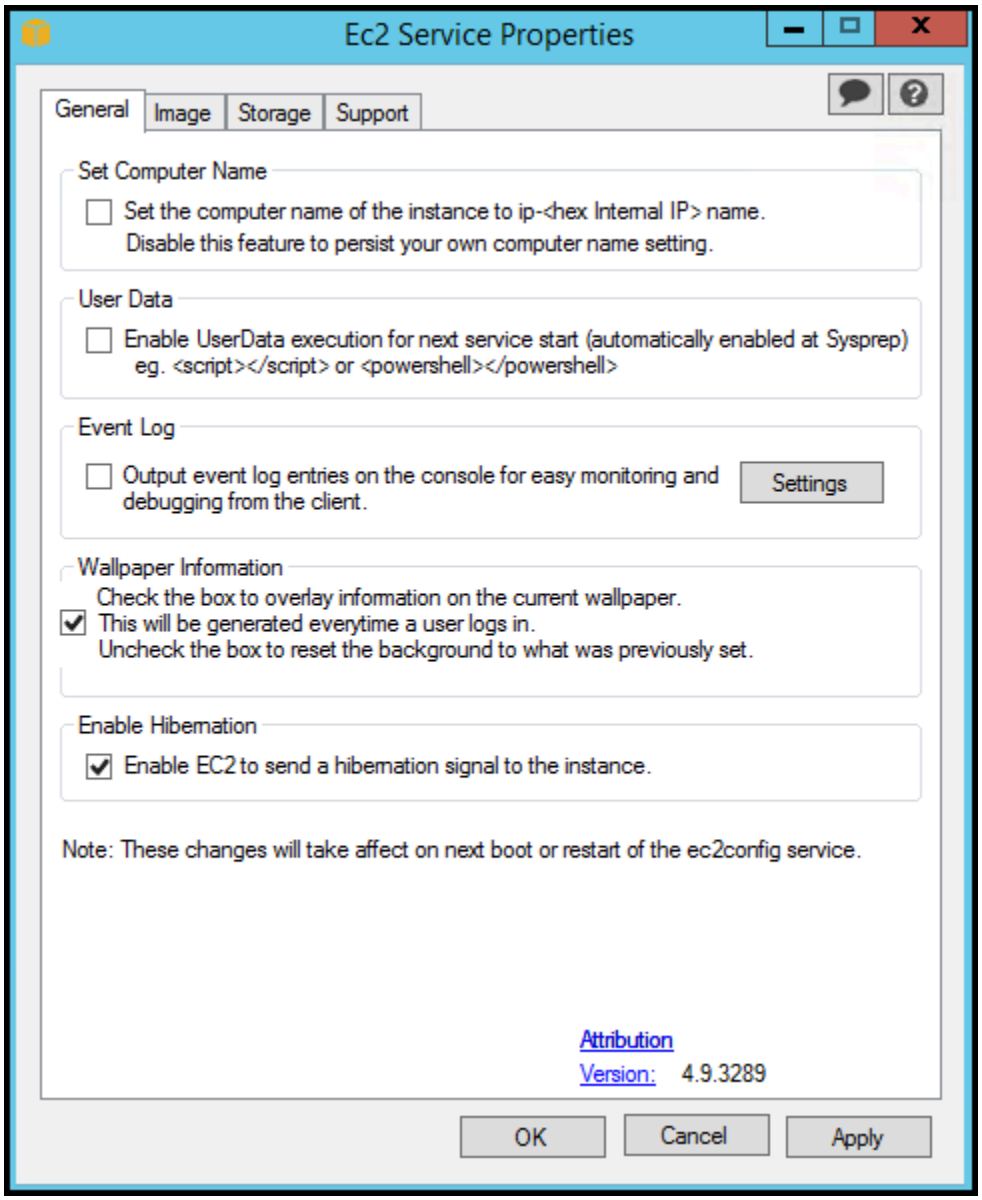
Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

Propriedades do serviço do EC2

O procedimento a seguir descreve como usar a caixa de diálogo Propriedades do serviço Ec2 para permitir ou desabilitar configurações.

Para alterar as configurações usando a caixa de diálogo Propriedades do serviço Ec2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, clique em Todos os programas e escolha Configurações do EC2ConfigService.



3. Na guia General (Geral) da caixa de diálogo EC2 Service Properties (Propriedades do EC2 Service), é possível habilitar ou desabilitar as configurações a seguir.

Definir o nome do computador

Se essa configuração estiver habilitada (está desabilitada por padrão), o nome do host será comparado ao endereço IP interno atual a cada inicialização; se o nome de host e o endereço IP interno não corresponderem, o nome do host será redefinido para conter o endereço IP interno, e o sistema reiniciará para pegar o novo nome de host. Ao configurar seu próprio nome de host ou para impedir a modificação de um nome de host existente, não habilite essa configuração.

Dados do usuário

A execução de dados do usuário permite especificar scripts nos metadados da instância. Por padrão, esses scripts são executados durante a execução inicial. Também é possível configurá-los para que sejam executados na próxima vez que você reiniciar ou iniciar a instância, ou sempre que fizer esse procedimento.

Se você tem um script grande, recomendamos usar dados do usuário para fazer download do script e, em seguida, executá-lo.

Para ter mais informações, consulte Execução de dados do usuário.

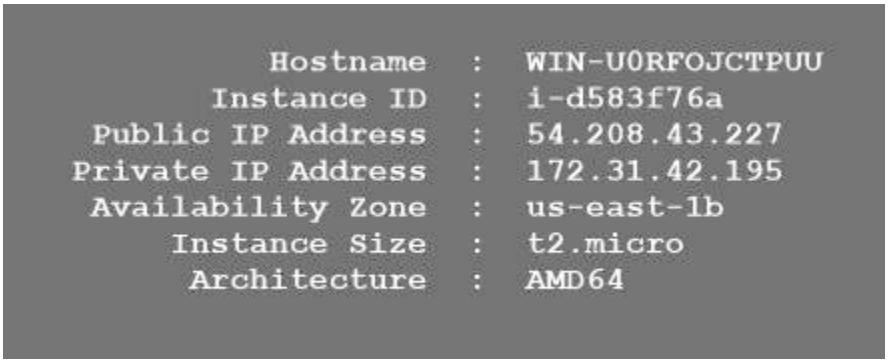
Log de eventos

Use essa configuração para exibir entradas de log de eventos no console durante a inicialização para facilitar o monitoramento e a depuração.

Clique em Configurações para especificar filtros para as entradas do log enviadas ao console. O filtro padrão enviar as três entradas de erros mais recentes do log de eventos do sistema ao console.

Informações sobre o papel de parede

Use essa configuração para exibir informações do sistema no segundo plano do desktop. A seguir está um exemplo das informações exibidas na tela de fundo do desktop.

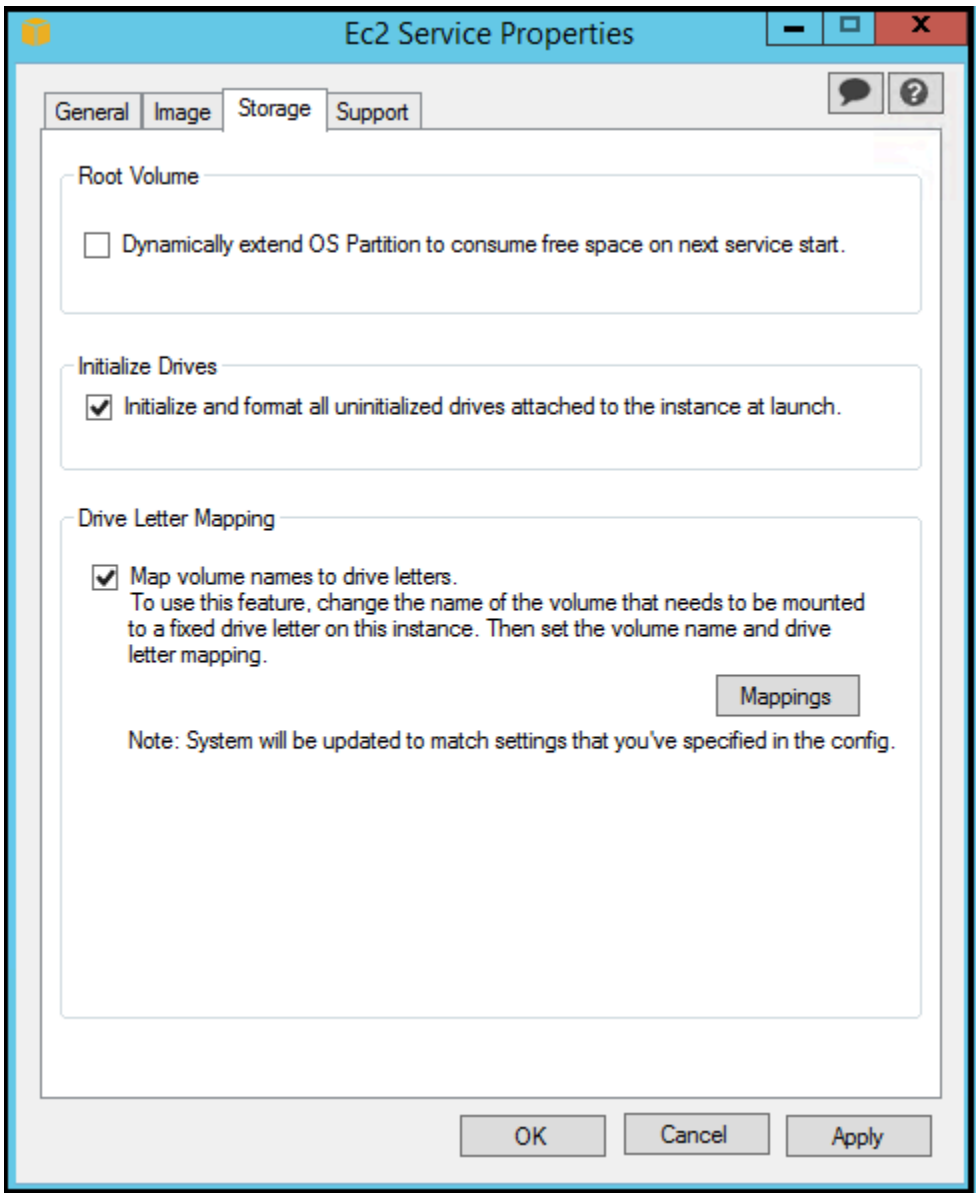


As informações exibidas em segundo plano no desktop são controladas pelo arquivo de configurações `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Habilitar a hibernação)

Use essa configuração para permitir que o EC2 sinalize ao sistema operacional para executar a hibernação.

4. Clique na guia Armazenamento. É possível habilitar ou desabilitar as configurações a seguir.



Volume do dispositivo raiz

Essa configuração amplia dinamicamente o Disco 0/Volume 0 para incluir qualquer espaço não particionado. Isso pode ser útil quando a instância for inicializada a partir de um volume do dispositivo raiz com tamanho personalizado.

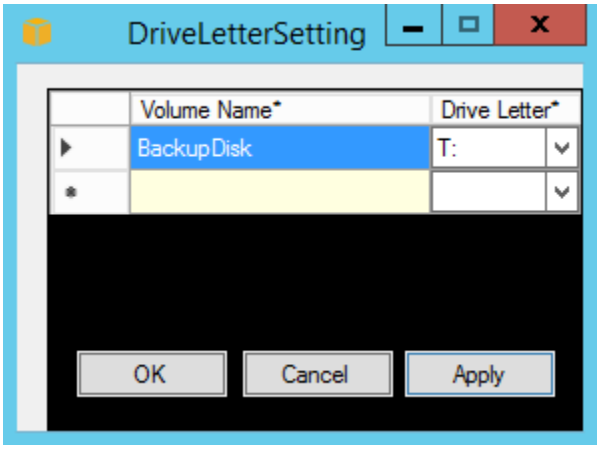
Inicializar unidades

Essa configuração formata e monta todos os volumes associados à instância durante a inicialização.

Mapeamento da letra da unidade

O sistema mapeia os volumes associados a uma instância para as letras de unidade. Para volumes do Amazon EBS, o padrão é atribuir letras de unidade que vão de D: a Z:. Para volumes de armazenamento de instâncias, o padrão depende do driver AWS. Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A: Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:.

Para selecionar as letras de unidade para seus volumes, clique em Mapeamentos. Na caixa de diálogo DriveLetterSetting, especifique os valores de Volume Name (Nome do volume) e Drive Letter (Letra da unidade) para cada volume e clique em Apply (Aplicar) e, em seguida, OK. Recomendamos que você selecione letras de unidade que evitem conflitos com as letras de unidade que provavelmente estão em uso, como as do meio do alfabeto.



Após especificar um mapeamento de letra de unidade e associar um volume com o mesmo rótulo que um dos nomes de volume especificado, o EC2Config atribui automaticamente sua letra especificada para esse volume. Contudo, o mapeamento da letra de unidade falhará se a letra já estiver em uso. Observe que EC2Config não altera as letras de unidade dos volumes já montados ao especificar o mapeamento da letra de unidade.

5. Para salvar suas configurações e continuar trabalhando nelas depois, clique em OK para fechar a caixa de diálogo EC2 Service Properties (Propriedades do EC2 Service). Se você tiver concluído a personalização da sua instância e quiser criar uma AMI com base nessa instância, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.

Arquivos de configurações do EC2Config

Os arquivos de configurações controlam a operação do serviço EC2Config. Esses arquivos estão localizados no diretório `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`—Controla a ativação do produto usando um servidor de gerenciamento de chaves (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`: controla quais contadores de performance enviar ao CloudWatch e quais logs enviar ao CloudWatch Logs.
- `BundleConfig.xml`—Controla como o EC2Config prepara uma instância com armazenamento de instâncias para criação da AMI.
- `Config.xml`—Controla as configurações primárias.
- `DriveLetterConfig.xml`—Controla os mapeamentos da letra de unidade.
- `EventLogConfig.xml`—Controla as informações do log de eventos exibidas no console enquanto a instância está inicializando.
- `WallpaperSettings.xml`—Controla as informações exibidas na tela de fundo do desktop.

ActivationSettings.xml

Esse arquivo contém as configurações que controlam a ativação do produto. Quando o Windows inicializa, o serviço EC2Config verifica se o Windows já está ativado. Se o Windows ainda não estiver ativado, ele tentará ativar o Windows procurando pelo servidor AWS KMS específico.

- `SetAutodiscover` indica se é necessário detectar um AWS KMS automaticamente.
- `TargetKMSServer` armazena o endereço IP privado de um AWS KMS. O AWS KMS deve estar na mesma região que a instância.
- `DiscoverFromZone` descobre o servidor AWS KMS da zona de DNS especificada.
- `ReadFromUserData` obtém o servidor AWS KMS de UserData.
- `LegacySearchZones` descobre o servidor AWS KMS da zona de DNS especificada.
- `DoActivate`—Tenta a ativação usando as configurações especificadas na seção. Esse valor pode ser `true` ou `false`.
- `LogResultToConsole`—Exibe o resultado para o console.

BundleConfig.xml

Este arquivo contém configurações que controlam como o EC2Config prepara uma instância para criação da AMI.

- `AutoSysprep`—Indica se o Sysprep deve ser usado automaticamente. Altere o valor para `Yes` para usar o Sysprep.
- `SetRDPCertificate`: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use RDP com segurança nas instâncias. Altere o valor para `Yes` se as novas instâncias precisarem ter o certificado.

  Essa configuração não é usada para instâncias com versões do sistema operacional anteriores ao Windows Server 2016, pois estas podem gerar seus próprios certificados.
- `SetPasswordAfterSysprep`—Define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor dessa configuração para No se as novas instâncias não forem definidas como uma senha criptografada aleatória.

Config.xml

Plugins

- `Ec2SetPassword`—Gera uma senha criptografada aleatória sempre que você executar uma instância. Esse recurso é desabilitado por padrão após a primeira execução, de forma que as reinicializações dessa instância não alterem uma senha definida pelo usuário. Altere essa configuração para `Enabled` para continuar a gerar senhas sempre que você executar uma instância.

  Essa configuração é importante se você estiver planejando criar um AMI a partir da sua instância.
- `Ec2SetComputerName`—Define o nome do host da instância para um nome exclusivo baseado no endereço IP da instância e reinicializa a instância. Ao configurar seu próprio nome de host ou impedir a modificação de um nome de host existente, é preciso desabilitar essa configuração.
- `Ec2InitializeDrives`—Inicializa e formata todos os volumes durante o startup. Esse recurso está habilitado por padrão.
- `Ec2EventLog`—Exibe entradas no log de eventos do console. Por padrão, são exibidas as três entradas de erro mais recentes do log de eventos do sistema. Para especificar as entradas no log de evento a serem exibidas, edite o arquivo `EventLogConfig.xml` localizado no diretório

`EC2ConfigService\Settings`. Para obter informações sobre as configurações nesse arquivo, consulte Eventlog Key na biblioteca do MSDN.

- `Ec2ConfigureRDP`—Define um certificado autoatribuído na instância, de forma que os usuários possam acessar com segurança a instância usando o Desktop Remoto. Essa configuração não é usada para instâncias com versões do sistema operacional anteriores ao Windows Server 2016, pois estas podem gerar seus próprios certificados.
- `Ec2OutputRDPCert`—Exibe informações do certificado de Desktop Remoto ao console, de forma que o usuário possa verificá-las contra o thumbprint.
- `Ec2SetDriveLetter`— Define as letras de unidade dos volumes montados com base em configurações definidas pelo usuário. Por padrão, quando um volume do Amazon EBS estiver associado a uma instância, ele poderá ser montado usando a letra de unidade na instância. Para especificar os mapeamentos da sua letra de unidade, edite o arquivo `DriveLetterConfig.xml` localizado no diretório `EC2ConfigService\Settings`.
- `Ec2WindowsActivate`— O plugin lida com ativação do Windows. Verifica para ver se o Windows está ativado. Caso contrário, atualiza as configurações do cliente AWS KMS e, então, ativa o Windows.

  Para modificar as configurações do AWS KMS, edite o arquivo `ActivationSettings.xml` localizado no diretório `EC2ConfigService\Settings`.
- `Ec2DynamicBootVolumeSize`—Estende o disco 0/Volume 0 para incluir qualquer espaço não particionado.
- `Ec2HandleUserData`—Cria e executa scripts criados pelo usuário na primeira execução de uma instância depois que o Sysprep for executado. Os comandos envolvidos nas tag do script são gravados no arquivo em lote, e os comandos envolvidos nas tags do PowerShell são gravados em um arquivo .ps1 (corresponde à caixa de seleção User Data [Dados do usuário] na caixa de diálogo Ec2 Service Properties [Propriedades do serviço Ec2]).
- `Ec2ElasticGpuSetup`—Instala o pacote de software para GPU elástica se a instância estiver associada a uma GPU elástica.
- `Ec2FeatureLogging`—Envia a instalação do recurso do Windows e o status do serviço correspondente ao console. Válido somente para o recurso Microsoft Hyper-V e o serviço vmms correspondente.

Configurações globais

- `ManageShutdown`—Assegura que as instâncias executadas pelas AMIs com armazenamento de instâncias não sejam encerradas ao executar Sysprep.
- `SetDnsSuffixList`—Define o sufixo DNS do adaptador de rede para Amazon EC2. Isso permite resolução do DNS dos servidores em execução no Amazon EC2 sem fornecer o nome de domínio totalmente qualificado.

  > **Note**
  >
  > Isso adiciona uma pesquisa de sufixo DNS para o domínio apresentado a seguir e configura outros sufixos padrão. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configuração do sufixo DNS para agentes de inicialização do Windows.
  >
  > ```
  > region.ec2-utilities.amazonaws.com
  > ```

- `WaitForMetaDataAvailable`—Assegura que o serviço EC2Config aguardará os metadados estarem acessíveis e redes estarem disponíveis antes de continuar com a inicialização. Essa verificação garante que o EC2Config possa obter informações dos metadados para ativação e outros plugins.
- `ShouldAddRoutes`—Adiciona uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando múltiplos NICs estiverem associados: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.
- `RemoveCredentialsfromSyspreponStartup`—Remove a senha do administrador de `Sysprep.xml` da próxima vez que o serviço iniciar. Para garantir que essa senha persista, edite essa configuração.

DriveLetterConfig.xml

Esse arquivo contém configurações que controlam os mapeamentos de letra da unidade. Por padrão, um volume pode ser mapeado para qualquer letra de unidade disponível. É possível montar um volume em uma letra de unidade específica, da seguinte forma.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
```

```
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName`—A etiqueta de volume. Por exemplo, *`My Volume`*. Para especificar um mapeamento para um volume de armazenamento de instâncias, use a etiqueta `Temporary Storage X`, onde `X` é um número de 0 a 25.
- `DriveLetter`—A letra de unidade. Por exemplo, *`M:`*. O mapeamento falhará se a letra de unidade já estiver em uso.

EventLogConfig.xml

Este arquivo contém configurações que controlam as informações do log de eventos exibidas no console enquanto a instância estiver sendo inicializada. Por padrão, exibimos as três entradas de erro mais recentes do log de eventos do sistema.

- `Category`—A chave de log do evento a ser monitorada.
- `ErrorType`—O tipo de evento (por exemplo, `Error`, `Warning`, `Information`.)
- `NumEntries`—O número de eventos armazenados para essa categoria.
- `LastMessageTime`—Para impedir que a mesma mensagem seja enviada repetidamente, o serviço atualizará esse valor sempre que enviar uma mensagem.
- `AppName`: a origem do evento ou a aplicação que o registrou.

WallpaperSettings.xml

Esse arquivo contém as configurações que controlam as informações exibidas na tela de fundo do desktop. As informações a seguir são exibidas por padrão.

- `Hostname`—Exibe o nome do computador.
- `Instance ID`—Exibe o ID da instância.
- `Public IP Address`—Exibe o endereço IP público da instância.
- `Private IP Address`—Exibe o endereço IP privado da instância.

- `Availability Zone`—Exibe a zona de disponibilidade na qual a instância está em execução.
- `Instance Size`—Exibe o tipo de instância.
- `Architecture`: exibe a configuração da variável de ambiente `PROCESSOR_ARCHITECTURE`.

É possível remover qualquer informação exibida por padrão ao excluir essa entrada. É possível adicionar metadados de instância adicionais para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

É possível adicionar variáveis do ambiente do sistema para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Esse arquivo contém as configurações que controlam como o EC2Config inicializa as unidades.

Por padrão, o EC2Config inicializa as unidades que não foram trazidas online com o sistema operacional. É possível personalizar o plugin conforme a seguir.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Use um grupo de configurações para especificar como deseja inicializar as unidades:

FormatWithTRIM

> Permite o comando TRIM ao formatar as unidades. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

A partir do EC2Config versão 3.18, o comando TRIM é desativado durante a operação de formatação do disco, por padrão. Isso aprimora o tempo de formatação. Use essa configuração para permitir a TRIM durante a operação de formatação do disco para o EC2Config versão 3.18 e posterior.

FormatWithoutTRIM

Desabilita o comando TRIM ao formatar as unidades e melhorar o tempo de formatação no Windows. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

DisableInitializeDrives

Desabilita a formatação de novas unidades. Use essa configuração para inicializar as unidades manualmente.

Configure as definições de proxy para o serviço do EC2Config

É possível configurar o serviço EC2Config para se comunicar por meio de um proxy usando um dos seguintes métodos: AWS SDK for .NET, o elemento `system.net` as políticas de grupo da Microsoft e o Internet Explorer. O uso do AWS SDK para .NET é o método preferido, pois é possível especificar credenciais de login.

Métodos

- Configurar definições de proxy usando a opção AWS SDK for .NET (Preferencial)
- Definir as configurações de proxy usando o elemento system.net
- Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer

Configurar definições de proxy usando a opção AWS SDK for .NET (Preferencial)

É possível configurar as configurações de proxy para o serviço EC2Config ao especificar o elemento `proxy` no arquivo `Ec2Config.exe.config`. Para obter mais informações, consulte Referência de arquivos de configuração do AWS SDK for .NET.

Para especificar o elemento de proxy em Ec2Config.exe.config

1. Edite o arquivo `Ec2Config.exe.config` em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório: `%ProgramFiles%\Amazon\Ec2ConfigService`.

2. Adicione o elemento `aws` a seguir para o `configSections`. Não adicione isso a nenhum `sectionGroups` existente.

   Para EC2Config versões 3.17 ou anteriores

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

   Para EC2Config versões 3.18 ou posteriores

   ```
   <configSections>
        <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
   </configSections>
   ```

3. Adicione o elemento `aws` a seguir ao arquivo `Ec2Config.exe.config`.

   ```
   <aws>
      <proxy
        host="string value"
        port="string value"
        username="string value"
        password="string value" />
   </aws>
   ```

4. Salve as alterações.

Definir as configurações de proxy usando o elemento system.net

É possível especificar as configurações de proxy em um elemento `system.net` no arquivo `Ec2Config.exe.config`. Para obter mais informações, consulte o elemento defaultProxy (configurações de rede) em MSDN.

Para especificar o elemento system.net em Ec2Config.exe.config

1. Edite o arquivo `Ec2Config.exe.config` em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Adicione uma entrada `defaultProxy` a `system.net`. Para obter mais informações, consulte o elemento defaultProxy (configurações de rede) em MSDN.

Por exemplo, a configuração a seguir roteia todo o tráfego para usar o proxy atualmente configurado para Internet Explorer, com exceção de metadados e tráfego de licenciamento, que contorneará o proxy.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
    <bypasslist>
        <add address="169.254.169.250" />
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Salve as alterações.

Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer

O serviço EC2Config é executado sob a conta do usuário do sistema local. É possível especificar configurações de proxy em toda a instância para essa conta no Internet Explorer depois de alterar as configurações de Política do Grupo na instância.

Para definir as configurações de proxy usando as políticas de grupo e o Internet Explorer

1. Em uma instância na qual você deseja que o serviço EC2Config se comunique por um proxy, abra um prompt de comando como administrador, digite **`gpedit.msc`** e pressione Enter.
2. No editor de políticas do grupo local, em Política do computador local, escolha Configuração do computador, Modelos administrativos, Componentes do Windows, Internet Explorer.
3. No painel à direita, escolha Definir as configurações de proxy por máquina (não por usuário) e, em seguida, Editar configuração da política.
4. Selecione Habilitado e, em seguida, selecione Aplicar.
5. Abra o Internet Explorer e selecione o botão Ferramentas.
6. Escolha Opção de Internet e escolha a guia Conexões.
7. Escolha Configurações da LAN.
8. Em Servidor proxy, escolha a opção Usar um Servidor Proxy para LAN.
9. Especifique as informações de endereço e porta e selecione OK.

Histórico de versões do EC2Config

As AMIs do Windows antes do Windows Server 2016 incluem um serviço opcional chamado serviço EC2Config (`EC2Config.exe`). O EC2Config é iniciado quando a instância inicia e executa tarefas durante o startup e sempre você iniciar ou para iniciar a instância.

É possível receber notificações quando novas versões do serviço EC2Config forem liberadas. Para ter mais informações, consulte Assinar as notificações de serviço do EC2Config.

A tabela a seguir descreve as versões liberadas do EC2Config. Para obter informações sobre as atualizações do SSM Agent, consulte Notas de release do Systems Manager SSM Agent.

Versão	Detalhes	Data de lançamento
4.9.5777	• Corrigido o problema em que a configuração de RSS era definida incorretamente para alguns tipos de instância. • Nova versão do SSM Agent `3.3.484.0` .	17 de junho de 2024
4.9.5554	• Limitação da devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nova versão do SSM Agent `3.2.1630.0` .	4 de outubro de 2023
4.9.5467	• Adicionado o recurso de repetição de tentativas para descobrir a porta do console. • Nova versão do SSM Agent `3.1.2282.0` .	1º de agosto de 2023
4.9.5288	• O AWS Core SDK foi atualizado para a versão `3.7.103.23` . •	8 de março de 2023

Versão	Detalhes	Data de lançamento
	Corrigido problema em que o documento SSM `AWS-UpdateEC2Config` falhava ao atualizar `EC2Config` em instâncias habilitadas somente com o IMDSv2. • Nova versão do SSM Agent `3.1.2144.0` .	
4.9.5231	• Nova versão do SSM Agent 3.1.1927.0.	14 de fevereiro de 2023
4.9.5103	• Corrigido um problema em que volumes efêmeros eram identificados incorretamente nas famílias de instâncias r5d e i4i. • Nova versão do SSM Agent 3.1.1856.0.	5 de dezembro de 2022
4.9.5064	• Atualizado para usar de informações do segmento PCI para selecionar a porta do console. • Assinados scripts do PowerShell e adicionados cabeçalhos de direitos autorais. • Corrigida a lógica da seleção do adaptador da rede primária. • Nova versão do SSM Agent 3.1.1732.0.	16 de novembro de 2022
4.9.4588	• Atualizada a lógica de espera IMDS para fazer somente solicitações IMDSv2. • Adicionada a biblioteca compartilhada do agente de inicialização libec2launch.dll. • Nova versão do SSM Agent 3.1.1188.0.	31 de maio de 2022

Versão	Detalhes	Data de lançamento
4.9.4556	• Adicionada lógica de espera para garantir a inicialização completa da NIC antes do uso. • A nova versão do Log4Net 2.0.14.0 inclui o patch de segurança. • A nova versão do SSM Agent 3.1.1045.0 inclui o patch de segurança.	1º de março de 2022
4.9.4536	• Corrigido um problema em que os dados do usuário falham quando a pasta Temp está ausente. • Nova versão do SSM Agent 3.1.804.0.	31 de janeiro de 2022
4.9.4508	• Correção do problema para calcular corretamente o caminho do script diskpart. • Nova versão do SSM Agent 3.1.338.0.	6 de outubro de 2021
4.9.4500	• `Install-EgpuManagerConfig` atualizado com suporte a IMDS v2. • Links atualizados para usar https. • Nova versão do SSM Agent 3.1.282.0	7 de setembro de 2021
4.9.4419	• Lógica de fallback de versão 1 IMDS corrigida. • Atualizado todo o uso do diretório temporário do Windows para o diretório temporário do EC2Config • Nova versão do SSM Agent 3.0.1124.0	2 de junho de 2021

Versão	Detalhes	Data de lançamento
4.9.4381	• Adicionado suporte para o esquema de documentos SSM versão 2.2 no EC2ConfigUpdater • Incluída a versão do pacote do AWS Nitro Enclaves no log do console • Nova versão do SSM Agent 3.0.529.0	4 de maio de 2021
4.9.4326	• Todos os links na interface do usuário de configurações foram removidos • Esta é a última versão do EC2Config que oferece suporte ao Windows Server 2008.	3 de março de 2021
4.9.4279	• Corrigido problema de segurança relacionado à tarefa `Ec2ConfigMonitor` agendada • Corrigido problema de mapeamento de letras de unidade fixa e contagem de disco temporário incorreta • Adicionados`OsCurrentBuild` e `OsReleaseId` à saída do console. • Nova versão do SSM Agent 2.3.871.0	11 de dezembro de 2020
4.9.4222	• Lógica de fallback de versão 1 IMDS corrigida. • Nova versão do SSM Agent 2.3.842.0	7 de abril de 2020
4.9.4122	• Suporte adicionado para IMDS v2 • Nova versão do SSM Agent 2.3.814.0	4 de março de 2020
4.9.3865	• Correção de um problema que detecta a porta COM para Windows Server 2008 R2 em instâncias metal • Nova versão do SSM Agent 2.3.722.0	31 de outubro de 2019
4.9.3519	• Nova versão do SSM Agent 2.3.634.0	18 de junho de 2019

Versão	Detalhes	Data de lançamento
4.9.3429	• Nova versão do SSM Agent 2.3.542.0	25 de abril de 2019
4.9.3289	• Nova versão do SSM Agent 2.3.444.0	11 de fevereiro de 2019
4.9.3270	• Plugin adicionado a fim de configurar o monitor para nunca desligar ao corrigir problemas de ACPI • Edição e versão do SQL Server gravadas no console • Nova versão do SSM Agent 2.3.415.0	22 de janeiro de 2019
4.9.3230	• A descrição do Mapeamento da letra da unidade foi atualizad a para se alinhar melhor à funcionalidade. • Nova versão do SSM Agent 2.3.372.0	10 de janeiro de 2019
4.9.3160	• Aumentado o tempo de espera para NIC primário • Adição de configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA • Hibernação desabilitada durante Sysprep • Nova versão do SSM Agent 2.3.344.0 • AWS SDK atualizado para 3.3.29.13	15 de dezembro de 2018
4.9.3067	• Melhorias feitas na hibernação de instâncias • Nova versão do SSM Agent 2.3.235.0	8 de novembro de 2018
4.9.3034	• Adição da rota 169.254.169.253/32 para servidor DNS • Nova versão do SSM Agent 2.3.193.0	24 de outubro de 2018
4.9.2986	• Adição de assinatura para todos os binários relacionados ao EC2Config • Nova versão do SSM Agent 2.3.136.0	11 de outubro de 2018

Versão	Detalhes	Data de lançamento
4.9.2953	Nova versão do SSM Agent (2.3.117.0)	2 de outubro de 2018
4.9.2926	Nova versão do SSM Agent (2.3.68.0)	18 de setembro de 2018
4.9.2905	• Nova versão do SSM Agent (2.3.50.0) • Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN • Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID • Corrigido um problema que fazia com que os volumes do EBS NVMe fossem marcados como efêmeros	17 de setembro de 2018
4.9.2854	Nova versão do SSM Agent (2.3.13.0)	17 de agosto de 2018
4.9.2831	Nova versão do SSM Agent (2.2.916.0)	7 de agosto de 2018
4.9.2818	Nova versão do SSM Agent (2.2.902.0)	31 de julho de 2018
4.9.2756	Nova versão do SSM Agent (2.2.800.0)	27 de junho de 2018
4.9.2688	Nova versão do SSM Agent (2.2.607.0)	25 de maio de 2018
4.9.2660	Nova versão do SSM Agent (2.2.546.0)	11 de maio de 2018
4.9.2644	Nova versão do SSM Agent (2.2.493.0)	26 de abril de 2018

Versão	Detalhes	Data de lançamento
4.9.2586	Nova versão do SSM Agent (2.2.392.0)	28 de março de 2018
4.9.2565	• Nova versão do SSM Agent (2.2.355.0) • Foi corrigido um problema nas instâncias M5 e C5 (não conseguem encontrar os drivers PV) • Adicionado o registro em log no console para tipo de instância , drivers PV mais recentes e drivers NVMe	13 de março de 2018
4.9.2549	Nova versão do SSM Agent (2.2.325.0)	8 de março de 2018
4.9.2461	Nova versão do SSM Agent (2.2.257.0)	15 de fevereiro de 2018
4.9.2439	Nova versão do SSM Agent (2.2.191.0)	6 de fevereiro de 2018
4.9.2400	Nova versão do SSM Agent (2.2.160.0)	16 de janeiro de 2018
4.9.2327	• Nova versão do SSM Agent (2.2.120.0) • Descoberta de porta COM adicionada em instâncias bare metal do Amazon EC2 • Registro em log de status Hyper-V adicionado em instâncias bare metal do Amazon EC2	2 de janeiro de 2018
4.9.2294	Nova versão do SSM Agent (2.2.103.0)	4 de dezembro de 2017

Versão	Detalhes	Data de lançamento
4.9.2262	Nova versão do SSM Agent (2.2.93.0)	15 de novembro de 2017
4.9.2246	Nova versão do SSM Agent (2.2.82.0)	11 de novembro de 2017
4.9.2218	Nova versão do SSM Agent (2.2.64.0)	29 de outubro de 2017
4.9.2212	Nova versão do SSM Agent (2.2.58.0)	23 de outubro de 2017
4.9.2203	Nova versão do SSM Agent (2.2.45.0)	19 de outubro de 2017
4.9.2188	Nova versão do SSM Agent (2.2.30.0)	10 de outubro de 2017
4.9.2180	• Nova versão do SSM Agent (2.2.24.0) • Plugin de GPU elástica adicionado a instâncias de GPU	5 de outubro de 2017
4.9.2143	Nova versão do SSM Agent (2.2.16.0)	1º de outubro de 2017
4.9.2140	Nova versão do SSM Agent (2.1.10.0)	
4.9.2130	Nova versão do SSM Agent (2.1.4.0)	
4.9.2106	Nova versão do SSM Agent (2.0.952.0)	
4.9.2061	Nova versão do SSM Agent (2.0.922.0)	
4.9.2047	Nova versão do SSM Agent (2.0.913.0)	

Versão	Detalhes	Data de lançamento
4.9.2031	Nova versão do SSM Agent (2.0.902.0)	
4.9.2016	• Nova versão do SSM Agent (2.0.879.0) • Caminho do diretório do CloudWatch Logs corrigido para o Windows Server 2003	
4.9.1981	• Nova versão do SSM Agent (2.0.847.0) • Corrigido o problema com `important.txt` sendo gerado em volumes do EBS.	
4.9.1964	Nova versão do SSM Agent (2.0.842.0)	
4.9.1951	• Nova versão do SSM Agent (2.0.834.0) • Corrigido o problema com letra de unidade não mapeada de Z: para discos temporários.	
4.9.1925	• Nova versão do SSM Agent (2.0.822.0) • [Bug] Essa versão não é um destino de atualização válido do SSM Agent v4.9.1775.	
4.9.1900	Nova versão do SSM Agent (2.0.805.0)	
4.9.1876	• Nova versão do SSM Agent (2.0.796.0) • Corrigido um problema com redirecionamento de saída/erro para execução de userdata do administrador.	

Versão	Detalhes	Data de lançamento
4.9.1863	• Nova versão do SSM Agent (2.0.790.0) • Corrigidos problemas com a conexão de vários volumes do EBS a uma instância do Amazon EC2. • Melhorado o CloudWatch para pegar um caminho de configuração, mantendo a retrocompatibilidade.	
4.9.1791	Nova versão do SSM Agent (2.0.767.0)	
4.9.1775	Nova versão do SSM Agent (2.0.761.0)	
4.9.1752	Nova versão do SSM Agent (2.0.755.0)	
4.9.1711	Nova versão do SSM Agent (2.0.730.0)	
4.8.1676	Nova versão do SSM Agent (2.0.716.0)	
4.7.1631	Nova versão do SSM Agent (2.0.682.0)	
4.6.1579	• Nova versão do SSM Agent (2.0.672.0) • Corrigido problema de atualização do agente com v4.3, v4.4 e v4.5	
4.5.1534	Nova versão do SSM Agent (2.0.645.1)	
4.4.1503	Nova versão do SSM Agent (2.0.633.0)	
4.3.1472	Nova versão do SSM Agent (2.0.617.1)	
4.2.1442	Nova versão do SSM Agent (2.0.599.0)	
4.1.1378	Nova versão do SSM Agent (2.0.558.0)	

Versão	Detalhes	Data de lançamento
4.0.1343	• O Run Command, o State Manager, o agente do CloudWatch e o suporte à união de domínios foram transferidos para outro agente, chamado SSM Agent. O SSM Agent será instalado como parte do upgrade do EC2Config. Para ter mais informações, consulte EC2Config e AWS Systems Manager. • Se você tiver um proxy configurado no EC2Config, precisará atualizar suas configurações de proxy para o SSM Agent antes de fazer o upgrade. Se você não atualizar as configurações do proxy, não poderá usar o comando Executar para gerenciar suas instâncias. Para evitar isso, consulte as informações a seguir antes de atualizar para a versão mais recente: Instalação e configuração do SSM Agent em instâncias do Windows no Guia do usuário do AWS Systems Manager. • Se você tiver previamente habilitado a integração com o CloudWatch nas suas instâncias usando um arquivo de configuração local (`AWS.EC2.Windows.CloudWatch.json`), precisará configurar o arquivo para trabalhar com o SSM Agent.	
3.19.1153	• Reativado o plugin de ativação para instâncias com a configuração antiga do AWS KMS. Ignore a ativação para usuários BYOL. • Altere o comportamento padrão do TRIM para estar desabilitado durante a operação de formatação do disco e adicione FormatWithTRIM para sobrescrever o plugin InitializeDisks com userdata.	

Versão	Detalhes	Data de lançamento
3.18.1118	• Correção para adicionar rotas com confiança ao adaptador de rede primário. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.17.1032	• As correções duplicam os logs do sistema que aparecem quando os filtros são colocados na mesma categoria. • Correções para evitar suspensão durante a inicialização do disco.	
3.16.930	Adicionado suporte ao evento no log "A janela está pronta para usar" ao log do evento no Windows no início.	
3.15.880	Correção para permitir upload da saída do Systems Manager Run Command para nomes do bucket S3 com o caractere ".".	
3.14.786	Adicionado suporte para sobrescrever as configurações de plugin de InitializeDisks. Por exemplo: Para acelerar a inicializ ação do disco SSD, é possível temporariamente desabilitar o TRIM ao especificar o seguinte em userdata: <InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings	
3.13.727	Systems Manager Run Command – Correções dos comandos do processo com confiança após reinicialização do Windows.	

Versão	Detalhes	Data de lançamento
3.12.649	• Correção para lidar tranquilamente com a reinicialização ao executar comandos/scripts. • Correção para cancelar com confiança os comandos de execução. • Adicione suporte para carregar (opcionalmente) logs de MSI no S3 ao instalar aplicações via Systems Manager Run Command.	
3.11.521	• Correções para permitir a geração de thumbprint de RDP para Windows Server 2003. • Correções para incluir o fuso horário e a compensação do UTC nas linhas de log do EC2Config. • Suporte a Systems Manager para executar comandos do Run Command em paralelo. • Retornar à alteração anterior para colocar discos particion ados online.	
3.10.442	• Corrigir falhas de configuração do Systems Manager ao instalar aplicações MSI. • Correção para colocar discos de armazenamento online com confiança. • Atualizações para melhorar o suporte aos serviços da AWS.	

Versão	Detalhes	Data de lançamento
3.9.359	• Correção no script pós-Sysprep para deixar a configuração do Windows atualizar em um estado padrão. • Correção do plugin de geração de senha para melhorar a confiabilidade ao obter as configurações da política de senha do GPO. • Restrição às permissões da pasta do log de EC2Config/SSM ao grupo Administradores local. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.8.294	• Corrigido um problema com o CloudWatch que impedia os logs de serem atualizados quando não estivessem na unidade primária. • Melhorado o processo de inicialização de disco ao adicionar a lógica de repetição. • Adicionada manipulação de erro melhorada quando o plugin SetPassword falhava ocasionalmente durante a criação de AMI. • Atualizações para melhorar o suporte aos serviços da AWS.	

Versão	Detalhes	Data de lançamento
3.7.308	• Melhorias ao utilitário ec2config-cli para testes de config e a solução de problemas na instância. • Evite adicionar rotas estáticas ao serviço de metadados do AWS KMS em um adaptador OpenVPN. • Corrigido um problema no qual a execução de dados do usuário não estava honrando a tag "persist". • A manipulação de erro melhorada ao fazer login no console do EC2 não está disponível. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.6.269	• Correção de confiabilidade da ativação do Windows para usar primeiro o endereço local do link 169.254.0.250/251 para ativar o Windows via AWS KMS • Manuseio do proxy aprimorado para cenários de Systems Manager, Windows Activation e Domain Join • Corrigido um problema em que linhas duplicadas de contas de usuário eram adicionadas ao arquivo de resposta do Sysprep	
3.5.228	• Resolvido um cenário em que o plugin do CloudWatch poderia consumir em excesso CPU e memória ao ler os logs de evento do Windows • Adicionado um link para a documentação de configuração do CloudWatch na UI de configurações do EC2Config	

Versão	Detalhes	Data de lançamento
3.4.212	• Correções do EC2Config quando usadas em combinação com o VM Import. • Corrigido o problema de nomeação do serviço no instalador do WiX.	
3.3.174	• Melhorada a manipulação de exceção para Systems Manager e falhas de junção de domínio. • Alteração para dar suporte ao versionamento do esquema do Systems Manager SSM. • Corrigida a formação de discos temporários em Win2K3. • Alteração para suporte do tamanho do disco de configuração maior que 2TB. • Uso reduzido de memória virtual ao definir o modo GC para padrão. • Suporte para baixar artefatos do caminho UNC nos plugins `aws:psModule` e `aws:application` . • Melhora no registro em log do plugin de ativação do Windows.	

Versão	Detalhes	Data de lançamento
3.2.97	• Melhorias de performance ao atrasar o carregamento de montagens do Systems Manager SSM. • Melhora na manipulação de exceção para sysprep2008.xml malformado. • Suporte à linha de comando para a configuração "Apply (Aplicar)" do Systems Manager. • Alteração para suporte de união do domínio quando houver uma renomeação de computador pendente. • Suporte para parâmetros opcionais no plugin `aws:applications` . • Suporte para o array de comando no plugin `aws:psModule` .	
3.0.54	• Habilitar suporte para Systems Manager. • O domínio integra automaticamente as instâncias do EC2 do Windows a um diretório da AWS via Systems Manager. • Configure e carregue logs/métricas do CloudWatch via Systems Manager. • Instale os módulos do PowerShell via Systems Manager. • Instale as aplicações de MSI via Systems Manager.	

Versão	Detalhes	Data de lançamento
2.4.233	• Adicionada uma tarefa programada para recuperar o EC2Config de falhas no startup do serviço. • Melhorias nas mensagens de erro do log do Console. • Atualizações para melhorar o suporte aos serviços da AWS.	
2.3.313	• Corrigido o problema do grande consumo de memória em alguns casos quando o recurso CloudWatch Logs estiver habilitado. • Corrigido um bug no upgrade, de forma que versões do EC2Config anteriores à 2.1.19 agora podem atualizar para a mais recente. • Atualizada a exceção de abertura de porta COM para ser mais amigável e útil em logs. • A UI do Ec2configServiceSettings desabilitou o redimensi onamento e corrigiu a atribuição e o posicionamento de exibição da versão na UI.	
2.2.12	• NullPointerException processado ao consultar uma chave do registro para determinar o estado do Windows Sysprep que retorna nulo ocasionalmente. • Liberados recursos não gerenciados no bloco final.	
2.2.11	Corrigido um problema no plugin do CloudWatch para lidar com linhas vazias do log.	

Versão	Detalhes	Data de lançamento
2.2.10	• Removidas a configuração dos ajustes dos CloudWatch Logs por meio de UI. • Permitir que os usuários definam configurações do CloudWatch Logs no arquivo `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` para permitir melhorias futuras.	
2.2.9	Corrigida a exceção não gerenciada e adicionado registro em log.	
2.2.8	• Corrige verificação da versão do SO do Windows no instalador do EC2Config para dar suporte ao Windows Server 2003 SP1 e posterior. • Corrige o manuseio do valor nulo ao ler as chaves de registro relacionadas à atualização dos arquivos de config do Sysprep.	
2.2.7	• Adicionado suporte para o EC2Config executar durante a execução do Sysprep para Windows 2008 e posterior. • Manipulação de exceções aperfeiçoada e registro em log para melhores diagnósticos	
2.2.6	• Reduzida a carga na instância e no CloudWatch Logs ao carregar os eventos de log. • Resolvido um problema de upgrade, no qual o plugin do CloudWatch Logs nem sempre ficava habilitado	

Versão	Detalhes	Data de lançamento
2.2.5	• Adicionado suporte ao carregamento de logs para o CloudWatch Log Service. • Corrigido um problema de condição de raça no plugin Ec2OutputRDPCert • Alterada a opção de recuperação do serviço EC2Config para reiniciar a partir de TakeNoAction • Adicionada mais informações de exceção quando o EC2Config dá erro	
2.2.4	• Corrigido um erro em PostSysprep.cmd • Corrigido o bug em que o EC2Config não se fixa no menu Iniciar para OS2012+	

Versão	Detalhes	Data de lançamento
2.2.3	• Adicionada opção de instalar o EC2Config sem que o serviço comece imediatamente após a instalação. Para usar, execute 'Ec2Install.exe start=false' pelo prompt de comando • Adicionado parâmetro no plugin do papel de parede para controlar a adição/remoção do papel de parede. Para usar, execute "Ec2WallpaperInfo.exe set" ou "Ec2WallpaperInfo.exe revert" no prompt de comando • Adicionada verificação da chave RealTimeIsUniversal, configurações incorretas de saída da chave de registro de RealTimeIsUniveral para o console • Removida dependência do EC2Config na pasta de temporári os do Windows • Removida dependência de execução de UserData no .Net 3.5	
2.2.2	• Adicionada a verificação para comportamento de parada de serviço para verificar se os recursos estão sendo liberados • Corrigido o problema com longos períodos de execução ao ingressar no domínio	

Versão	Detalhes	Data de lançamento
2.2.1	• Atualizado o instalador para permitir upgrades de versões mais antigas • Corrigido o bug Ec2WallpaperInfo no ambiente exclusivo do .Net4.5 • Corrigindo o bug de detecção do driver intermitente • Adicionada a opção de instalação silenciosa. Execute Ec2Install.exe com a opção '-q', por exemplo: 'Ec2Install.exe -q'	
2.2.0	• Adicionado suporte para ambientes exclusivos de .Net4 e .Net4.5 • Atualizado o instalador	
2.1.19	• Adicionado suporte à etiqueta do disco efêmera ao usar o driver de rede da Intel (por exemplo, tipo de instância C3). Para ter mais informações, consulte Redes aperfeiçoadas no Amazon EC2. • Adicionado suporte à versão de origem da AMI e ao nome de origem da AMI para a saída do console • Alterações feitas à saída do Console para formatação/análise consistente • Arquivo de ajuda atualizado	

Versão	Detalhes	Data de lançamento
2.1.18	• Adicionado objetivo de WMI do EC2Config para notificação de conclusão (-Namespace root\Amazon -Class EC2_ConfigService) • Performance aprimorada da consulta de WMI de startup com grandes logs de evento; pode causar uso elevado prolongado da CPU durante a execução inicial	
2.1.17	• Corrigido problema de execução com enchimento de buffer de saída padrão e erro padrão • O thumbprint de RDP incorreto fixo que às vezes aparece em saída do console para o SO >= w2k8 • A saída do console agora contém "RDPCERTIFICATE-SubjectName:" para Windows 2008+, que contém o valor do nome da máquina • Adicionado D:\ ao menu suspenso de mapeamento da letra de unidade • Movido o botão Ajuda para o canto direito superior e alterada a aparência • Adicionado link de pesquisa de Feedback ao canto direito superior	

Versão	Detalhes	Data de lançamento
2.1.16	• A guia Geral inclui o link da página de download do EC2Config para novas versões • A sobreposição do papel de parede do desktop agora está armazenada na pasta Users Local Appdata, em vez de em Meus Documentos, compatível com o redirecionamento do MyDoc • Nome do MSSQLServer sincronizado com o sistema no script do Post-Sysprep (2008+) • Pasta de aplicação reordenada (arquivos movidos para o diretório Plugin e removidos os arquivos em duplicata) • Alterada saída do log do sistema (Console): • *Movido para o formato data, nome, valor para facilitar a análise (comece a migrar as dependências para um novo formato) • *Adicionado o status do plugin 'Ec2SetPassword' • *Adicionado a hora de início e fim do Sysprep • Corrigido o problema de discos temporários não serem marcados como "Armazenamento Temporário" para sistemas operacionais não em inglês • Corrigida a falha de desinstalação do EC2Config depois de executar Sysprep	

Versão	Detalhes	Data de lançamento
2.1.15	• Solicitações otimizadas do serviço de metadados • Os metadados agora contornam as configurações do proxy • Discos temporários marcados como "Armazenamento temporário" e Important.txt colocados no volume quando encontrados (somente drivers do Citrix PV). Para ter mais informações, consulte Atualizar drivers de PV em instâncias do Windows. • Discos temporários com letras Z a A (somente drivers do Citrix PV) – a atribuição pode ser sobrescrita usando o plugin de mapeamento de letra da unidade com etiquetas de Volume "Armazenamento Temporário X", onde x é um número 0-25 • O UserData agora é executado imediatamente depois de "Windows está pronto"	
2.1.14	Correções do papel de parede do desktop	
2.1.13	• Por padrão, o papel de parede do desktop exibirá o hostname • Dependência removida do serviço de Horário do Windows • Rota adicionada nos casos em que vários IPs são atribuídos a uma única interface	
2.1.11	• Alterações feitas no plugin Ec2Activation • - Verifica o status de Ativação cada 30 dias • - Se o período de carência tiver 90 dias restantes (dos 180), tenta novamente a ativação	

Versão	Detalhes	Data de lançamento
2.1.10	• A sobreposição do papel de parede do desktop não persiste mais com Sysprep ou desativação sem Sysprep • Opção de UserData para executar em cada início de serviço com <persist>true</persist> • Local e nome alterados de /DisableWinUpdate.cmd para /Scripts/PostSysprep.cmd • Senha do administrador definida para não expirar por padrão em /Scripts/PostSysprep.cmd • A desinstalação removerá o script PostSysprep do EC2Config c:\windows\setup\script\CommandComplete.cmd • O Add Route suporta métricas de interface personalizada	
2.1.9	A execução de UserData não é mais limitada a 3851 caracteres	

Versão	Detalhes	Data de lançamento
2.1.7	• Identificador da versão do SO e do idioma gravado no console • Versão do EC2Config gravada no console • Versão do driver PV gravada no console • Detecção de verificação de bugs e saída para o console na inicialização seguinte, quando encontrado • Adicionada opção para o config.xml manter as credenciais de Sysprep • Adicionar lógica de Route Retry nos casos em que o ENI está indisponível no início • PID de execução dos dados do usuário gravados no console • Comprimento mínimo de senha gerado recuperado de GPO • Ajuste o início do serviço para refazer 3 tentativas • Adicionados exemplos S3_DownloadFile.ps1 e S3_Upload file.ps1 à pasta /Scripts	

Versão	Detalhes	Data de lançamento
2.1.6	• Informações da versão adicionadas à guia Geral • Guia Pacote renomeada para Imagem • Simplificado o processo de especificação de senhas e movidas as UIs relacionadas à senha da guia Geral para a guia Imagem • Guia Configurações do disco rebatizada de Armazenamento • Adicionada a guia Suporte com ferramentas comuns para a resolução de problemas • `sysprep.ini` do Windows 2003 configurado para ampliar a partição do SO por padrão • Adicionado o endereço IP privado ao papel de parede • Endereço IP privado exibido no papel de parede • Lógica de tentativas adicionada à saída do Console • Exceção da porta de Com fixa para acessibilidade de metadados – fez com que o EC2Config fosse encerrado, pois a saída do console é exibida • Verifica o status da ativação em cada inicialização – ativa conforme o necessário • Problema corrigido de caminhos relativos – causado ao executar manualmente o atalho do papel de parede pela pasta de startup; apontando para Administrador/logs •	

Versão	Detalhes	Data de lançamento
	Cor de fundo padrão corrigida para usuário do Windows Server 2003 (além do Administrador)	

Versão	Detalhes	Data de lançamento
2.1.2	• Timestamps do console em UTC (Zulu) • Removida a aparência hyperlink na guia Sysprep • Adição de recurso para expandir dinamicamente o volume do dispositivo raiz na primeira inicialização para Windows 2008+ • Quando a opção Set-Password estiver habilitada, permite automaticamente que o EC2Config defina a senha • O EC2Config verifica o status de ativação antes de executar o Sysprep (apresenta uma advertência se não estiver ativado) • O `Sysprep.xml` do Windows Server 2003 agora usa como padrão o fuso horário UTC em vez de hora do Pacífico • Servidores de ativação aleatórios • Guia Mapeamento da unidade rebatizada para Configurações do disco • Itens de UI de Inicializar unidades movidas da guia Geral para a guia Configurações do disco • O botão Ajuda agora aponta para o arquivo de ajuda HTML • Arquivo HTML de ajuda atualizado com alterações • Texto "Observação" atualizado para mapeamentos das letras da unidade • Adicionado InstallUpdates.ps1 à pasta /Scripts para automatizar patches e limpeza antes de Sysprep	

Versão	Detalhes	Data de lançamento
2.1.0	• O papel de parede do desktop exibe informações da instância por padrão no primeiro login (não desconectar/reconectar) • O PowerShell pode ser executado a partir de userdata ao cercar o código com <powershell></powershell>	

Assinar as notificações de serviço do EC2Config

O Amazon SNS pode notificá-lo quando novas versões do serviço EC2Config forem liberadas. Use o procedimento a seguir para se inscrever nessas notificações.

Para se inscrever nas notificações do EC2Config

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
   a. Para o ARN do tópico, use o seguinte ARN (nome de recurso da Amazon):

      ```
      arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
      ```

   b. Para Protocolo, selecione `Email`.
   c. Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações.
   d. Selecione Create subscription.
6. Você receberá um e-mail solicitando que você confirme sua assinatura. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que uma nova versão do serviço EC2Config for liberada, nós enviaremos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a inscrição das notificações do EC2Config

1. Abra o console do Amazon SNS.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a assinatura e escolha Actions, Delete subscriptions. Quando solicitado para confirmação, escolha Delete.

Solucionar problemas com o serviço do EC2Config

As informações a seguir podem ajudá-lo a resolver problemas com o serviço EC2Config.

Atualizar o EC2Config em uma instância inacessível

Use o procedimento a seguir para atualizar o serviço EC2Config em uma instância do Windows Server inacessível usando o Desktop Remoto.

Para atualizar o EC2Config em um a instância do Windows baseada no Amazon EBS à qual você não pode se conectar

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Escolha Launch instances (Executar instância) e crie uma instância `t2.micro` temporária na mesma zona de disponibilidade que a instância afetada. Use uma AMI diferente da que você usou para executar a instância afetada.

> **Important**
>
> Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No console do EC2, selecione Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Desanexe o volume e anexe o volume à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para se conectar à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.
8. Faça download da versão mais recente do serviço EC2Config. Extraia arquivos do arquivo `.zip` para o diretório `Temp` na unidade que você associou.
9. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **`regedit`** e pressione Enter.
10. Selecione `HKEY_LOCAL_MACHINE`. No menu Arquivo, escolha Carregar Hive. Escolha a unidade, vá até ele e abra o seguinte arquivo: `Windows\System32\config\SOFTWARE`. Quando solicitado, especifique o nome da chave.
11. Selecione a chave que você acabou de carregar e vá até `Microsoft\Windows \CurrentVersion`. Escolha a chave `RunOnce`. Se essa chave não existir, escolha `CurrentVersion` no menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Chave. Nomeie a chave `RunOnce`.
12. No menu contextual (clique com o botão direito do mouse), escolha a chave `RunOnce`, escolha Novo e escolha no Valor da string. Insira `Ec2Install` como o nome e `C:\Temp \Ec2Install.exe /quiet` como dados.
13. Escolha a chave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT \CurrentVersion\Winlogon`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira **`AutoAdminLogon`** como o nome e **`1`** como dados.
14. Escolha a chave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira **`DefaultUserName`** como o nome e **`Administrator`** como dados.

15. Escolha a chave HKEY_LOCAL_MACHINE*specified key name*\Microsoft\Windows NT\CurrentVersion\Winlogon. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Digite **DefaultPassword** como nome e digite uma senha nos dados de valor.
16. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.
17. No menu Arquivo, escolha Descarregar Hive.
18. No utilitário Gerenciamento de Disco, escolha o disco que você anexou anteriormente, abra o menu de contexto (botão direito do mouse) e escolha Offline.
19. No console do Amazon EC2, separe o volume afetado da instância temporária e reanexe-o à instância original com o nome de dispositivo /dev/sda1. Especifique o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
20. Início e interrupção de instâncias do Amazon EC2 a instância.
21. Depois que a instância for iniciada, verifique o log do sistema e veja se a mensagem Windows is ready to use aparece.
22. Abra o Editor de Registro e escolha HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Exclua as chaves de valor da string criada anteriormente: AutoAdminLogon, DefaultUserName e DefaultPassword.
23. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Uso do EC2 Fast Launch para as instâncias do Windows

Cada instância Windows do Amazon EC2 deve passar pelas etapas padrão de execução do sistema operacional Windows (SO), que incluem várias reinicializações, e frequentemente levam 15 minutos ou mais para serem concluídas. As AMIs do Windows Server do Amazon EC2 que têm o atributo EC2 Fast Launch habilitado concluem algumas dessas etapas e são reinicializadas com antecedência para reduzir o tempo necessário para iniciar uma instância.

Quando você configura uma AMI do Windows Server para o EC2 Fast Launch, o Amazon EC2 cria um conjunto de snapshots pré-provisionados que serão usados para uma inicialização mais rápida, como se segue.

1. O Amazon EC2 lança um conjunto de instâncias t3 temporárias, com base em suas configurações.

2. À medida que cada instância temporária completa as etapas de lançamento padrão, o Amazon EC2 cria um snapshot pré-provisionado da instância. Ele armazena o snapshot em seu bucket do Amazon S3.
3. Quando o snapshot estiver pronto, o Amazon EC2 encerra a instância t3 associada para manter os custos dos recursos o mais baixos possível.
4. A próxima vez que o Amazon EC2 iniciar uma instância usando uma AMI habilitada para o EC2 Fast Launch, ele usará um dos snapshots para reduzir significativamente o tempo necessário para a inicialização.

O Amazon EC2 reabastece automaticamente os snapshots que você tem disponíveis à medida que os usa para iniciar instâncias usando a AMI habilitada para o EC2 Fast Launch.

Qualquer conta que tenha acesso a uma AMI com o EC2 Fast Launch pode se beneficiar de tempos de inicialização reduzidos. Quando o proprietário da AMI concede acesso para você iniciar instâncias, os snapshots pré-provisionados vêm da conta do proprietário da AMI.

Se uma AMI compatível com o EC2 Fast Launch for compartilhada com você, você mesmo poderá habilitar ou desabilitar a inicialização mais rápida na AMI compartilhada. Se você habilitar uma AMI compartilhada para o EC2 Fast Launch, o Amazon EC2 criará os snapshots pré-provisionados diretamente na sua conta. Se você esgotar os snapshots da sua conta, ainda poderá usar os snapshots da conta do proprietário da AMI.

> **Note**
>
> O EC2 Fast Launch exclui os snapshots pré-provisionados assim que eles são consumidos por uma inicialização para minimizar os custos de armazenamento e evitar a reutilização. No entanto, se os snapshots excluídos corresponderem a uma regra de retenção, a Lixeira os reterá automaticamente. Recomendamos que você revise o escopo das regras de retenção da Lixeira para que isso não aconteça. Para ter mais informações, consulte Considerações. Esse atributo não é o mesmo que a restauração rápida de snapshots do EBS. É necessário habilitar explicitamente a restauração rápida de snapshots do EBS em cada snapshot, e ela tem seus próprios custos associados.

O vídeo a seguir demonstra como configurar sua AMI do Windows para uma inicialização mais rápida com uma visão geral rápida dos principais termos relacionados e suas definições: Lançamento de instâncias do EC2 Windows até 65% mais rápido na AWS.

Custos com recursos

O serviço de configuração das AMIs do Windows para o EC2 Fast Launch não é cobrado. No entanto, o preço padrão se aplica a qualquer recurso da AWS subjacente que o Amazon EC2 usa. Para saber mais sobre os custos de recursos associados e como gerenciá-los, consulte Gerenciamento de custos de recursos com o EC2 Fast Launch.

Conteúdo

- Principais termos
- Pré-requisitos do EC2 Fast Launch
- Configurar o EC2 Fast Launch para a AMI do Windows Server do Amazon EC2
- Visualização de AMIs com o EC2 Fast Launch habilitado
- Gerenciamento de custos de recursos com o EC2 Fast Launch
- Monitorar o EC2 Fast Launch
- Perfil vinculado ao serviço para o EC2 Fast Launch

Principais termos

O atributo EC2 Fast Launch usa os seguintes termos básicos:

Snapshot pré-provisionado

Um snapshot de uma instância que foi iniciada de uma AMI do Windows com o EC2 Fast Launch habilitado e que concluiu as etapas de inicialização do Windows a seguir, reinicializando conforme necessário.

- Especialização sysprep
- Experiência Imediata do Windows (OOBE)

Quando essas etapas são concluídas, o EC2 Fast Launch interrompe a instância e cria um snapshot que é usado posteriormente para uma inicialização mais rápida usando a AMI, de acordo com a sua configuração.

Frequência de execução

Controla o número de snapshots pré-provisionados que o Amazon EC2 pode executar durante o período especificado. Quando você habilita o EC2 Fast Launch para a AMI, o Amazon EC2 cria o conjunto inicial de snapshots pré-provisionados em segundo plano. Por exemplo, se a

frequência de inicialização for definida como cinco inicializações por hora, que é o padrão, o EC2 Fast Launch criará um conjunto inicial de cinco snapshots pré-provisionados.

Quando o Amazon EC2 inicia uma instância usando uma AMI com o EC2 Fast Launch habilitado, ele usa um dos snapshots pré-provisionados para reduzir o tempo de inicialização. Conforme são usados, os snapshots são automaticamente reabastecidos até o número especificado pela frequência de execução.

Se você espera um pico no número de instâncias que são iniciadas a partir da AMI (durante um evento especial, por exemplo), é possível aumentar a frequência de execução com antecedência para cobrir as instâncias adicionais necessárias. Quando sua taxa de execuções voltar ao normal, é possível reajustar a frequência e diminuí-la.

Se você observar um número de inicializações superior ao previsto, poderá usar todos os snapshots pré-provisionados que estiverem disponíveis. Isso não faz com que nenhuma execução falhe. No entanto, isso pode resultar em algumas instâncias passando pelo processo de início padrão, até que os snapshots possam ser reabastecidos.

Contagem de recursos de destino

O número de snapshots pré-provisionados a ser mantido disponível para uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado.

Número máximo de execuções paralelas

Controla quantas instâncias o Amazon EC2 pode iniciar ao mesmo tempo para criar snapshots pré-provisionados para o EC2 Fast Launch. Se a contagem de recursos de destino for maior que o número máximo de execuções em paralelo, o Amazon EC2 iniciará o número de instâncias especificado por Máximo de execuções em paralelo para começar a criar os snapshots. Quando essas instâncias concluem o processo, o Amazon EC2 tira o snapshot e interrompe a instância. Em seguida, ele continua iniciando mais instâncias até que o número total de instantâneos disponíveis atinja a contagem de recursos desejada. O valor de Número máximo de execuções paralelas deve ser 6 ou maior.

Pré-requisitos do EC2 Fast Launch

Antes de configurar o EC2 Fast Launch, certifique-se de ter atendido aos seguintes pré-requisitos de criação de snapshots para as AMIs em sua Conta da AWS:

- Se não usar um modelo de inicialização para definir as configurações, certifique-se de que uma VPC padrão esteja configurada para a região em que você usa o EC2 Fast Launch.

> **Note**
>
> Se você acidentalmente excluir a VPC padrão da região em que planeja configurar o EC2 Fast Launch, poderá criar uma nova VPC padrão nessa região. Para saber mais, consulte Criar uma VPC padrão no Guia do Usuário da Amazon VPC.

- Para especificar uma VPC não padrão, é necessário usar um modelo de execução ao configurar a inicialização mais rápida do Windows. Para ter mais informações, consulte Usar um modelo de inicialização ao configurar o EC2 Fast Launch.
- Se a conta incluir uma política que imponha o IMDSv2 para instâncias do Amazon EC2, é necessário criar um modelo de execução que especifique a configuração de metadados para aplicar o IMDSv2.
- As AMIs do EC2 Fast Launch devem ser compatíveis com a execução de scripts de dados do usuário.
- Para configurar o EC2 Fast Launch para uma AMI, você deve criar a AMI usando Sysprep com a opção de desligamento. Atualmente, o atributo EC2 Fast Launch não é compatível com AMIs criadas em uma instância em execução.

  Para criar uma AMI usando Sysprep, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.
- A cota padrão para Número máximo de execuções paralelas em todas as AMIs em uma Conta da AWS é de 40 por região. É possível solicitar um aumento do Service Quotas de sua conta, da maneira a seguir.

  1. Faça login no AWS Management Console e abra o console do Service Quotas em https://console.aws.amazon.com/servicequotas/.
  2. No painel de navegação, escolha Serviços da AWS.
  3. Na barra de pesquisa, digite `EC2 Fast Launch` e selecione o resultado.
  4. Selecione o link para `Parallel instance launches`. Isso leva você para a página de detalhes da cota de serviço Execução de instâncias em paralelo.
  5. Selecione Solicitar aumento de cota.

  Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Configurar o EC2 Fast Launch para a AMI do Windows Server do Amazon EC2

Você pode configurar o EC2 Fast Launch para as AMIs do Windows de que é proprietário ou para as AMIs compartilhadas com você usando o AWS Management Console, a API, os SDKs, o CloudFormation ou a AWS Command Line Interface (AWS CLI). Antes de configurar o EC2 Fast Launch, certifique-se de que a AMI atenta a todos os pré-requisitos para a criação de snapshots pré-provisionados. Para ter mais informações, consulte Pré-requisitos do EC2 Fast Launch.

Quando você habilita o EC2 Fast Launch, o Amazon EC2 verifica se você tem as permissões necessárias para executar instâncias da AMI e do modelo de inicialização especificados (se fornecidos), incluindo permissões para AMIs criptografadas. Para evitar erros durante o processo de inicialização da instância, o serviço valida suas permissões antes que o EC2 Fast Launch seja habilitado. Caso não haja permissões obrigatórias, o serviço retornará um erro e não habilitará o EC2 Fast Launch.

As seções a seguir abrangem as etapas de configuração para o console do Amazon EC2 e a AWS CLI.

Habilitar o EC2 Fast Launch

Para habilitar o EC2 Fast Launch, escolha a guia correspondente ao seu ambiente e siga as etapas.

> **Note**
>
> Antes de alterar essas configurações, certifique-se de que sua AMI e região de execução atendam a todos os Pré-requisitos do EC2 Fast Launch.

Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. Para começar a usar snapshots pré-provisionados para iniciar instâncias da sua AMI do Windows com mais rapidez, marque a caixa de seleção Habilitar o início rápido do Windows.

6. Na lista suspensa Set anticipated launch frequency (Definir a frequência antecipada de execução), escolha um valor para especificar o número de snapshots que são criados e mantidos para cobrir o volume esperado de execuções de instância.
7. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

> **Note**
>
> Se você precisar usar um modelo de inicialização para especificar uma VPC não padrão ou para definir configurações de metadados para IMDSv2, consulte Usar um modelo de inicialização ao configurar o EC2 Fast Launch.

AWS CLI

O comando enable-fast-launch chama a operação de API EnableFastLaunch do Amazon EC2.

Sintaxe:

```
aws ec2 enable-fast-launch \
  --image-id <value> \
  --resource-type <value> \ (optional)
  --snapshot-configuration <value> \ (optional)
  --launch-template <value> \ (optional)
  --max-parallel-launches <value> \ (optional)
  --dry-run | --no-dry-run \  (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Exemplo:

O exemplo de enable-fast-launch a seguir habilita o EC2 Fast Launch para a AMI especificada, iniciando seis instâncias paralelas para pré-provisionamento. `ResourceType` é definido como `snapshot`, que é o valor padrão.

```
aws ec2 enable-fast-launch \
        --image-id ami-01234567890abcedf  \
        --max-parallel-launches 6 \
        --resource-type snapshot
```

Saída:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {
         "TargetResourceCount": 10
     },
     "LaunchTemplate": {},
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "enabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
 }
```

PowerShell

O cmdlet Enable-EC2FastLaunch chama a operação de API EnableFastLaunch do Amazon EC2 para habilitar o EC2 Fast Launch na AMI do Windows.

Sintaxe:

```
Enable-EC2FastLaunch
      -ImageId <String>
      -LaunchTemplate_LaunchTemplateId <String>
      -LaunchTemplate_LaunchTemplateName <String>
      -MaxParallelLaunch <Int32>
      -ResourceType <String>
      -SnapshotConfiguration_TargetResourceCount <Int32>
      -LaunchTemplate_Version <String>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Exemplo:

O exemplo de Enable-EC2FastLaunch a seguir habilita o EC2 Fast Launch para a AMI especificada, iniciando seis instâncias paralelas para pré-provisionamento. `ResourceType` é definido como `snapshot`, que é o valor padrão.

```
Enable-EC2FastLaunch `
 -ImageId ami-01234567890abcedf `
```

```
-MaxParallelLaunch 6 `
-Region us-west-2 `
-ResourceType snapshot
```

Saída:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Desabilitar o EC2 Fast Launch

Para desabilitar o EC2 Fast Launch, escolha a guia correspondente ao seu ambiente e siga as etapas.

> **Note**
>
> Antes de alterar essas configurações, certifique-se de que sua AMI e região de execução atendam a todos os Pré-requisitos do EC2 Fast Launch.

Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. Desmarque a caixa de seleção Habilitar inicialização rápida para o Windows para desabilitar o EC2 Fast Launch e remover os snapshots pré-provisionados. Isso resulta na AMI usando o processo de início padrão para cada instância, daqui para frente.

> **Note**
>
> Quando você desabilita a otimização de imagens do Windows, todos os snapshots pré-provisionados existentes são excluídos automaticamente. Essa etapa deve ser concluída antes que você possa começar a usar o recurso novamente.

6. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

AWS CLI

O comando disable-fast-launch chama a operação de API DisableFastLaunch do Amazon EC2.

Sintaxe:

```
aws ec2 disable-fast-launch \
  --image-id <value> \
  --force | --no-force \ (optional)
  --dry-run | --no-dry-run \ (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Exemplo:

O exemplo de disable-fast-launch a seguir desabilita o EC2 Fast Launch na AMI especificada e limpa os snapshots pré-provisionados existentes.

```
aws ec2 disable-fast-launch \
        --image-id ami-01234567890abcedf
```

Saída:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {},
     "LaunchTemplate": {
         "LaunchTemplateId": "lt-01234567890abcedf",
         "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
         "Version": "1"
```

```
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

O cmdlet Disable-EC2FastLaunch chama a operação de API DisableFastLaunch do Amazon EC2.

Sintaxe:

```
Disable-EC2FastLaunch
      -ImageId <String>
      -ForceStop <Boolean>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Exemplo:

O exemplo de Disable-EC2Fast-Launch a seguir desabilita o EC2 Fast Launch na AMI especificada e limpa os snapshots pré-provisionados existentes.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcedf
```

Saída:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Usar um modelo de inicialização ao configurar o EC2 Fast Launch

Com um modelo de inicialização, é possível configurar um conjunto de parâmetros de inicialização que é usado pelo Amazon EC2 toda vez que ele inicializa uma instância com base nesse modelo. É possível especificar opções como uma AMI a ser usada para sua imagem base, tipos de instância, armazenamento, configurações de rede e muito mais.

Os modelos de inicialização são opcionais, exceto nos seguintes casos específicos em que é necessário usar um modelo de inicialização para sua AMI do Windows ao configurar a inicialização mais rápida:

- É necessário usar um modelo de inicialização para especificar uma VPC não padrão para a AMI do Windows.
- Se a conta incluir uma política que imponha o IMDSv2 para instâncias do Amazon EC2, é necessário criar um modelo de execução que especifique a configuração de metadados para aplicar o IMDSv2.

  Use o modelo de inicialização que inclui sua configuração de metadados do console do EC2 console ou execute o comando enable-fast-launch na AWS CLI ou chame a ação da API EnableFastLaunch.

O EC2 Fast Launch do Amazon EC2 não é compatível com a configuração a seguir quando você usa um modelo de inicialização. Se você usar um modelo de inicialização para o EC2 Fast Launch, não deverá especificar nenhum dos seguintes itens:

- Scripts de dados do usuário
- Termination protection
- Metadados desabilitados
- Opção spot
- Comportamento de desligamento que encerra a instância
- Etiquetas de recursos para solicitações de interfaces de rede, de gráficos elásticos ou de instâncias spot

Especificar uma VPC não padrão

Etapa 1: Criar um modelo de execução

Crie um modelo de execução que especifique os seguintes detalhes para suas instâncias do Windows:

- A sub-rede da VPC.
- Um tipo de instância de `t3.xlarge`.

Para ter mais informações, consulte Criar um modelo de inicialização.

Etapa 2: especificar o modelo de inicialização para a AMI do EC2 Fast Launch

Escolha a guia que corresponde ao seu processo:

Console

Para especificar o modelo de inicialização para o EC2 Fast Launch no AWS Management Console, siga estas etapas:

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. A caixa Launch template (Modelo de inicialização) executa uma pesquisa filtrada que localiza modelos de inicialização em sua conta na região atual que correspondem ao texto digitado. Especifique todo ou parte do nome ou ID do modelo de inicialização na caixa para mostrar uma lista de modelos de inicialização correspondentes. Por exemplo, se você inserir `fast` na caixa, o Amazon EC2 encontrará todos os modelos de inicialização em sua conta na região atual que contêm "fast" no nome.

   Para criar um novo modelo de inicialização, escolha Create launch template (Criar modelo de inicialização).
6. Quando um modelo de inicialização é selecionado, o Amazon EC2 mostra a versão padrão desse modelo na caixa Source template version (Versão do modelo de origem). Para especificar uma versão diferente, realce a versão padrão para substituí-la e insira o número da versão desejada na caixa.
7. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

AWS CLI, API

Para especificar o modelo de inicialização do EC2 Fast Launch usando a AWS CLI, especifique o nome ou o ID do modelo de inicialização no parâmetro `--launch-template` ao executar o comando enable-fast-launch na AWS CLI.

Para especificar o modelo de inicialização do EC2 Fast Launch em uma solicitação da API, especifique o nome ou o ID do modelo de inicialização no parâmetro `LaunchTemplate` ao chamar a ação da API EnableFastLaunch.

Para obter mais informações sobre modelos de inicialização do EC2, consulte Executar uma instância a partir de um modelo de execução.

Criar uma imagem personalizada com EC2 Fast Launch habilitado

O EC2 Fast Launch do Amazon EC2 se integra ao EC2 Image Builder para ajudar você a criar imagens personalizadas com o EC2 Fast Launch habilitado. Para obter mais informações, consulte Criar configurações de distribuição para uma AMI Windows com o EC2 Fast Launch habilitado (AWS CLI) no Guia do usuário do EC2 Image Builder.

Visualização de AMIs com o EC2 Fast Launch habilitado

Você pode usar o comando describe-fast-launch-images na AWS CLI ou o Cmdlet Get-EC2FastLaunchImage do Tools for PowerShell para obter os detalhes das AMIs que têm o EC2 Fast Launch habilitado.

O Amazon EC2 fornece os seguintes detalhes para cada AMI do Windows retornada nos resultados:

- O ID da imagem de uma AMI com o EC2 Fast Launch habilitado.
- O tipo de recurso usado para pré-provisionamento da AMI do Windows associada. Valor compatível: `snapshot`.
- A configuração de snapshot, que é um grupo de parâmetros usados para pré-provisionar a AMI do Windows associada usando snapshots.
- Informações do modelo de execução, incluindo o ID, o nome e a versão do modelo de execução que a AMI associada usa quando executa instâncias do Windows de snapshots pré-provisionados.
- O número máximo de instâncias que podem ser executadas ao mesmo tempo para a criação de recursos.
- O ID do proprietário da AMI associada. Isso não é preenchido para as AMIs que são compartilhadas com você.

- O estado atual do EC2 Fast Launch para a AMI associada. Os valores com suporte incluem: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> É possível ver também o estado atual exibido na página Manage image optimization (Gerenciar otimização de imagens) no console do EC2 em Image optimization state (Estado da otimização de imagem).

- O motivo pelo qual o EC2 Fast Launch para a AMI associada foi alterado para o estado atual.
- A hora em que o EC2 Fast Launch para a AMI associada foi alterado para o estado atual.

Escolha a guia correspondente ao ambiente de linha de comando:

AWS CLI

O comando describe-fast-launch-images chama a operação de API DescribeFastLaunchImages do Amazon EC2.

Sintaxe:

```
aws ec2 describe-fast-launch-images \
 --image-ids <value> \ (optional)
 --filters <value> \ (optional)
 --dry-run | --no-dry-run \ (optional)
 --cli-input-json <value> \ (optional)
 --starting-token <value> \ (optional)
 --page-size <value> \ (optional)
 --max-items <value> \ (optional)
 --generate-cli-skeleton <value> \ (optional)
```

Exemplo:

O exemplo de describe-fast-launch-images a seguir descreve os detalhes de todas as AMIs da conta que estão configuradas para o EC2 Fast Launch. Neste exemplo, apenas uma AMI da conta está configurada para o EC2 Fast Launch.

```
aws ec2 describe-fast-launch-images
```

Saída:

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Tools for PowerShell

O cmdlet Get-EC2FastLaunchImage chama a operação de API DescribeFastLaunchImages do Amazon EC2.

Sintaxe:

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
-Select <String>
-NoAutoIteration <SwitchParameter>
```

Exemplo:

O exemplo de Get-EC2FastLaunchImage a seguir descreve os detalhes de todas as AMIs da conta que estão configuradas para o EC2 Fast Launch. Neste exemplo, apenas uma AMI da conta está configurada para o EC2 Fast Launch.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcedf
```

Saída:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Gerenciamento de custos de recursos com o EC2 Fast Launch

O serviço de configuração das AMIs do Windows para o EC2 Fast Launch não é cobrado. Porém, quando você habilita o EC2 Fast Launch. para uma AMI do Windows do Amazon EC2, os preços padrão se aplicam aos recursos subjacentes da AWS que o Amazon EC2 usa para preparar e armazenar os snapshots pré-provisionados. Você pode configurar tags de alocação de custos para ajudar a rastrear e gerenciar os custos associados aos recursos do EC2 Fast Launch. Para obter mais informações sobre como configurar tags de alocação de custos, consulte Acompanhar os custos do EC2 Fast Launch em sua fatura.

O exemplo a seguir demonstra como os custos associados aos snapshots do EC2 Fast Launch podem ser alocados.

Cenário de exemplo: a empresa de exemplo AtoZ tem uma AMI do Windows com um volume raiz do EBS com 50 GiB. A empresa habilitou o EC2 Fast Launch.para a AMI e definiu o número de recursos de destino como cinco. No decorrer de um mês, o uso do EC2 Fast Launch para a AMI custa aproximadamente USD 5,00. O detalhamento de custos é o seguinte:

1. Quando o exemplo da AtoZ habilita o EC2 Fast Launch, o Amazon EC2 inicia cinco instâncias pequenas. Cada instância é executada pelas etapas de execução Sysprep e OOBE Windows, reinicializando conforme necessário. Isso leva vários minutos para cada instância (o tempo pode variar de acordo com o nível de movimentação da região ou Availability Zone [AZ – Zona de disponibilidade] e com o tamanho da AMI).

Custos

- Custos de runtime de instância (ou tempo mínimo de execução, se for o caso): 5 instâncias
- Custos de volume: 5 volumes raiz do EBS

2. Quando o processo de pré-provisionamento é concluído, o Amazon EC2 obtém um snapshot da instância e armazena no Amazon S3. Normalmente, os snapshots são armazenados por 4 a 8 horas antes de serem consumidos por uma inicialização. Nesse caso, o custo é de aproximadamente USD 0,02 a USD 0,05 por snapshot.

   Custos

   - Armazenamento de snapshots (Amazon S3): 5 snapshots

3. Após obter o snapshot, o Amazon EC2 interrompe a instância. Nesse momento, a instância não está mais acumulando custos. No entanto, os custos por volume do EBS continuam sendo acumulados.

   Custos

   - Volumes do EBS: os custos continuam para os volumes raiz associados do EBS.

> **Note**
>
> Os custos apresentados aqui são apenas para fins de demonstração. Seus custos vão variar de acordo com a configuração da AMI e do plano de preços.

Acompanhar os custos do EC2 Fast Launch em sua fatura

As tags de alocação de custos podem ajudar você a organizar sua fatura da AWS para refletir os custos associados ao EC2 Fast Launch. Você pode usar a seguinte tag que o Amazon EC2 adiciona aos recursos que cria ao preparar e armazenar snapshots pré-provisionados para o EC2 Fast Launch:

Chave de etiqueta: `CreatedBy`, Valor: `EC2 Fast Launch`

Após a etiqueta ser ativada no console do Billing and Cost Management e seu relatório de faturamento detalhado ser configurado, a coluna `user:CreatedBy` aparece no relatório. A coluna inclui valores de todos os serviços. No entanto, se você baixar o arquivo CSV, poderá importar os

dados para uma planilha e filtrar por `EC2 Fast Launch` no valor. Essas informações também são exibidas no AWS Cost and Usage Report quando a etiqueta está ativada.

Etapa 1: ativar etiquetas de alocação de custos definidas pelo usuário

Para incluir etiquetas de recursos nos relatórios de custos, é necessário ativá-las primeiro no console do Billing and Cost Management. Para obter mais informações, consulte Ativar tags de alocação de custos definidos pelo usuário no Guia do usuário do AWS Billing and Cost Management.

> **Note**
>
> A ativação pode demorar até 24 horas.

Etapa 2: configurar um relatório de custos

Se você já tiver um relatório de custos configurado, uma coluna para sua etiqueta será exibida na próxima vez que o relatório for executado após a conclusão da ativação. Para configurar os relatórios de custos pela primeira vez, escolha uma das opções a seguir.

- Consulte Setting up a monthly cost allocation report (Configurar um relatório de alocação de custos mensal) no Guia do usuário do AWS Billing and Cost Management.
- Consulte Creating cost and usage reports (Criar relatórios de custos e uso) no Guia do usuário do AWS Cost and Usage Report.

> **Note**
>
> Pode demorar até 24 horas para que a AWS comece a entregar relatórios em seu bucket do S3.

Você pode configurar o EC2 Fast Launch para as AMIs do Windows das quais é o proprietário ou das AMIs compartilhadas com você usando o console, a API e os SDKs do Amazon EC2, o CloudFormation ou os comandos ec2 da AWS CLI. As seções a seguir abrangem as etapas de configuração para o console do Amazon EC2 e a AWS CLI.

Você também pode criar AMIs do Windows personalizadas que são configuradas para o EC2 Fast Launch com o EC2 Image Builder. Para obter mais informações, consulte Create distribution settings for a Windows AMI with EC2 Fast Launch enabled (AWS CLI).

Monitorar o EC2 Fast Launch

Esta seção aborda como monitorar as AMIs do Windows Server do Amazon EC2 da sua conta que têm o EC2 Fast Launch habilitado.

Monitorar as alterações de estado do EC2 Fast Launch com o EventBridge

Quando o estado de uma AMI do Windows com o EC2 Fast Launch habilitado é alterado, o Amazon EC2 gera um evento de `EC2 Fast Launch State-change Notification`. Em seguida, o Amazon EC2 envia o evento de mudança de estado ao Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events).

É possível criar regras do EventBridge que acionem uma ou mais ações em resposta ao evento de mudança de estado. Por exemplo, você pode criar uma regra do EventBridge que detecta quando o EC2 Fast Launch está habilitado e executa as seguintes ações:

- Envia uma mensagem para um tópico do Amazon SNS que notifica seus assinantes.
- Invoca uma função do Lambda que executa alguma ação.
- Envia os dados de alteração de estado ao Amazon Data Firehose para análise.

Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos no Guia do usuário do Amazon EventBridge.

Eventos de alteração de estado

O atributo EC2 Fast Launch faz todos os esforços para emitir eventos de alteração de estado no formato JSON. O Amazon EC2 envia os eventos ao EventBridge praticamente em tempo real. Esta seção descreve os campos do evento e mostra um exemplo do formato do evento.

`EC2 Fast Launch State-change Notification`

imageId

Identifica a AMI com a alteração de estado do EC2 Fast Launch.

resourceType

O tipo de recurso a ser usado para pré-provisionamento. Valor compatível: `snapshot`. O valor padrão é `snapshot`.

estado

O estado atual do atributo EC2 Fast Launch para a AMI especificada. Entre os valores válidos estão os seguintes:

- enabling: você habilitou o atributo EC2 Fast Launch para a AMI, e o Amazon EC2 iniciou a criação de snapshots para o processo de pré-provisionamento.
- enabling-failed: houve algum tipo de problema que causou falha no processo de pré-provisionamento a primeira vez que você habilitou o EC2 Fast Launch para uma AMI. Isso pode acontecer a qualquer momento durante o processo de pré-provisionamento.
- enabled: o atributo EC2 Fast Launch está habilitado. O estado é alterado para `enabled` assim que o Amazon EC2 cria o primeiro snapshot pré-provisionado para uma AMI do EC2 Fast Launch recém-habilitada. Se a AMI já estiver habilitada e passar pelo pré-provisionamento novamente, a mudança de estado ocorrerá imediatamente.
- enabled-failed: esse estado só se aplicará se não for a primeira vez que a AMI do EC2 Fast Launch passa pelo processo de pré-provisionamento. Isso poderá acontecer se o atributo EC2 Fast Launch for desabilitado e depois habilitado novamente, se houver uma alteração na configuração ou outro erro após o pré-provisionamento ser concluído pela primeira vez.
- disabling: o proprietário da AMI desativou o atributo EC2 Fast Launch para a AMI e o Amazon EC2 iniciou o processo de limpeza.
- disabled: o atributo EC2 Fast Launch está desabilitado. O estado muda para `disabled` assim que o Amazon EC2 conclui o processo de limpeza.
- disabling-failed (falha de desabilitando): algo deu errado e causou a falha no processo de limpeza. Isso significa que alguns snapshots pré-provisionados ainda podem permanecer na conta.

stateTransitionReason

O motivo pelo qual o estado da AMI do EC2 Fast Launch foi alterado.

> **Note**
>
> Todos os campos desta mensagem de evento são obrigatórios.

O exemplo a seguir mostra uma AMI do EC2 Fast Launch recém-habilitada que iniciou a primeira instância para começar o processo de pré-provisionamento. Neste ponto, o estado é `enabling`. Depois que o Amazon EC2 cria o primeiro snapshot pré-provisionado, o estado muda para `enabled`.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Monitorar as métricas do EC2 Fast Launch com o CloudWatch

As AMIs do Amazon EC2 com o EC2 Fast Launch habilitado enviam métricas para o Amazon CloudWatch. Você pode usar o AWS Management Console, a AWS CLI ou uma API para listar as métricas que o EC2 Fast Launch envia para o CloudWatch. O namespace `AWS/EC2` inclui as seguintes métricas do EC2 Fast Launch:

Métrica	Descrição
NumberOfAvailableFastLaunchSnapshots	O número de snapshots pré-provisionados disponível por AMI habilitada para o EC2 Fast Launch.
NumberOfInstancesFastLaunched	O número de instâncias por AMI habilitada para o EC2 Fast Launch que foram iniciadas em snapshots pré-provisionados.
NumberOfInstancesNotFastLaunched	O número de instâncias por AMI habilitada para o EC2 Fast Launch que resultaram em uma inicialização a frio devido à falta de instantân

Métrica	Descrição
	eos pré-provisionados disponíveis na hora da inicialização.
FastLaunchSnapshotUsedToRefillStartTime	A data e hora em que o Amazon EC2 iniciou uma nova imagem usando uma AMI habilitad a para o EC2 Fast Launch para criar outro snapshot após um snapshot existente ser usado.
FastLaunchSnapshotCreationTime	Mede o tempo que o Amazon EC2 leva para iniciar uma instância e criar um snapshot para uma AMI habilitada para o EC2 Fast Launch.

Perfil vinculado ao serviço para o EC2 Fast Launch

O Amazon EC2 usa funções vinculadas ao serviço para as permissões necessárias para chamar outros Serviços da AWS em seu nome. O perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS service (Serviço da AWS). Os perfis vinculados a serviços oferecem uma maneira segura de delegar permissões a outros Serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações sobre o Amazon EC2 usa as funções do IAM, incluindo funções vinculadas ao serviço, consulte Funções do IAM para Amazon EC2.

O Amazon EC2 usa a função vinculada ao serviço de nome `AWSServiceRoleForEC2FastLaunch` para criar e gerenciar um conjunto de snapshots pré-provisionados que reduzem o tempo necessário para iniciar instâncias a partir da sua AMI do Windows.

Você não precisa criar manualmente essa função vinculada ao serviço. Quando você começa a usar o EC2 Fast Launch para a AMI, o Amazon EC2 cria o perfil vinculado ao serviço, caso ele ainda não exista.

> **Note**
>
> Se o perfil vinculado ao serviço for excluído de sua conta, você poderá habilitar o EC2 Fast Launch para outra AMI do Windows a fim de recriar o perfil em sua conta. Ou então, você pode desabilitar o EC2 Fast Launch para a AMI atual e, em seguida, habilitá-lo novamente.

No entanto, desabilitar o atributo resulta em sua AMI usando o processo de início padrão para todas as novas instâncias, enquanto o Amazon EC2 remove todos os snapshots pré-provisionados. Depois que todos os snapshots pré-provisionados são excluídos, você pode habilitar novamente o uso do EC2 Fast Launch para a AMI.

O Amazon EC2 não permite que você edite a função vinculada ao serviço do `AWSServiceRoleForEC2FastLaunch`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

É possível excluir uma função vinculada ao serviço somente depois de excluir todos os recursos relacionados. Isso protege os recursos do Amazon EC2 que estão associados à AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado, pois não será possível remover acidentalmente a permissão para acessar os recursos.

O Amazon EC2 é compatível com o perfil vinculado ao serviço do EC2 Fast Launch em todas as regiões em que o serviço do Amazon EC2 está disponível. Para ter mais informações, consulte Regiões.

Permissões concedidas pelo **`AWSServiceRoleForEC2FastLaunch`**

O Amazon EC2 usa a política gerenciada `EC2FastLaunchServiceRolePolicy` para concluir as ações a seguir:

- `cloudwatch:PutMetricData`: publicar os dados das métricas associadas ao EC2 Fast Launch para o namespace do Amazon EC2.
- `ec2:CreateLaunchTemplate`: criar um modelo de inicialização para a AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado.
- `ec2:CreateSnapshot`: criar snapshots pré-provisionados para a AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado.
- `ec2:CreateTags`: criar tags para os recursos associados à inicialização e ao pré-provisionamento de instâncias do Windows para a AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado.
- `ec2:DeleteSnapshots`: excluir todos os snapshots pré-provisionados associados se o EC2 Fast Launch for desabilitado para uma AMI anteriormente habilitada.
- `ec2:DescribeImages`: descreve imagens para todos os recursos.

- `ec2:DescribeInstanceAttribute`: descreve os atributos da instância para todos os recursos.
- `ec2:DescribeInstanceStatus`: descreve os status da instância para todos os recursos.
- `ec2:DescribeInstances`: descreve as instâncias para todos os recursos.
- `ec2:DescribeInstanceTypeOfferings`: descreve as ofertas de tipos de instância para todos os recursos.
- `ec2:DescribeLaunchTemplates`: descreve modelos de início para todos os recursos.
- `ec2:DescribeLaunchTemplateVersions`: descreve versões de modelos de início para todos os recursos.
- `ec2:DescribeSnapshots`: descreva recursos de snapshot para todos os recursos.
- `ec2:DescribeSubnets`: descreva sub-redes para todos os recursos.
- `ec2:RunInstances`: iniciar instâncias em uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado para realizar as etapas de provisionamento.
- `ec2:StopInstances`: interromper as instâncias que foram iniciadas em uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado para criar snapshots pré-provisionados.
- `ec2:TerminateInstances`: encerrar uma instância que foi iniciada usando uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado após criar o snapshot pré-provisionado usando essa instância.
- `iam:PassRole`: permite que a função vinculada ao serviço `AWSServiceRoleForEC2FastLaunch` inicie instâncias em seu nome usando o perfil da instância do modelo de execução.

Para obter mais informações sobre o uso de políticas gerenciadas no Amazon EC2, consulte Políticas gerenciadas pela AWS para o Amazon EC2.

Acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Pré-requisito

- Para permitir que o Amazon EC2 acesse uma AMI criptografada em seu nome, é necessário ter permissão para a ação `createGrant` na chave gerenciada pelo cliente.

Quando você habilita o EC2 Fast Launch para uma AMI criptografada, o Amazon EC2 garante que seja concedida ao perfil de `AWSServiceRoleForEC2FastLaunch` permissão de usar a chave gerenciada pelo cliente para acessar a AMI. Essa permissão é necessária para iniciar instâncias e criar snapshots pré-provisionados em seu nome.

Uso de aceleradores Amazon Elastic Graphics em instâncias do Windows

> **Important**
>
> O Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.

O Amazon Elastic Graphics oferece aceleração gráfica flexível, de baixo custo e de alta performance para suas instâncias do Windows. Os aceleradores do Elastic Graphics são fornecidos em vários tamanhos e são uma alternativa de baixo custo ao uso de tipos de instância de gráficos de GPU (como a instância G3). Você tem a flexibilidade de escolher um tipo de instância que atenda às necessidades de computação, memória e armazenamento de sua aplicação. Em seguida, escolha o acelerador para sua instância que atenda aos requisitos gráficos de sua workload.

O Elastic Graphics é adequado para aplicações que exigem uma quantidade pequena ou intermitente de aceleração gráfica adicional e que usam o suporte gráfico OpenGL. Se você precisa de acesso a GPUs completas e anexadas diretamente e precisa usar frameworks de computação paralela DirectX, CUDA ou Open Computing Language (OpenCL), use um tipo de instância de computação acelerada.

Conteúdo

- Conceitos básicos de Elastic Graphics
- Definição de preço do Elastic Graphics
- Limitações de Elastic Graphics
- Como trabalhar com o Elastic Graphics
- Manutenção do Elastic Graphics
- Usar métricas do CloudWatch para monitorar o Elastic Graphics
- Solução de problemas

Conceitos básicos de Elastic Graphics

Para usar o Elastic Graphics, execute uma instância do Windows e especifique um tipo de aceleradora para a instância durante a execução. A AWS encontra a capacidade disponível para

o Elastic Graphics e estabelece uma conexão de rede entre a instância e a aceleradora do Elastic Graphics.

> **Note**
>
> Não há suporte para instâncias bare metal

As aceleradoras do Elastic Graphics estão disponíveis nas seguintes regiões da AWS: `us-east-1`, `us-east-2`, `us-west-2`, `ap-northeast-1`, `ap-southeast-1`, `ap-southeast-2`, `eu-central-1` e `eu-west-1`.

Os tipos de instância a seguir oferecem suporte a aceleradores do Elastic Graphics:

- Uso geral: M3, M4, M5, M5d, M5dn, M5n, T2, T3

  > **Note**
  >
  > Há suporte somente para `t2.medium` e maiores e `t3.medium` e maiores.

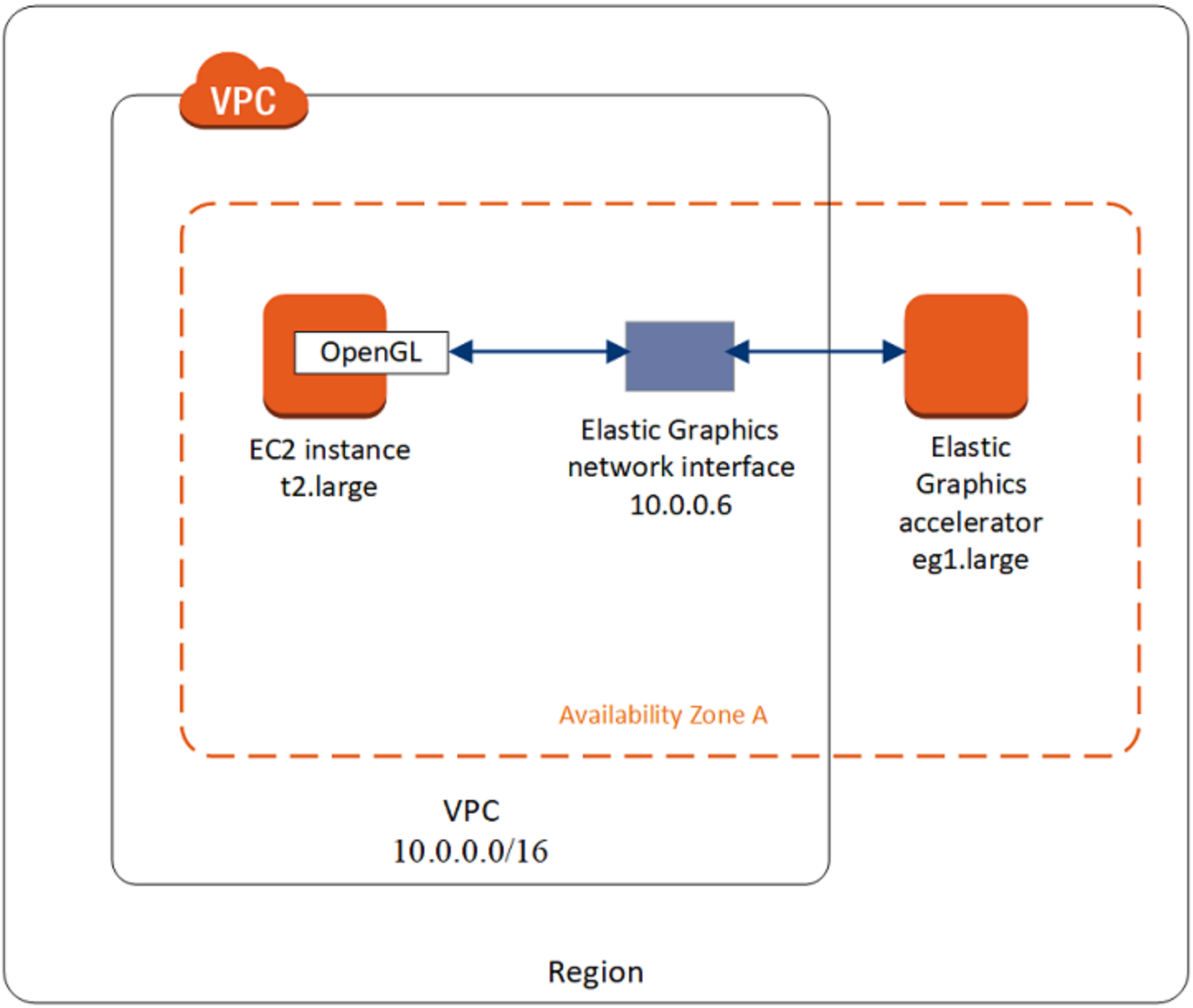
- Otimizadas para computação: C3, C4, C5, C5a, C5ad, C5d, C5n
- Otimizadas para memória: R3, R4, R5, R5d, R5dn, R5n, X1, X1e, z1d
- Otimizadas para armazenamento: D2, D3, D3en, H1, I3, I3en
- Computação acelerada: P2, P3, P3dn

O aceleradores do Elastic Graphics a seguir estão disponíveis. Você pode anexar qualquer acelerador do Elastic Graphics a qualquer tipo de instância compatível.

Aceleradora do Elastic Graphics	Memória gráfica (GB)
`eg1.medium`	1
`eg1.large`	2
`eg1.xlarge`	4
`eg1.2xlarge`	8

Um acelerador do Elastic Graphics não faz parte do hardware de sua instância. Em vez disso, ele é anexado à rede por meio de uma interface de rede, conhecida como a interface de rede do Elastic Graphics. Ao executar ou reiniciar uma instância com aceleração gráfica, a interface de rede do Elastic Graphics é criada em sua VPC.

A interface de rede do Elastic Graphics é criada nas mesmas sub-rede e VPC de sua instância e recebe um IPv4 privado dessa sub-rede. O acelerador anexado a sua instância do Amazon EC2 é alocado a partir de um grupo de aceleradores disponíveis na mesma zona de disponibilidade de sua instância.



Os aceleradores do Elastic Graphics oferecem suporte aos padrões da API do OpenGL 4.3 e anteriores, que podem ser usados para aplicações em lotes ou para aceleração gráfica em 3D. Uma biblioteca do OpenGL otimizada pela Amazon em sua instância detecta o acelerador anexado. Ela direciona as chamadas à OpenGL API de sua instância para o acelerador, que, em seguida, processa as solicitações e retorna os resultados. O tráfego entre a instância e o acelerador usa a mesma largura de banda que o tráfego de rede da instância, portanto, recomendamos que você tenha largura de banda de rede adequada disponível. Consulte seu fornecedor de software em relação a dúvidas sobre conformidade e versão do OpenGL.

Como padrão, o grupo de segurança padrão de sua VPC é associado à interface de rede do Elastic Graphics. O tráfego de rede do Elastic Graphics usa o protocolo TCP e a porta 2007. Certifique-se de que o grupo de segurança de sua instância permita isso. Para obter mais informações, consulte Configurar grupos de segurança.

Definição de preço do Elastic Graphics

Você será cobrado por cada segundo em que um acelerador do Elastic Graphics estiver anexado a uma instância no estado `running` quando o acelerador estiver no estado `0k`. Você não é cobrado por um acelerador anexado a uma instância que esteja no estado `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`. Você também não é cobrado quando um acelerador estiver no estado `Unknown` ou `Impaired`.

A definição de preço de aceleradores está disponível apenas a taxas sob demanda. Você pode anexar um aceleradora a uma instância reservada ou instância spot, no entanto, o preço sob demanda da aceleradora se aplica.

Para obter mais informações, consulte Definição de preço Amazon Elastic Graphics.

Limitações de Elastic Graphics

Antes de começar a usar aceleradores do Elastic Graphics, esteja ciente das seguintes limitações:

- Só é possível anexar aceleradores a instâncias do Windows com o Microsoft Windows Server 2012 R2 ou posterior. No momento, não há suporte às instâncias do Linux.
- É possível anexar uma aceleradora por vez a uma instância.
- É possível anexar apenas uma aceleradora durante o lançamento da instância. Não é possível anexar uma aceleradora a uma instância existente.
- Você não pode hibernar uma instância com uma aceleradora anexada.

- Não é possível compartilhar um acelerador entre instâncias.
- Não é possível desanexar um acelerador de uma instância ou transferi-lo para outra instância. Se você não precisar mais de um acelerador, será necessário encerrar a instância. Para alterar o tipo de acelerador, crie uma AMI a partir de sua instância, encerre-a e execute uma nova instância com uma especificação de acelerador diferente.
- As únicas versões compatíveis da OpenGL API são a 4.3 e anteriores. DirectX, CUDA, e OpenCL não são compatíveis.
- O acelerador do Elastic Graphics não é visível ou acessível por meio do gerenciador de dispositivos de sua instância.
- Você não pode reservar ou programar capacidade para o acelerador.

Como trabalhar com o Elastic Graphics

> **Important**
>
> O Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.

Você pode executar uma instância e associá-la a um acelerador do Elastic Graphics durante a execução. Em seguida, você deve instalar as bibliotecas necessárias manualmente em sua instância que permitam a comunicação com o acelerador. Para obter limitações, consulte Limitações de Elastic Graphics.

Tarefas

- Configurar grupos de segurança
- Iniciar uma instância com uma aceleradora do Elastic Graphics
- Instalar o software necessário para o Elastic Graphics
- Verificar a funcionalidade do Elastic Graphics em sua instância
- Ver informações do Elastic Graphics
- Enviar feedback

Configurar grupos de segurança

O Elastic Graphics requer um grupo de segurança de autorreferência que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O grupo de segurança deve incluir as regras de entrada e saída a seguir.

Entrada

Tipo	Protocolo	Port (Porta)	Origem
Elastic Graphics	TCP	2007	O ID do grupo de segurança (seu próprio ID de recurso)

Saída

Tipo	Protocolo	Port Range (Intervalo de portas)	Destination (Destino)
Elastic Graphics	TCP	2007	O ID do grupo de segurança (seu próprio ID de recurso)

Ao usar o console do Amazon EC2 para iniciar sua instância com um acelerador do Elastic Graphics, você poderá permitir que o assistente de execução crie automaticamente as regras do grupo de segurança necessárias ou selecione uma segurança criada anteriormente.

Se você estiver iniciando sua instância usando a AWS CLI ou um SDK, será necessário especificar um grupo de segurança criado anteriormente.

Para criar um grupo de segurança para o Elastic Graphics

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:

    a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como `Elastic Graphics security group`.

b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.
c. Em VPC, selecione a VPC na qual você pretende usar o Elastic Graphics.
d. Escolha Create security group (Criar grupo de segurança).

4. No painel de navegação, escolha Security Groups (Grupos de segurança), selecione o grupo de segurança que você acabou de criar e na guia Details (Detalhes), copie o ID do grupo de segurança.
5. Na guia Inbound rules (Regras de entrada), escolha Edit inbound rules (Editar regras de entrada) e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Em Type (Tipo), escolha Elastic Graphics.
   c. Em Source type (Tipo de origem), escolha Custom (Personalizado).
   d. Em Source (Origem), cole o ID do grupo de segurança que copiou anteriormente.
   e. Escolha Salvar regras.
6. Na guia Outbound rules (Regras de saída), escolha Edit outbound rules (Editar regras de saída) e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Em Type (Tipo), escolha Elastic Graphics.
   c. Em Destination type (Tipo de destino), escolha Custom (Personalizado).
   d. Em Destination (Destino), cole o ID do grupo de segurança que copiou anteriormente.
   e. Escolha Salvar regras.

Para ter mais informações, consulte Grupos de segurança do Amazon EC2 para as instâncias do EC2.

Iniciar uma instância com uma aceleradora do Elastic Graphics

É possível associar um acelerador do Elastic Graphics a uma instância durante a execução. Se houver falha na execução, os seguintes motivos serão possíveis:

- Capacidade insuficiente do acelerador do Elastic Graphics
- Limite excedido nos aceleradores do Elastic Graphics na região
- Não há endereços IPv4 privados suficientes em sua VPC para criar uma interface de rede para o acelerador

Para obter mais informações, consulte Limitações de Elastic Graphics.

Para associar um acelerador do Elastic Graphics durante a execução da instância (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Launch Instance (Executar instância).
3. Em Nome e tags, insira um valor para Nome. Opcionalmente, você pode escolher Adicionar tags adicionais para adicionar outras tags aos recursos associados à instância que você está iniciando.
4. Em Imagens de aplicações e sistema operacional (imagem de máquina da Amazon), selecione uma AMI do Windows.
5. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para ter mais informações, consulte Conceitos básicos de Elastic Graphics.
6. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
7. Ao lado de Configurações de rede, escolha Editar e especifique as configurações de rede a serem usadas para a instância.
   a. Em Rede, selecione a VPC para a instância.
   b. Em Sub-rede, escolha a sub-rede na qual deseja iniciar a instância.
   c. Na página Firewall (grupos de segurança), você pode deixar o grupo de segurança que criou manualmente em Configurar grupos de segurança ou deixar o console criar um grupo de segurança com as regras de entrada e de saída necessárias. Adicione grupos de segurança adicionais conforme necessário.
8. (Opcional) Em Configurar armazenamento, configure o tamanho do volume raiz e adicione ouros volumes conforme necessário.
9. Expanda a seção Detalhes avançados.
10. Em Detalhes avançados, para GPU elástico, selecione um tipo de acelerador de gráficos elásticos.
11. No painel Resumo painel, escolha Iniciar instância.

Para associar uma aceleradora do Elastic Graphics durante a execução da instância (AWS CLI)

Você pode usar o comando run-instances da AWS CLI com o seguinte parâmetro:

```
--elastic-gpu-specification Type=eg1.medium
```

Para o parâmetro `--security-group-ids`, você deve incluir um grupo de segurança que tenha as regras de entrada e saída necessárias. Para obter mais informações, consulte Configurar grupos de segurança.

Para associar um acelerador do Elastic Graphics durante a execução da instância (Tools for Windows PowerShell).

Use o comando New-EC2Instance do Tools for Windows PowerShell.

Instalar o software necessário para o Elastic Graphics

Se você tiver executado a instância usando uma AMI Do Windows para AWS, o software necessário será instalado automaticamente durante a primeira inicialização. Se tiver executado a instância usando AMIs do Windows que não instalam o software necessário automaticamente, você deverá instalar o software necessário na instância manualmente.

Para instalar o software necessário para o Elastic Graphics (se necessário)

1. Conecte-se à instância.
2. Faça download do Instalador do Elastic Graphics e abra-o. O gerenciador de instalação conecta-se ao endpoint do Elastic Graphics e faz download da versão mais recente do software necessário.

   > **Note**
   >
   > Se o link para baixar não funcionar, tente um navegador diferente ou copie o endereço do link e cole-o em uma nova guia do navegador.

3. Reinicie a instância para verificar.

Verificar a funcionalidade do Elastic Graphics em sua instância

Os pacotes do Elastic Graphics em sua instância incluem ferramentas que você pode usar para visualizar o status do acelerador e verificar se os comandos do OpenGL de sua instância para o acelerador estão funcionais.

Se sua instância foi executada com uma AMI que não tenha os pacotes do Elastic Graphics pré-instalados, você mesmo poderá fazer download e instalá-los. Para ter mais informações, consulte Instalar o software necessário para o Elastic Graphics.

Você pode usar um dos métodos a seguir para verificar a funcionalidade do Elastic Graphics em sua instância.

> **Note**
>
> Se o monitor de status do Elastic Graphics ou a ferramenta da linha de comando retornar um resultado inesperado, consulte Resolver problemas de status não íntegros.

Elastic Graphics status monitor

Você pode usar a ferramenta de monitor de status para visualizar informações sobre o status de um acelerador do Elastic Graphics. Por padrão, essa ferramenta está disponível na área de notificação da barra de tarefas em sua instância do Windows e mostra o status do acelerador gráfico. Os valores possíveis são os seguintes.

Integridade

O acelerador do Elastic Graphics está habilitado e íntegro.

Atualizando

O status do acelerador do Elastic Graphics é em atualização no momento. Pode levar alguns minutos para que o status seja exibido.

Fora de serviço

O acelerador do Elastic Graphics está fora de serviço. Para obter mais informações sobre o erro, escolha Read More (Leia mais).

Elastic Graphics command line tool

É possível usar a ferramenta da linha de comando do Elastic Graphics, `egcli.exe`, para verificar o status do acelerador. Se houver um problema com o acelerador, a ferramenta retornará uma mensagem de erro.

Para executar a ferramenta, abra um prompt de comando em sua instância e execute o seguinte comando:

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

A ferramenta também oferece suporte aos seguintes parâmetros:

`--json`, `-j`

Indica se a mensagem JSON deve ser mostrada. Os valores possíveis são `true` e `false`. O padrão é `true`.

`--imds`, `-i`

Indica se os metadados da instância devem ser verificados para ver a disponibilidade do acelerador. Os valores possíveis são `true` e `false`. O padrão é `true`.

A seguir está um exemplo de saída. O status de `OK` indica que o acelerador está habilitado e íntegro.

```
EG Infrastructure is available.
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6
Instance Type eg1.large
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL
 Redirector)
EG Status: Healthy
JSON Message:
{
  "version": "2016-11-30",
  "status": "OK"
}
```

Os valores possíveis para são os seguinte `status`:

`OK`

O acelerador do Elastic Graphics está habilitado e íntegro.

`UPDATING`

O driver do Elastic Graphics está sendo atualizado.

`NEEDS_REBOOT`

O driver do Elastic Graphics foi atualizado e uma reinicialização da instância do Amazon EC2 é necessária.

`LOADING_DRIVER`

O driver do Elastic Graphics está sendo carregado.

`CONNECTING_EGPU`

O driver do Elastic Graphics está verificando a conectividade com o acelerador do Elastic Graphics.

`ERROR_UPDATE_RETRY`

Ocorreu um erro ao atualizar o driver do Elastic Graphics, uma atualização será tentada novamente em breve.

`ERROR_UPDATE`

Ocorreu um erro irrecuperável ao atualizar o driver do Elastic Graphics.

`ERROR_LOAD_DRIVER`

Ocorreu um erro ao carregar o driver do Elastic Graphics.

`ERROR_EGPU_CONNECTIVITY`

O acelerador do Elastic Graphics está inacessível.

Ver informações do Elastic Graphics

É possível visualizar as informações sobre o acelerador do Elastic Graphics anexado a sua instância.

Para visualizar informações sobre um acelerador do Elastic Graphics (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Na guia Details (Detalhes) , localize o Elastic Graphics ID (ID do Elastic Graphics). Escolha o ID para visualizar as seguintes informações sobre o acelerador do Elastic Graphics:
   - Attachment State (Estado do anexo)
   - Tipo
   - Status de integridade

Para visualizar informações sobre uma aceleradora do Elastic Graphics (AWS CLI)

Você pode usar o comando da AWS CLI describe-elastic-gpus:

```
aws ec2 describe-elastic-gpus
```

Você pode usar o comando describe-network-interfaces da AWS CLI e filtrar por ID de proprietário para visualizar informações sobre a interface de rede do Elastic Graphics.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-
id,Values=amazon-elasticgpus"
```

Para visualizar informações sobre um acelerador do Elastic Graphics (Tools for Windows PowerShell)

Use os seguintes comandos:

- Get-EC2ElasticGpu
- Get-EC2NetworkInterface

Para visualizar informações sobre um acelerador do Elastic Graphics usando metadados da instância

1. Conecte-se à instância do Windows que está usando um acelerador do Elastic Graphics.
2. Execute um destes procedimentos:
   - No PowerShell, use o seguinte cmdlet:

     ```
     PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-
     gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

   - No navegador da Web, cole a seguinte URL no campo de endereço:

     ```
     http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-
     f6d94dfa66df4883b284e96db7397ee6
     ```

Enviar feedback

Você pode enviar comentários sobre sua experiência com o Elastic Graphics para que a equipe possa fazer aperfeiçoamentos adicionais.

Para enviar comentários usando o monitor de status do Elastic Graphics

1. Na área de notificação da barra de tarefas da instância do Windows, abra o monitor de status do Elastic Graphics.
2. No canto inferior esquerdo, escolha Feedback (Comentários).
3. Digite seus comentários e selecione Submit.

Manutenção do Elastic Graphics

> **Important**
>
> O Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.

AWS pode determinar que um acelerador Elastic Graphics está em um estado não íntegro se:

- For necessária uma atualização de segurança ou infraestrutura
- For necessária uma atualização de software
- Houver um problema com o host subjacente

Quando AWS determina que um acelerador do Elastic Graphics está em um estado não íntegro, ele programa o acelerador para desativação. AWS notifica você sobre a aposentadoria pendente do acelerador e fornece as etapas corretivas que você precisa tomar.

Tópicos

- Como serei notificado?
- O que preciso fazer?
- O que acontece quando um acelerador atinge sua data de desativação?

Como serei notificado?

Quando AWS programar um acelerador Elastic Graphics para desativação, ele envia um aviso de desativação do acelerador para o seu AWS Health Dashboard. AWS também envia um email para

o endereço de email associado à sua conta da AWS. Esse é o mesmo endereço de email que você usa para fazer login no AWS Management Console.

> **Note**
>
> Se você usar uma conta de email que não verifique regularmente, use o AWS Health Dashboard para determinar se alguns dos seus aceleradores Elastic Graphics estão programados para desativação. Você também pode alterar as informações de contato da sua conta da AWS na página Account Settings (Configurações da conta).

O aviso de desativação fornece o seguinte:

- O ID da instância à qual o acelerador do está anexado
- Informações sobre o problema que afeta o acelerador
- A data de desativação do acelerador
- As etapas corretivas que você deve tomar

O que preciso fazer?

Quando você for notificado de que o acelerador do Elastic Graphics está programado para desativação, é necessário parar e iniciar a instância à qual o acelerador está anexado, para que o antigo acelerador não íntegro seja substituído por um novo acelerador íntegro.

Recomendamos que você feche aplicações gráficas em execução na instância antes de parar e reiniciar a instância.

> **Important**
>
> Se você não parar e iniciar a instância antes da data de desativação programada, o acelerador associado à instância será parado automaticamente, o que pode fazer com que suas aplicações parem de funcionar.
> Você deve parar e iniciar a instância. A reinicialização da instância não substituirá o acelerador não íntegro por um íntegro.

O que acontece quando um acelerador atinge sua data de desativação?

Quando um acelerador do Elastic Graphics não íntegro atinge sua data de desativação programada, a AWS o termina permanentemente. Para receber uma substituição para o acelerador não íntegro, antes ou depois da data de desativação, você deve parar e iniciar a instância à qual o acelerador está conectado.

Se você não parar e iniciar a instância antes da data de desativação programada, o acelerador associado à instância será parado automaticamente, o que pode fazer com que suas aplicações parem de funcionar.

Usar métricas do CloudWatch para monitorar o Elastic Graphics

> **Important**
>
> O Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.

É possível monitorar o acelerador do Elastic Graphics usando o Amazon CloudWatch, que coleta métricas sobre a performance do acelerador. Essas estatísticas são registradas por um período de duas semanas, para que você possa acessar informações históricas e obter uma perspectiva melhor sobre a performance de seu serviço.

Por padrão, os aceleradores do Elastic Graphics enviam dados de métricas ao CloudWatch em períodos de 5 minutos.

Para obter mais informações sobre o Amazon CloudWatch, consulte o Guia do usuário do Amazon CloudWatch.

Métricas do Elastic Graphics

O namespace `AWS/ElasticGPUs` inclui as seguintes métricas para o Elastic Graphics.

Métrica	Descrição
GPUConnectivityCheckFailed	Informa se a conectividade com o acelerador do Elastic Graphics está ativa ou falhou. Um valor de

Métrica	Descrição
	zero (0) indica que a conexão está ativa. Um valor de um (1) uma falha de conectividade. Unidades: contagem
GPUHealthCheckFailed	Informa se o acelerador do Elastic Graphics foi aprovado na verificação de integridade de status no último minuto. Um valor de zero (0) indica que a verificação de status obteve aprovação. Um valor de um (1) uma falha na verificação de status. Unidades: contagem
GPUMemoryUtilization	A memória da GPU usada. Unidades: MiB

Dimensões do Elastic Graphics

Você pode filtrar os dados de métricas de seus aceleradores do Elastic Graphics usando as seguintes dimensões.

Dimensão	Descrição
`EGPUId`	Filtra os dados pelo acelerador do Elastic Graphics.
`InstanceId`	Filtra os dados pela instância à qual o acelerador do Elastic Graphics está anexado.

Visualizar métricas do CloudWatch para o Elastic Graphics

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, pelas várias dimensões com suporte. Você pode usar os procedimentos a seguir para visualizar as métricas dos aceleradores do Elastic Graphics.

Para visualizar as métricas do Elastic Graphics no console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que o acelerador do Elastic Graphics reside. Para obter mais informações, consulte Regiões e endpoints.
3. No painel de navegação, selecione Metrics (Métricas).
4. Em All metrics (Todas as métricas), selecione Elastic Graphics, Elastic Graphics Metrics (Métricas do Elastic Graphics).

Para visualizar métricas do Elastic Graphics (AWS CLI)

Use o comando list-metrics a seguir:

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Criar alarmes do CloudWatch para monitorar o Elastic Graphics

Você pode criar um alarme do CloudWatch que envia uma mensagem de Amazon SNS quando o alarme mudar de estado. Um alarme observa uma única métrica por um período especificado por você e envia uma notificação para um tópico do Amazon SNS com base no valor da métrica em relação a determinado limite ao longo de vários períodos.

Por exemplo, é possível criar um alarme que monitore a integridade de um acelerador do Elastic Graphics e envie uma notificação quando ocorrer uma falha na verificação de integridade do acelerador gráfico por três períodos consecutivos de cinco minutos.

Para criar um alarme para o status de integridade de um acelerador do Elastic Graphics

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarms, Create Alarm.
3. Escolha Select metric (Selecionar métrica), Elastic Graphics, Elastic Graphics Metrics (Métricas do Elastic Graphics).
4. Selecione a métrica GPUHealthCheckFailed e escolha Select metric (Selecionar métrica).
5. Configure o alarme desta forma:

    a. Em Alarm details (Detalhes do alarme), digite um nome e uma descrição para o alarme. Em Whenever (Sempre), escolha >= e digite 1.

b. Em Actions (Ações), selecione uma lista de notificações existente ou escolha New list (Nova lista).

c. Escolha Create Alarm.

Solução de problemas

> **Important**
>
> O Amazon Elastic Graphics chegou ao fim da vida útil em 8 de janeiro de 2024. Para workloads que precisam de aceleração gráfica, recomendamos que você use instâncias G4ad, G4dn ou G5 do Amazon EC2.

Veja a seguir erros comuns e etapas de solução de problemas.

Sumário

- Investigar problemas na performance da aplicação
  - Problemas de performance na renderização do OpenGL
  - Problemas na performance do acesso remoto
- Resolver problemas de status não íntegros
  - Verifique a configuração da instância
  - Interromper e iniciar a instância
  - Verificar os componentes instalados
  - Verificar os logs do Elastic Graphics
- Por que estou vendo várias ENIs?

Investigar problemas na performance da aplicação

O Elastic Graphics usa a rede de instâncias para enviar comandos OpenGL a uma placa gráfica remotamente anexada. Além disso, um desktop que executa uma aplicação OpenGL com um acelerador do Elastic Graphics geralmente é acessado usando uma tecnologia de acesso remoto. É importante distinguir entre um problema de performance relativo à renderização do OpenGL ou à tecnologia de acesso remoto da área de trabalho.

Problemas de performance na renderização do OpenGL

A performance da renderização do OpenGL é determinada pelo número de comandos e quadros do OpenGL gerados na instância remota.

A performance da renderização pode variar dependendo dos seguintes fatores:

- Performance do acelerador do Elastic Graphics
- Performance da rede
- Performance da CPU
- Modelo de renderização, complexidade do cenário
- Comportamento da aplicação OpenGL

Uma maneira fácil de avaliar a performance é exibir o número de quadros renderizados na instância remota. As aceleradoras do Elastic Graphics exibem um máximo de 25 quadros por segundo na instância remota para obter a melhor qualidade percebida e, ao mesmo tempo, reduzir o uso da rede.

Para mostrar o número de quadros produzidos

1. Abra o arquivo a seguir em um editor de texto. Se o arquivo não existir, crie-o.

   ```
   C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
   ```

2. Identifique a seção `[Application]`, ou adicione-a se não estiver presente, e adicione o seguinte parâmetros de configuração:

   ```
   [Application]
   show_fps=1
   ```

3. Reinicie a aplicação e verifique o FPS novamente.

Se os quadros/s atingirem 15 a 25 quadros/s ao atualizar a cena renderizada, o acelerador do Elastic Graphics estará executando em pico. Qualquer outro problema de performance percebido provavelmente estará relacionado ao acesso remoto no computador da instância. Se esse for o caso, consulte a seção Problemas de performance do acesso remoto.

Se o número de FPS for menor que 15, você pode testar o seguinte:

- Melhore a performance do acelerador do Elastic Graphics selecionando um tipo de acelerador gráfico mais potente.
- Melhore a performance geral da rede usando estas dicas:
  - Verifique a quantidade de largura de banda de entrada e de saída do endpoint do acelerador do Elastic Graphics. O endpoint do acelerador do Elastic Graphics pode ser recuperado com o seguinte comando do PowerShell:

    ```
    PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/
    associations/[ELASTICGPU_ID]).content
    ```

  - O tráfego de rede da instância para o endpoint do acelerador do Elastic Graphics é relacionado ao volume de comandos que a aplicação OpenGL está produzindo.
  - O tráfego de rede do endpoint do acelerador do Elastic Graphics para a instância está relacionado ao número de quadros gerados pelo acelerador gráfico.
  - Caso perceba que o uso da rede está alcançando o throughput máximo da rede para as instâncias, tente usar uma instância com uma variação maior no throughput da rede.
- Melhore a performance da CPU:
  - As aplicações podem exigir muitos recursos da CPU além do que o acelerador do Elastic Graphics precisa. Se o Gerenciador de Tarefas do Windows estiver informando um uso elevado dos recursos da CPU, tente usar uma instância com mais potência de CPU.

Problemas na performance do acesso remoto

Uma instância com um acelerador do Elastic Graphics anexado pode ser acessada usando diferentes tecnologias de acesso remoto. A performance e a qualidade podem variar dependendo:

- Da tecnologia de acesso remoto
- Performance da instância
- Performance do cliente
- Latência e largura de banda de rede entre o cliente e a instância

Possíveis opções para o protocolo de acesso remoto incluem:

- Conexão de área de trabalho remota da Microsoft
- NICE DCV

- VNC

Para obter mais informações sobre otimização, consulte o protocolo específico.

Resolver problemas de status não íntegros

Se o acelerador do Elastic Graphics estiver em um estado não íntegro, use as etapas de solução de problemas a seguir para resolver o problema.

Verifique a configuração da instância

Se a ferramenta da linha de comando do Elastic Graphics, `egcli.exe`, retornar uma saída semelhante à saída abaixo, certifique-se de que o grupo de segurança esteja configurado corretamente e que você executou a instância com o serviço de metadados da instância habilitado.

```
EG Version 1.0.7.4240 (Manager) / N/A (OpenGL Library) / N/A (OpenGL Redirector)
EG Status: Out Of Service
Something prevented the EG Infrastructure to work properly.
```

Interromper e iniciar a instância

Se o acelerador do Elastic Graphics estiver em um estado não íntegro, parar a instância e reiniciá-la é a opção mais simples. Para obter mais informações, consulte Início e interrupção manuais das instâncias.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Verificar os componentes instalados

Abra o Painel de Controle do Windows e confirme se os seguintes componentes estão instalados:

- Gerenciador do Amazon Elastic Graphics
- Biblioteca de OpenGL do Amazon Elastic Graphics
- Redirecionador de OpenGL para GPUs elásticas do Amazon EC2

Se qualquer um desses itens estiver ausente, você deve instalá-lo manualmente. Para obter mais informações, consulte Instalar o software necessário para o Elastic Graphics.

Verificar os logs do Elastic Graphics

Abra o Visualizador de eventos do Windows, expanda a seção Application and Services Logs (Logs de aplicações e de serviços) e pesquise por erros nos seguintes logs de eventos:

- EC2ElasticGPUs
- GUI do EC2ElasticGPUs

Por que estou vendo várias ENIs?

Ao chamar StartInstances em uma instância do EC2 com um acelerador Elastic Graphics, uma nova interface de rede elástica (ENI) é criada na instância para permitir que comandos OpenGL sejam enviados para a placa gráfica conectada remotamente.

Se você chamar StartInstances muitas vezes em um curto período de tempo (alguns segundos ou menos) na mesma instância do EC2, uma nova interface de rede será criada em cada chamada. No entanto:

- Somente uma interface de rede será usada pelo acelerador do Elastic Graphics.
- Interfaces de rede extras não incorrem em nenhum custo e serão lançadas automaticamente em 24 horas.

Instale o WSL em sua instância do Windows

O Subsistema do Windows para Linux (WSL) é um download gratuito que pode ser instalado na sua instância do Windows. Ao instalar o WSL, você pode executar ferramentas de linha de comando do Linux diretamente na sua instância do Windows e usar as ferramentas do Linux para o desenvolvimento de scripts, junto com a sua área de trabalho tradicional do Windows. Você pode alternar facilmente entre Linux e Windows em uma única instância do Windows, o que pode ser útil em um ambiente de desenvolvimento.

Para obter mais informações sobre o WSL, consulte a Documentação do Subsistema Windows para Linux no site do Microsoft Build.

Limitações

- O WSL está disponível em duas versões: WSL 1 e WSL 2.
  - Para instâncias `.metal` do EC2, você pode instalar o WSL 1 ou o WSL 2.
  - Para instâncias virtualizadas do EC2, você deve instalar o WSL 1.
- Para sistemas operacionais do Windows Server, o WSL só pode ser instalado em instâncias que executam o seguinte:
  - Windows Server 2019
  - Windows Server 2022

Instalar o WSL

As instruções a seguir instalam o WSL em uma instância do EC2 que esteja executando o Windows Server 2022. Para obter instruções sobre como instalar o WSL em uma instância do EC2 que esteja executando o Windows Server 2019, consulte Instalação do WSL em versões anteriores do Windows Server no site da Microsoft. Depois de seguir essas instruções, será possível usar a etapa 3 nas instruções abaixo para configurar o WSL para usar o WSL 1.

Instalar o WSL 1

1. Para instalar o WSL, execute o seguinte comando de instalação padrão em sua instância do EC2, mas certifique-se de habilitar o WSL 1 ao incluir `--enable-wsl1`. O WSL 2 é instalado por padrão. Se sua instância foi executada usando um tipo de instância virtualizada, você deve concluir a etapa 3 deste procedimento para definir a versão como WSL 1.

   ```
   wsl --install --enable-wsl1 --no-launch
   ```

2. Reinicie sua instância do EC2.

   ```
   shutdown -r -t 20
   ```

3. Para configurar o WSL a usar o WSL 1, execute o comando a seguir na sua instância. Para obter mais informações sobre como definir a versão WSL, consulte Etapas de instalação manual para versões mais antigas do WSL no site do Microsoft Build.

   ```
   wsl --set-default-version 1
   ```

4. Instale a distribuição padrão.

```
wsl --install
```

Instalar o WSL 2

- Para instalar o WSL, execute o comando de instalação padrão a seguir em sua instância do EC2. O WSL 2 é instalado por padrão. Se você estiver instalando o WSL em uma instância `.metal`, esta é a única etapa a ser executada.

  ```
  wsl --install
  ```

  Para obter mais informações, consulte Instalar o Linux no Windows com o WSL no site do Microsoft Build.

Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server.

Há dois métodos para atualizar uma versão anterior do Windows Server em execução em uma instância: atualização local e migração (também denominada atualização lado a lado). Uma atualização local atualiza os arquivos do sistema operacional, enquanto as configurações e os arquivos pessoais ficam intactos. A migração envolve a captura de configurações, as configurações, os dados e a portabilidade dos mesmos para um sistema operacional mais recente em uma nova instância do Amazon EC2.

A Microsoft recomenda tradicionalmente a migração para uma versão mais recente do Windows Server em vez de atualizá-lo. A migração pode resultar em menos erros ou problemas de atualização, mas pode demorar mais do que uma atualização local devido à necessidade de provisionar uma nova instância, planejar e fazer a portabilidade de aplicações e ajustar as configurações na nova instância. Uma atualização local pode ser mais rápida, mas incompatibilidades de software podem produzir erros.

Conteúdo

- Execução de uma atualização local na instância do Windows
- Execução de uma atualização automatizada na instância do Windows
- Migração de uma instância do Windows para um tipo de instância da geração atual

- Assistente de redefinição de plataforma Windows para Linux para bancos de dados Microsoft SQL Server
- Solução de problemas de atualização em uma instância do Windows

Execução de uma atualização local na instância do Windows

Para executar uma atualização local, é necessário determinar quais drivers de rede a instância está executando. Os drivers de rede PV permitem que você acesse sua instância usando o Desktop Remoto. As instâncias usam drivers PV da AWS, do adaptador de rede Intel ou da rede avançada. Para ter mais informações, consulte Drivers paravirtuais para as instâncias do Windows.

Antes de iniciar uma atualização no local

Execute as seguintes tarefas e observe os seguintes detalhes importantes antes de começar a atualização local.

- Leia a documentação da Microsoft para compreender os requisitos de atualização, os problemas conhecidos e as restrições. Além disso, leia as instruções oficiais de atualização.
  - Opções de atualização para Windows Server 2012
  - Opções de atualização para Windows Server 2012 R2
  - Opções de atualização e conversão para Windows Server 2016
  - Opções de atualização e conversão para Windows Server 2019
  - Opções de atualização e conversão para Windows Server 2022
  - Centro de Atualização do Windows Server
- Recomendamos a execução de uma atualização do sistema operacional em instâncias com pelo menos 2 vCPUs e 4 GB de RAM. Se necessário, é possível alterar a instância para um tamanho maior do mesmo tipo (t2.small para t2.large, por exemplo), executar a atualização e redimensioná-la de volta para o tamanho original. Se você precisar manter o tamanho da instância, poderá monitorar o progresso usando o instance console screenshot. Para ter mais informações, consulte Alterar o tipo de instância.
- Verifique se o volume raiz de sua instância do Windows tem espaço em disco suficiente. O processo de configuração do Windows poderá não avisá-lo sobre espaço em disco insuficiente. Para obter informações sobre a quantidade de espaço em disco que é necessária para atualizar um sistema operacional específico, consulte a documentação da Microsoft. Se o volume não tiver espaço suficiente, é possível expandi-lo. Para obter mais informações, consulte Volumes Elásticos do Amazon EBS no Guia do usuário do Amazon EBS.

- Determine seu caminho de atualização. É necessário atualizar o sistema operacional para a mesma arquitetura. Por exemplo, atualize um sistema de 32 bits para um sistema de 32 bits. O Windows Server 2008 R2 e posterior são apenas 64 bits.
- Desabilite o software antivírus e antispyware e os firewalls. Esses tipos de software podem entrar em conflito com o processo de atualização. Habilite novamente o software antivírus e antispyware e os firewalls quando a atualização for concluída.
- Atualize para os drivers mais recentes, conforme descrito em Migração de uma instância do Windows para um tipo de instância da geração atual.
- O Upgrade Helper Service só oferece suporte a instâncias que estejam executando drivers Citrix PV. Se a instância estiver executando drivers Red Hat, atualize manualmente esses drivers primeiro.

Atualizar uma instância no local com AWS PV, adaptador de rede Intel ou drivers de rede avançada

Use o seguinte procedimento para atualizar uma instância do Windows Server usando AWS PV, adaptador de rede Intel ou drivers de rede avançada.

Para executar a atualização local

1. Crie uma AMI do sistema que você planeja atualizar para fins de backup ou teste. Em seguida, é possível fazer a atualização na cópia a fim de simular um ambiente de teste. Se a atualização for concluída, será possível alternar o tráfego para essa instância com um período de inatividade curto. Se ocorrer falha na atualização, será possível reverter para o backup. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
2. Verifique se a instância do Windows Server está usando os drivers de rede mais recentes.
    a. Para atualizar seu driver do AWS PV, consulte Atualizar drivers de PV em instâncias do Windows.
    b. Para atualizar seu driver do ENA, consulte Instalação do driver do Adaptador de Rede Elástica (ENA).
    c. Para atualizar seus drivers da Intel, consulte Habilitação de redes aperfeiçoadas com a interface Intel 82599 VF nas instâncias do EC2.
3. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

4. No painel de navegação, escolha Instances (Instâncias). Localize a instância. Anote o ID da instância e o ID da zona de disponibilidade da instância. Você precisará dessas informações mais tarde neste procedimento.
5. Se você estiver atualizando o Windows Server 2012 ou 2012 R2 para o Windows Server 2016, 2019 ou 2022, faça o seguinte na instância antes de continuar:
   a. Desinstale o serviço EC2Config. Para ter mais informações, consulte Interromper, reiniciar, excluir ou desinstalar o EC2Config.
   b. Instale o EC2Launch v1 ou o agente EC2Launch v2. Para obter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch e Configurar uma instância do Windows usando o EC2Launch v2.
   c. Instalar o SSM Agent do AWS Systems Manager. Para obter mais informações, consulte Trabalho com o SSM Agent no Guia do usuário do AWS Systems Manager.
6. Crie um o novo volume de um snapshot de mídia de instalação do Windows Server.
   a. No painel de navegação à esquerda, em Elastic Block Store, escolha Snapshots.
   b. Na barra do filtro, escolha Snapshots públicos.
   c. Na barra de pesquisa, especifique os seguintes filtros:
      - Escolha Alias do proprietário, depois = e depois amazon.
      - Escolha Descrição e comece a digitar **`Windows`**. Selecione o filtro do Windows que corresponde à arquitetura do sistema e à preferência de idioma para as quais você está fazendo a atualização. Por exemplo, escolha Windows 2019 English Installation Media para fazer a atualização para o Windows Server 2019.
   d. Marque a caixa de seleção ao lado do snapshot que corresponde à arquitetura do sistema e à preferência de idioma para a qual você está fazendo a atualização e, em seguida, escolha Ações, Criar volume com base no snapshot.
   e. Na página Criar volume, escolha a zona de disponibilidade que corresponde à instância do Windows e escolha Criar volume.
7. No banner Volume vol-***`1234567890example`*** criado com êxito na parte superior da página, escolha o ID do volume que você acabou de criar.
8. Escolha Actions (Ações), Attach volume (Anexar volume).
9. Na página Anexar volume, em Instância, selecione o ID da instância do Windows e, em seguida, escolha Anexar volume.

10. Disponibilize o novo volume para uso ao seguir as etapas apresentadas em Make an Amazon EBS volume available for use.

> **Important**
>
> Não inicialize o disco porque isso excluirá os dados existentes.

11. No Windows PowerShell, mude para a nova unidade de volume. Comece a atualização abrindo o volume de mídia de instalação que você anexou à instância.

    a. Se você estiver fazendo a atualização para o Windows Server 2016 ou posterior, execute o seguinte:

    ```
    .\setup.exe /auto upgrade /dynamicupdate disable
    ```

    > **Note**
    >
    > Executar setup.exe com a opção `/dynamicupdate` definida como desabilitada impede que o Windows instale atualizações durante o processo de upgrade do Windows Server, pois a instalação de atualizações durante o upgrade pode causar falhas. Você poderá instalar atualizações com o Windows Update após a conclusão do upgrade.

    Se você estiver fazendo a atualização para uma versão anterior do Windows Server, execute o seguinte:

    ```
    Sources\setup.exe
    ```

    b. Em Select the operating system you want to install, selecione o SKU de instalação completa da instância do Windows Server e escolha Next.

    c. Em Which type of installation do you want? (Qual tipo de instalação deseja?), escolha Upgrade (Atualizar).

    d. Assista todo o assistente.

A configuração do Windows Server copia e processa os arquivos. Após alguns minutos, sua sessão do Remote Desktop será encerrada. O tempo necessário para concluir a atualização depende do

número de aplicações e das funções de servidor em execução na instância do Windows Server. O processo de atualização pode levar 40 minutos ou várias horas. A instância apresentará falha nas verificações de status 1 e 2 durante o processo de atualização. Quando a atualização for concluída, as duas verificações de status ocorrerão com êxito. É possível verificar no log do sistema a saída do console ou usar as métricas do Amazon CloudWatch para a atividade do disco e da CPU a fim de determinar se a atualização está em andamento.

> **Note**
>
> Se você estiver fazendo a atualização para o Windows Server 2019, depois que a atualização for concluída, será possível alterar a tela de fundo do desktop manualmente para remover o nome do sistema operacional anterior, se desejado.

Se a instância não passou nas duas verificações de status após várias horas, consulte Solução de problemas de atualização em uma instância do Windows.

Tarefas de pós-atualização

1. Inicie a sessão na instância para iniciar uma atualização do .NET Framework e reinicializar o sistema quando solicitado.
2. Se ainda não tiver feito isso em uma etapa anterior, instale o agente do EC2Launch v1 ou do EC2Launch v2. Para obter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch e Configurar uma instância do Windows usando o EC2Launch v2.
3. Se você fez a atualização para o Windows Server 2012 R2, recomendamos atualizar os drivers PV para drivers AWS PV. Caso tenha atualizado em uma instância baseada em Nitro, recomendamos a instalação ou atualização dos drivers NVME e ENA. Para obter mais informações, consulte Windows Server 2012 R2, Instalar ou atualizar drivers AWS NVMe usando o PowerShell ou Habilitar redes avançadas no Windows.
4. Habilite novamente o software antivírus e antispyware e os firewalls.

Execução de uma atualização automatizada na instância do Windows

É possível executar uma atualização automatizada de suas instâncias do Windows e do SQL Server na AWS com runbooks do AWS Systems Manager Automation.

Conteúdo

- Serviços relacionados
- Opções de execução
- Atualizar o Windows Server
- Atualização do SQL Server

Serviços relacionados

Os seguintes serviços da AWS são usados no processo de atualização automatizada:

- AWS Systems Manager. O AWS Systems Manager é uma interface poderosa e unificada para gerenciar centralmente seus recursos da AWS. Para obter mais informações, consulte o Guia do usuário do AWS Systems Manager.
- O AWS Systems Manager Agent (SSM Agent) é um software da Amazon que pode ser instalado e configurado em uma instância do Amazon EC2, em um servidor on-premises ou em uma máquina virtual (VM). O SSM Agent permite que o Systems Manager atualize, gerencie e configure esses recursos. O agente processa as solicitações do serviço do Systems Manager na Nuvem AWS e as executa conforme especificado na solicitação. Para obter mais informações, consulte Trabalho com o SSM Agent no Guia do usuário do AWS Systems Manager.
- Runbooks do AWS Systems Manager SSM. Um runbook do SSM define as ações que o Systems Manager realiza nas suas instâncias gerenciadas. Os runbooks do SSM usam JavaScript Object Notation (JSON) ou YAML e incluem etapas e parâmetros especificados por você. Esse tópico usa dois runbooks do SSM do Systems Manager para automação. Para obter mais informações, consulte Referência de runbook do AWS Systems Manager Automation no Guia do usuário do AWS Systems Manager.

Opções de execução

Ao selecionar Automation (Automação) no console do Systems Manager, selecione Execute (Executar). Depois de selecionar um documento de automação, você será solicitado a escolher uma opção de execução da automação. É possível escolher entre as opções a seguir. Nas etapas dos caminhos fornecidos neste tópico, usamos a opção Simple execution (Execução simples).

Execução simples

Escolha esta opção se deseja atualizar uma única instância, mas não deseja passar por cada etapa de automação para auditar os resultados. Tal opção é explicada com mais detalhes nas etapas de atualização a seguir.

Rate control (Controle de taxa)

Escolha esta opção se você deseja aplicar a atualização a mais de uma instância. Defina as configurações a seguir.

- Parâmetro

  Essa configuração, que também é definida nas configurações Multi-Account and Region (Várias contas e região), define como sua automação se expande.

- Destinos

  Selecione o destino ao qual você deseja aplicar a automação. Essa configuração também é definida nas configurações Multi-Account and Region (Várias contas e região).

- Valores de parâmetros

  Use os valores definidos nos parâmetros do documento de automação.

- Grupo de recursos

  Na AWS , um recurso é uma entidade com a qual é possível trabalhar. Os exemplos incluem instâncias do Amazon EC2, pilhas do AWS CloudFormation ou buckets do Amazon S3. Se você trabalha com vários recursos, pode ser útil gerenciá-los como um grupo, em vez de migrar de um serviço da AWS para outro em todas as tarefas. Em alguns casos, é possível querer gerenciar um grande número de recursos relacionados, como instâncias do EC2 que compõem uma camada de aplicação. Nesse caso, você provavelmente precisará realizar ações em massa nesses recursos ao mesmo tempo.

- Tags

  As tags ajudam a categorizar os recursos da AWS de diferentes maneiras, como por finalidade, por proprietário ou por ambiente. Essa categorização é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico usando as tags atribuídas.

- Rate Control (Controle de taxa)

  A opção Rate Control (Controle de taxa) também é definida nas configurações Multi-Account and Region (Várias contas e região). Ao definir os parâmetros de controle de taxa, você define a quanto da sua frota a automação será aplicada, seja por contagem de alvos ou por porcentagem da frota.

Multi-Account and Region (Várias contas e região)

Além dos parâmetros especificados em Rate Control (Controle de taxa), que também são usados nas configurações Multi-Account and Region (Várias contas e região), há duas configurações adicionais:

- Contas e unidades organizacionais (UOs)

  Especifique várias contas nas quais você deseja executar a automação.
- Regiões da AWS

  Especifique várias Regiões da AWS nas quais você deseja executar a automação.

Execução manual

Esta opção é semelhante a Simple execution (Execução simples), mas permite percorrer cada etapa de automação e auditar os resultados.

Atualizar o Windows Server

O runbook `AWSEC2-CloneInstanceAndUpgradeWindows` cria uma imagem de máquina da Amazon (AMI) usando uma instância do Windows Server na sua conta e atualiza essa AMI para uma versão com suporte de sua escolha. Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Existem duas AMIs incluídas no processo de atualização automatizada:

- Instância atual em execução. A primeira AMI é a instância em execução atual, que não é atualizada. Essa AMI é usada para iniciar outra instância para executar a atualização no local. Quando o processo é concluído, essa AMI é excluída da sua conta, a menos que você solicite especificamente que a instância original seja mantida. Essa configuração é tratada pelo parâmetro `KeepPreUpgradeImageBackUp` (o valor padrão é `false`, o que significa que a AMI é excluída por padrão).
- AMI atualizada. Esta AMI é o resultado do processo de automação.

O resultado final é uma AMI, que é a instância atualizada da AMI.

Quando a atualização estiver concluída, será possível testar a funcionalidade da sua aplicação iniciando a nova AMI na sua Amazon VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade da aplicação antes de mudar completamente para a instância atualizada.

Pré-requisitos

Para automatizar a atualização do seu Windows Server com o documento do AWS Systems Manager Automation, é necessário executar as seguintes tarefas:

- Criar uma função do IAM com as políticas do IAM especificadas para permitir que o Systems Manager execute tarefas de automação nas suas instâncias do Amazon EC2 e verifique se você atende aos pré-requisitos para usar o Systems Manager. Para obter mais informações, consulte Criação de uma função para delegar permissões a um serviço da AWS no Guia do usuário do AWS Identity and Access Management.
- Selecione a opção de como você deseja que a automação seja executada. As opções para execução são Simple execution (Execução simples), Rate control (Controle de taxa), Multi-account and Region (Várias contas e região) e Manual execution (Execução manual). Para obter mais informações sobre essas opções, consulte Opções de execução.
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em instâncias do Amazon EC2 no Windows Server.
- O Windows PowerShell 3.0 ou posterior deve ser instalado em sua instância.
- Para instâncias ingressadas em um domínio do Microsoft Active Directory, é recomendável especificar um `SubnetId` que não tenha conectividade com seus controladores de domínio para ajudar a evitar conflitos de nome de host.
- A sub-rede da instância deve ter conectividade de saída com a Internet, o que fornece acesso a Serviços da AWS, como o Amazon S3, e acesso para baixar correções da Microsoft. Esse requisito será atendido se a sub-rede for pública e a instância tiver um endereço IP público ou se a sub-rede for uma sub-rede privada com uma rota que envie o tráfego da Internet para um dispositivo NAT público.
- Essa automação funciona com instâncias que executam o Windows Server 2008 R2, o Windows Server 2012 R2, o Windows Server 2016 e o Windows Server 2019.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização.
- Se a instância não usar uma licença do Windows fornecida pela AWS, especifique um ID de snapshot do Amazon EBS que inclua a mídia de instalação do Windows Server 2012 R2. Para fazer isso:
  1. Verifique se a instância do Amazon EC2 está executando o Windows Server 2012 ou posterior.
  2. Crie um volume do Amazon EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.

3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
5. Crie um snapshot do Amazon EBS do volume de 6 GB criado na etapa 2 acima.

Limitações de atualização do Windows Server

Essa automação não oferece suporte para a atualização de controladores de domínio do Windows, clusters ou sistemas operacionais de desktop do Windows. Além disso, essa automação não oferece suporte a instâncias do Amazon EC2 para Windows Server com as seguintes funções instaladas:

- Host de sessão de área de trabalho remota (RDSH)
- Agente de conexão de área de trabalho remota (RDCB)
- Host de virtualização de área de trabalho remota (RDVH)
- Acesso via Web à Área de Trabalho Remota (RDWA)

Etapas para executar uma atualização automatizada do Windows Server

Siga estas etapas para atualizar sua instância do Windows Server usando o runbook de automação AWSEC2-CloneInstanceAndUpgradeWindows.

1. Abra o Systems Manager no Console de Gerenciamento da AWS.
2. No painel de navegação à esquerda, em Change Management (Gerenciamento de alterações), escolha Automation (Automação).
3. Escolha Execute automation.
4. Procure o documento de automação chamado `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Quando o nome do documento aparecer, selecione-o. Ao selecioná-lo, os detalhes do documento aparecerão.
6. Selecione Execute automation (executar automação) para introduzir os parâmetros desse documento. Deixe Simple execution (Execução simples) selecionada na parte superior da página.
7. Insira os parâmetros solicitados com base na orientação a seguir.

   - `InstanceID`

Tipo: string

(Obrigatório) A instância que executa o Windows Server 2008 R2, 2012 R2, 2016 or 2019 w com o SSM Agent instalado.

- `InstanceProfile`.

  Tipo: string

  (Obrigatório) O perfil da instância do IAM. Essa é a função do IAM usada para executar a automação do Systems Manager em relação à instância do Amazon EC2 e às AMIs da AWS. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager no Manual do usuário do AWS Systems Manager.

- `TargetWindowsVersion`

  Tipo: string

  (Obrigatório) Selecione a versão de destino do Windows.

- `SubnetId`

  Tipo: string

  (Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

- `KeepPreUpgradedBackUp`

  Tipo: string

  (Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: string

  (Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

8. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, será possível monitorar o progresso da execução.
9. Quando a automação for concluída, você verá o ID da AMI. É possível iniciar a AMI para verificar se o sistema operacional Windows está atualizado.

> **Note**
>
> Não é necessário que a automação execute todas as etapas. As etapas são condicionais com base no comportamento da automação e da instância. O Systems Manager pode pular algumas etapas que não são obrigatórias.
> Além disso, algumas etapas podem expirar. O Systems Manager tenta atualizar e instalar todos os patches mais recentes. Às vezes, porém, os patches expiram com base em uma configuração de tempo limite definida para a etapa especificada. Quando isso acontece, a automação do Systems Manager segue para a próxima etapa para garantir que o sistema operacional interno seja atualizado para a versão do Windows Server de destino.

10. Após a conclusão da automação, é possível iniciar uma instância do Amazon EC2 usando o ID da AMI para revisar sua atualização. Para obter mais informações sobre como criar uma instância do Amazon EC2 usando uma AMI da AWS, consulte Como iniciar uma instância do EC2 a partir de uma AMI personalizada?

Atualização do SQL Server

O script `AWSEC2-CloneInstanceAndUpgradeSQLServer` cria uma AMI de uma instância do Amazon EC2 executando o SQL Server em sua conta e atualiza a AMI para uma versão posterior do SQL Server. Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Nesse fluxo de trabalho, a automação cria uma AMI da instância e inicia a nova AMI na sub-rede que você fornecer. A automação, então, executa uma atualização local do SQL Server. Após a conclusão da atualização, a automação cria uma nova AMI antes de encerrar a instância atualizada.

Existem duas AMIs incluídas no processo de atualização automatizada:

- Instância atual em execução. A primeira AMI é a instância em execução atual, que não é atualizada. Essa AMI é usada para iniciar outra instância para executar a atualização no local. Quando o processo é concluído, essa AMI é excluída da sua conta, a menos que você solicite especificamente que a instância original seja mantida. Essa configuração é tratada pelo parâmetro

`KeepPreUpgradeImageBackUp` (o valor padrão é `false`, o que significa que a AMI é excluída por padrão).

- AMI atualizada. Esta AMI é o resultado do processo de automação.

O resultado final é uma AMI, que é a instância atualizada da AMI.

Quando a atualização estiver concluída, será possível testar a funcionalidade da sua aplicação iniciando a nova AMI na sua Amazon VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade da aplicação antes de mudar completamente para a instância atualizada.

Pré-requisitos

Para automatizar a atualização do seu SQL Server com o documento do AWS Systems Manager Automation, é necessário executar as seguintes tarefas:

- Criar uma função do IAM com as políticas do IAM especificadas para permitir que o Systems Manager execute tarefas de automação nas suas instâncias do Amazon EC2 e verifique se você atende aos pré-requisitos para usar o Systems Manager. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do AWS Identity and Access Management.
- Selecione a opção de como você deseja que a automação seja executada. As opções para execução são Simple execution (Execução simples), Rate control (Controle de taxa), Multi-account and Region (Várias contas e região) e Manual execution (Execução manual). Para obter mais informações sobre essas opções, consulte Opções de execução.
- A instância do Amazon EC2 deve usar o Windows Server 2008 R2 ou posterior and o SQL Server 2008 ou posterior.
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Trabalho com o SSM Agent em instâncias do Amazon EC2 para Windows Server.
- Verifique se a instância tem espaço em disco suficiente:
  - Se estiver atualizando do Windows Server 2008 R2 para o 2012 R2 ou do Windows Server 2012 R2 para um sistema operacional posterior, verifique se você tem 20 GB de espaço livre no disco de inicialização da instância.
  - Se estiver atualizando do Windows Server 2008 R2 para o 2016 ou posterior, verifique se a instância tem 40 GB de espaço livre no disco de inicialização da instância.

- Para instâncias que usam uma versão Traga sua própria licença (BYOL) do SQL Server, os seguintes pré-requisitos adicionais se aplicam:
  - Forneça um ID de snapshot do Amazon EBS que inclua a mídia de instalação do SQL Server desejado. Para fazer isso:
    1. Verifique se a instância do Amazon EC2 está executando o Windows Server 2008 R2 ou posterior.
    2. Crie um volume do Amazon EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
    3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
    4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
    5. Crie um snapshot do Amazon EBS do volume de 6 GB criado na etapa 2.

Limitações da atualização automatizada do SQL Server

As seguintes limitações se aplicam ao usar o runbook AWSEC2-CloneInstanceAndUpgradeSQLServer para realizar uma atualização automatizada:

- A atualização só pode ser realizada em um SQL Server usando a autenticação do Windows.
- Verifique se há atualizações de patch de segurança pendentes nas instâncias. Abra Control Panel (Painel de controle) e, em seguida, escolha Check for updates (Verificar atualizações).
- Implantações do SQL Server no modo HA e espelhamento não são compatíveis.

Etapas para executar uma atualização automatizada do SQL Server

Siga estas etapas para atualizar sua instância do SQL Server usando o runbook de automação AWSEC2-CloneInstanceAndUpgradeSQLServer.

1. Se isso ainda não foi feito, faça download do arquivo .iso do SQL Server 2016 e monte-o no servidor de origem.
2. Após a montagem do arquivo .iso, copie todos os arquivos do componente e coloque-os em qualquer volume de sua escolha.

3. Faça um snapshot do volume do Amazon EBS e copie o ID do snapshot em uma área de transferência para uso posterior. Para obter mais informações, consulte Create Amazon EBS snapshots no Guia do usuário do Amazon EBS.
4. Anexe o perfil da instância à instância de origem do Amazon EC2. Isso permite que o Systems Manager se comunique com a instância do EC2 e execute comandos nele depois que ele é adicionado ao serviço do AWS Systems Manager. Para esse exemplo, nomeamos a função `SSM-EC2-Profile-Role` com a política `AmazonSSMManagedInstanceCore` anexada à função. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager no Guia do usuário do AWS Systems Manager.
5. No console do AWS Systems Manager, no painel de navegação à esquerda, selecione Managed Instances (Instâncias gerenciadas). Verifique se sua instância do EC2 está na lista de instâncias gerenciadas. Se você não vir a instância depois de alguns minutos, leia Onde estão minhas instâncias? no Guia do usuário do AWS Systems Manager.
6. No painel de navegação à esquerda, em Change Management (Gerenciamento de alterações), escolha Automation (Automação).
7. Escolha Execute automation.
8. Procure o documento de automação chamado `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Escolha documento do SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer` e selecione Next (Avançar).
10. Verifique se a opção Simple execution (Execução simples) está selecionada.
11. Insira os parâmetros solicitados com base na orientação a seguir.

    - `InstanceId`

      Tipo: string

      (Obrigatório) A instância executando o SQL Server 2008 R2 (ou posterior).

    - `IamInstanceProfile`

      Tipo: string

      (Obrigatório) O perfil da instância do IAM.

    - `SQLServerSnapshotId`

      Tipo: string

(Obrigatório) O ID do snapshot para a mídia de instalação do SQL Server de destino. Esse parâmetro não é necessário para instâncias incluídas na licença do SQL Server.

- `SubnetId`

  Tipo: string

  (Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

- `KeepPreUpgradedBackUp`

  Tipo: string

  (Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: string

  (Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

- `TargetSQLVersion`

  Tipo: string

  (Opcional) A versão do SQL Server de destino. O padrão é `2016`.

12. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, será possível monitorar o progresso da execução.
13. Quando Execution status (Status de execução) mostrar Success (Sucesso), expanda Outputs (Saídas) para visualizar as informações da AMI. É possível usar o ID da AMI para iniciar sua instância do SQL Server para a VPC de sua escolha.
14. Abra o console do Amazon EC2. No painel de navegação à esquerda, selecione AMIs. É necessário ver a nova AMI.
15. Para verificar se a nova versão do SQL Server foi instalada com êxito, selecione a nova AMI e escolha Launch (Iniciar).

16. Escolha o tipo de instância que você deseja para a AMI, a VPC e a sub-rede que você deseja implantar e o armazenamento que deseja usar. Como você está lançando a nova instância de uma AMI, os volumes são apresentados como uma opção para incluir na nova instância do EC2 que você está executando. É possível remover qualquer um desses volumes ou adicionar volumes.
17. Adicione uma tag para ajudar você a identificar sua instância.
18. Adicione o grupo de segurança ou grupos à instância.
19. Escolha Launch Instance (Executar instância).
20. Escolha o nome da tag para a instância e selecione Connect (Conectar) no menu suspenso Actions (Ações).
21. Verifique se a nova versão do SQL Server é mecanismo de banco de dados na nova instância.

Migração de uma instância do Windows para um tipo de instância da geração atual

As AMIs do Windows da AWS são configuradas com as definições padrão usadas pela mídia de instalação da Microsoft com algumas personalizações. As personalizações incluem drivers e configurações que são compatíveis com tipos de instância de última geração, que são instâncias desenvolvidas no AWS Nitro System, como uma instância M5 ou C5.

Ao migrar para as instâncias baseadas em Nitro, inclusive instâncias bare metal, recomendamos seguir as etapas deste tópico nos seguintes casos:

- Se você estiver iniciando instâncias a partir de AMIs personalizadas do Windows
- Se você estiver iniciando instâncias a partir de AMIs do Windows fornecidas pela Amazon que foram criadas antes de agosto de 2018

Para obter mais informações, consulte Atualização do Amazon EC2 – tipos de instância adicionais, Sistema Nitro e opções de CPU.

> **Note**
>
> Os procedimentos de migração a seguir podem ser executados no Windows Server versão 2008 R2 e posterior. Para migrar instâncias do Linux para os tipos de instância de última geração, consulte the section called “Alterar o tipo de instância”.

Sumário

- Parte 1: Instalar e atualizar drivers da AWS PV
- Parte 2: Instalar e atualizar ENA
- Parte 3: Atualizar drivers AWS NVMe
- Parte 4: Atualizar o EC2Config e o EC2Launch
- Parte 5: Instalar o driver de porta serial para instâncias bare metal
- Parte 6: Atualizar as configurações de gerenciamento de energia
- Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância
- (Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager
- Migração de uma instância do Windows de tipos de instância do Nitro para o Xen

> **Note**
>
> Como alternativa, é possível usar o documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` para automatizar os procedimentos descritos em Parte 1, Parte 2 e Parte 3. Se você optar por usar o procedimento automatizado, consulte (Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager e continue com a Parte 4 e a Parte 5.

Antes de começar

Esse procedimento pressupõe que, no momento, você esteja executando um tipo de instância baseado em Xen da geração anterior, como uma instância M4 ou C4, e esteja realizando a migração para uma instância desenvolvida no AWS Nitro System.

Use a versão 3.0 do PowerShell, ou posterior, para fazer a atualização com êxito.

> **Note**
>
> Ao migrar para a última geração de instâncias, as configurações de IP estático ou de DNS personalizado na ENI existente poderão ser perdidas uma vez que a instância será padronizada para um novo dispositivo de adaptador de redes avançadas.

Antes de seguir as etapas neste procedimento, recomendamos que você crie um backup de instância. No Console EC2, escolha a instância que requer a migração, abra o menu de contexto (botão direito do mouse), escolha Estado da instância e Parar.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

Abra o menu de contexto (clique com o botão direito do mouse) da instância, no Console EC2, escolha Imagem, e depois escolha Criar imagem.

> **Note**
>
> As partes 4 e 5 destas instruções podem ser concluídas após a migração ou a alteração do tipo de instância para a geração mais recente. No entanto, recomendamos que você as conclua antes da migração se estiver migrando especificamente para um tipo de instância bare metal.

Parte 1: Instalar e atualizar drivers da AWS PV

Embora os drivers AWS PV não sejam utilizados no sistema Nitro, você ainda deve atualizá-los se você estiver em versões anteriores do Citrix PV ou AWS PV. Os drivers AWS PV mais recentes resolvem erros em versões anteriores dos drivers que podem aparecer enquanto você estiver no sistema Nitro, ou se você precisar migrar de volta a uma instância baseada em Xen. Como prática recomendada, recomendamos sempre atualizar os drivers mais recentes de instâncias do Windows na AWS.

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, no Windows Server 2012, no Windows Server 2012 R2, no Windows Server 2016 ou no Windows Server 2019. Para ter mais informações, consulte Atualizar drivers de PV em instâncias do Windows.

Para atualizar um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV).

Para executar uma atualização de drivers AWS PV

1. Conecte-se à instância usando o Remote Desktop e prepare a instância a ser atualizada. Deixe offline todos os discos que não sejam do sistema antes de executar a atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Defina serviços não essenciais como inicialização Manual no console de Services.
2. Faça download do pacote de drivers mais recente na instância.
3. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância pode ficar indisponível por até 15 minutos.

Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se o novo driver foi instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para ter mais informações, consulte Histórico do pacote de drivers AWS PV.

Parte 2: Instalar e atualizar ENA

Atualize para o driver Elastic Network Adapter mais recente para garantir todos os recursos de rede sejam aceitos. Se você executou a instância e ela não tiver a rede avançada habilitada, faça download e instale o driver do adaptador de rede obrigatório na instância. Depois, defina o atributo da instância enaSupport para ativar a rede avançada. Você somente poderá ativar esse atributo em tipos de instância suportados e somente se o driver ENA estiver instalado. Para ter mais informações, consulte Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2.

1. Faça download do driver mais recente para a instância. Se você precisar de uma versão anterior do driver, consulte the section called “Driver do ENA para o Windows”.
2. Extraia o arquivo zip.
3. Instale o driver executando o script de PowerShell `install.ps1` da pasta extraída.

> **Note**
>
> Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

4. Verifique se AMI tem enaSupport ativado. Em caso negativo, continue seguindo a documentação em Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2.

Parte 3: Atualizar drivers AWS NVMe

Os drivers AWS NVMe são usados para interagir com volumes de armazenamento de instâncias de Amazon EBS e de SSD que são expostos como dispositivos de bloco de NVMe no sistema Nitro para melhor performance.

> **Important**
>
> As seguintes instruções são alteradas especificamente para quando você instala ou atualiza AWS NVMe em uma instância anterior de geração com a intenção para migrar a instância para o tipo de instância de geração mais recente.

1. Faça download do pacote de drivers mais recente na instância.
2. Extraia o arquivo zip.
3. Instale o driver executando `dpinst.exe`.
4. Abra uma sessão do PowerShell e execute este comando:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Para aplicar o comando, é necessário executar a sessão do PowerShell como administrador. As versões do PowerShell (x86) resultarão em um erro.
> Esse comando executa somente um sysprep em dispositivos do driver. Não executa uma preparação de sysprep completa.

5. Para o Windows Server 2008 R2 e o Windows Server 2012, feche a instância, altere o tipo para uma instância de última geração e inicie-a, depois, prossiga para a Parte 4. Se você iniciar a instância novamente em um tipo de instância de geração anterior antes de migrar para um tipo de instância mais recente, ele não será reiniciado. Para outras AMIs do Windows compatíveis, é possível alterar o tipo de instância a qualquer momento após o sysprep do dispositivo.

Parte 4: Atualizar o EC2Config e o EC2Launch

Para instâncias do Windows, os utilitários EC2Config e EC2Launch mais recentes fornecem funcionalidade e informações adicionais na execução em sistema Nitro, incluindo o Bare Metal EC2. Por padrão, o serviço EC2Config está incluído em AMIs anteriores ao Windows Server 2016. O EC2Launch substitui o EC2Config nas AMIs do Windows Server 2016 e posterior.

Quando os serviços EC2Config e EC2Launch forem atualizados, as novas AMIs do Windows da AWS incluirão a versão mais recente do serviço. Contudo, você precisa atualizar suas próprias instâncias e AMIs do Windows com a versão mais recente do EC2Config e EC2Launch.

Para instalar ou atualizar EC2Config

1. Faça download e descompacte o instalador do EC2Config.
2. Execute `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

Para ter mais informações, consulte Instalar a versão mais recente do EC2Config.

Para instalar ou atualizar EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Faça download do EC2-Windows-Launch.zip em um diretório na instância.
3. Faça download do install.ps1 no mesmo diretório onde você baixou o `EC2-Windows-Launch.zip`.
4. Execute `install.ps1`.

> **Note**
>
> Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para ter mais informações, consulte Configurar uma instância do Windows usando o EC2Launch.

Parte 5: Instalar o driver de porta serial para instâncias bare metal

O tipo de instância `i3.metal` usa um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. Os AMIs do Windows mais recentes automaticamente usam dispositivo de série baseado em PCI e tem o driver de porta serial instalados. Se você não estiver usando uma instância lançada de um AMI do Windows fornecido pela Amazon, datado de 11.04.2018 ou posterior, deverá instalar o Driver de porta serial para habilitar o dispositivo serial para recursos de EC2 como Geração de senha e Saída de console. Os utilitários EC2Config e EC2Launch mais recentes também suportam o i3.metal e fornecem funcionalidade adicional. Caso ainda não tenha feito, siga as etapas da Parte 4.

Para instalar o driver de porta serial

1. Faça download do pacote de drivers de série mais recente na instância.
2. Extraia o conteúdo da pasta, abra o menu de contexto (clique com o botão direito) em `aws_ser.INF` e selecione install (instalar).
3. Escolha OK.

Parte 6: Atualizar as configurações de gerenciamento de energia

A seguinte atualização das configurações de gerenciamento de energia definirá os vídeos para nunca desligarem, o que permite desligamentos normais do sistema operacional no sistema Nitro. Todas as AMIs do Windows fornecidas pela Amazon a partir de 2018.11.28 já têm essa configuração padrão.

1. Abra um prompt de comando ou uma sessão do PowerShell.
2. Execute os seguintes comandos:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância

Os tipos de instância `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` usam hardware que exige drivers de chipset que não foram instalados anteriormente nas AMIs do Windows. Se você não estiver usando uma instância executada de uma AMI do Windows fornecida pela Amazon, datada de 19/11/2018 ou posterior, deverá instalar os drivers usando o utilitário INF do Chipset Intel.

Para instalar os drivers de chipset

1. Faça download do utilitário chipset na instância.
2. Extraia os arquivos.
3. Execute `SetupChipset.exe`.
4. Aceite o contrato de licença do software Intel e instale os drivers do chipset.
5. Reinicialize a instância.

(Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager

O documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` automatiza as etapas descritas em Parte 1, Parte 2 e Parte 3. Esse método também pode reparar uma instância onde houve falha nas atualizações de driver.

O documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` atualiza ou repara os drivers AWS de armazenamento e rede na instância do EC2 especificada. O documento tenta instalar as versões mais recentes dos drivers da AWS online chamando o AWS Systems Manager Agent (SSM Agent). Se o SSM Agent não puder ser conectado, o documento poderá executar uma instalação offline dos drivers da AWS caso solicitado explicitamente.

> **Note**
>
> Esse procedimento falhará em um controlador de domínio. Para atualizar drivers em um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV).

Como atualizar automaticamente os drivers AWS PV, ENA e NVMe usando AWS Systems Manager

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager.

2. Escolha Automation (Automação), Execute Automation (Executar automação).
3. Pesquise e selecione o documento de automação AWSSupport-UpgradeWindowsAWSDrivers e escolha Executar automação.
4. Na seção Parâmetros de entrada, configure as seguintes opções:

   ID da instância

   Insira o ID exclusivo da instância a ser atualizada.

   AllowOffline

   (Opcional) Escolha uma das seguintes opções:

   - `True`: escolha essa opção para executar uma instalação offline. A instância é interrompida e reiniciada durante o processo de atualização.

     > **Warning**
     >
     > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

   - `False`: (Padrão) para executar uma instalação online, deixe essa opção selecionada. A instância é reiniciada durante o processo de atualização.

     > **Important**
     >
     > As atualizações online e offline criam uma AMI antes de tentar as operações de atualização. A AMI persiste depois da conclusão da automação. Garanta seu acesso à AMI ou exclua-o se não for mais necessário.

   SubnetId

   (Opcional) Insira um dos seguintes valores:

   - `SelectedInstanceSubnet` — (Padrão) O processo de atualização executa a instância helper na mesma sub-rede da instância que deve ser atualizada. A sub-rede deve permitir a comunicação com os endpoints Systems Manager (`ssm.*`).

- `CreateNewVPC` — O processo de atualização executa a instância helper em uma nova VPC. Use essa opção se não souber ao certo se a sub-rede da instância de destino permite a comunicação com os endpoints `ssm.*`. O usuário deve ter permissão para criar uma VPC.
- Um ID de sub-rede específico — Especifique o ID de uma sub-rede específica na qual executar a instância helper. A sub-rede na mesma zona de disponibilidade da instância que deve ser atualizada, e deve permitir a comunicação com os endpoints `ssm.*`.

5. Clique em Executar.
6. Deixe a atualização terminar. Pode levar até 10 minutos para concluir uma atualização online e até 25 minutos para concluir uma atualização offline.

Migração de uma instância do Windows de tipos de instância do Nitro para o Xen

O procedimento apresentado a seguir pressupõe que, no momento, você esteja realizando execuções em um tipo de instância baseado em Nitro e que esteja migrando para uma instância baseada no sistema Xen, como uma instância M4 ou C4. Para obter especificações sobre o tipo de instância, consulte o Guia de tipos de instância do Amazon EC2. Execute as seguintes etapas antes da migração para evitar erros durante o processo de inicialização.

Como migrar do Nitro para o Xen

1. Faça backup de seus dados.
2. Verifique se sua política de SAN do Windows permite que volumes de armazenamento que não são raiz permaneçam on-line.
3. Os drivers AWS PV devem ser instalados e atualizados em uma instância Nitro antes de migrar para uma instância Xen. Para as etapas de instalação e atualização de drivers AWS PV, consulte Parte 1: Instalar e atualizar drivers da AWS PV.
4. Atualize para a versão EC2Launch v2 mais recente. Consulte as etapas em Migrar para o EC2Launch v2.
5. Abra uma sessão do PowerShell e execute o seguinte comando como administrador para fazer o sysprep dos drivers do dispositivo. A execução do sysprep garante que os drivers de armazenamento de inicialização antecipada necessários para inicializar em instâncias Xen sejam devidamente registrados no Windows.

> **Note**
>
> Executar o comando usando as versões do PowerShell (x86) resultará em um erro. Este comando adiciona apenas os drivers de dispositivo críticos de inicialização ao banco de dados crítico do dispositivo. Não executa uma preparação de sysprep completa.

```
Start-Process rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

6. Execute a migração para um tipo de instância Xen quando o processo de sysprep for concluído.

Assistente de redefinição de plataforma Windows para Linux para bancos de dados Microsoft SQL Server

Para obter informações sobre como redefinir a plataforma Windows para Linux para bancos de dados Microsoft SQL Server, consulte o Assistente de redefinição de plataforma Windows para Linux para bancos de dados Microsoft SQL Server no Guia do usuário do Microsoft SQL Server no Amazon EC2.

Solução de problemas de atualização em uma instância do Windows

A AWS oferece suporte à atualização para problemas com o Upgrade Helper Service, um utilitário da AWS que ajuda você a executar atualizações no local que envolvem drivers Citrix PV.

Após a atualização, a instância pode apresentar temporariamente uma utilização de CPU maior do que a média enquanto o serviço .NET Runtime Optimization otimiza o .NET Framework. Esse comportamento é esperado.

Se a instância não passou nas duas verificações de status após várias horas, verifique o seguinte.

- Se você fez a atualização para o Windows Server 2008 e as duas verificações de status falharem após várias horas, a atualização pode ter falhado e estar apresentando um prompt para Clicar em OK a fim de confirmar a reversão. Como o console não está acessível nesse estado, não há como clicar no botão. Para contornar isso, execute uma reinicialização através da API ou do console do Amazon EC2. A reinicialização levará 10 minutos ou mais para ser iniciada. A instância pode se tornar disponível após 25 minutos.
- Remova as aplicações ou as funções do servidor e tente novamente.

Se a instância não passar nas verificações de status depois de remover as aplicações ou funções do servidor, faça o seguinte.

- Interrompa a instância e anexe o volume raiz a outra instância. Para obter mais informações, consulte a descrição de como parar e anexar o volume raiz a outra instância em "Esperando o serviço de metadados".
- Analise os arquivos de log de configuração e os logs de eventos do Windows para ver se há falhas.

Para outros problemas com uma atualização ou uma migração do sistema operacional, recomendamos analisar os artigos indicados em Antes de iniciar uma atualização no local.

Frota do EC2 e frota spot

O EC2 Fleet e a frota spot foram projetados para serem uma forma útil de executar uma frota ou um grupo de instâncias com a AWS. Cada instância em uma frota é baseada em um modelo de execução ou em um conjunto de parâmetros de execução que você configura manualmente ao iniciar a instância.

As frotas fornecem os recursos e benefícios a seguir. Esses benefícios possibilitam maximizar a economia de custos e otimizar a disponibilidade e o desempenho ao executar aplicações em várias instâncias do EC2.

Vários tipos de instâncias e várias opções de compra

Em uma única chamada de API, uma frota pode executar vários tipos de instâncias e opções de compra (instâncias spot e sob demanda), permitindo que você otimize os custos por meio do uso da instância spot. Você também pode aproveitar os descontos da instância reservada e do Savings Plans usando-os com as instâncias sob demanda na frota.

Distribuição de instâncias entre zonas de disponibilidade

Uma frota tenta distribuir automaticamente as instâncias de maneira uniforme entre várias zonas de disponibilidade para fornecer alta disponibilidade. Isso fornece resiliência caso uma zona de disponibilidade fique indisponível.

Substituição automatizada de instâncias spot

Caso a sua frota inclua instâncias spot, ela pode solicitar automaticamente a substituição da capacidade spot se suas instâncias spot forem interrompidas ou ficarem prejudicadas devido a uma mudança na integridade da instância. Por meio do rebalanceamento de capacidade, uma frota também pode monitorar e substituir proativamente as instâncias spot que apresentam um risco elevado de interrupção.

O EC2 Fleet é uma boa opção se você precisar de flexibilidade para gerenciar aspectos do ciclo de vida da instância ou dos mecanismos de escalabilidade. Você também pode usar a frota spot, mas não recomendamos que use por se tratar de uma API herdada sem investimento planejado. No entanto, se você já estiver usando a frota spot, poderá continuar o uso. A frota spot e o EC2 Fleet oferecem a mesma funcionalidade principal.

> **Tip**
>
> Como prática recomendada geral, recomendamos iniciar frotas de instâncias spot e sob demanda com o Amazon EC2 Auto Scaling, pois ele fornece recursos adicionais que você pode usar para gerenciar suas frotas. A lista de recursos adicionais inclui substituições automáticas da verificação de integridade para instâncias spot e sob demanda, verificações de integridade baseadas em aplicações e uma integração com o Elastic Load Balancing para garantir uma distribuição uniforme do tráfego de aplicações para as suas instâncias íntegras. Você também pode usar os grupos do Auto Scaling ao utilizar serviços da AWS, como o Amazon ECS, o Amazon EKS (grupos de nós autogerenciados) e o Amazon VPC Lattice. Para obter mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Tópicos

- EC2 Fleet
- Frota spot
- Monitorar eventos da frota usando o Amazon EventBridge
- Tutoriais para EC2 Fleet e frota spot
- Exemplo de configurações para EC2 Fleet e frota spot
- Quotas da frota

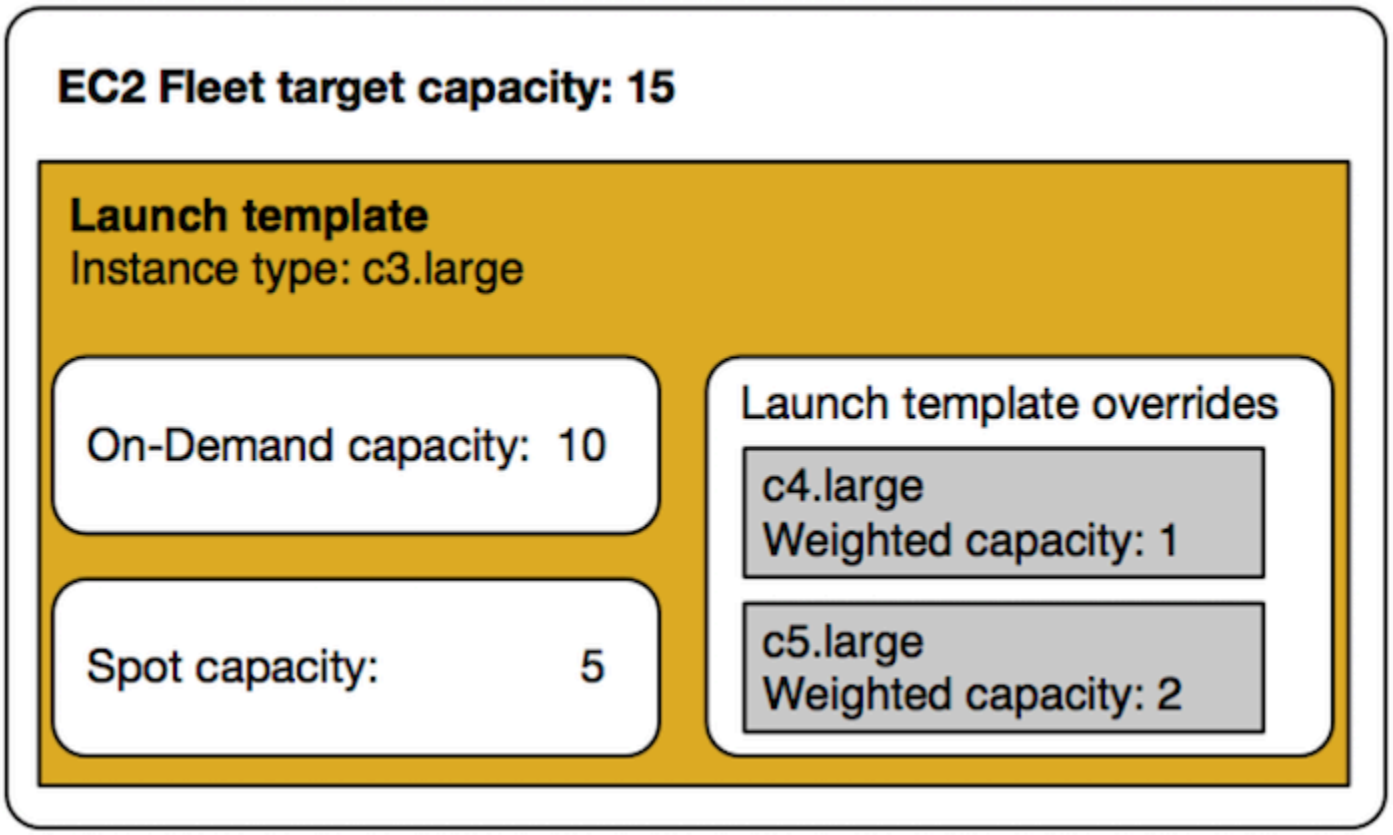
EC2 Fleet

Uma Frota do EC2 contém as informações de configuração para executar uma frota de instâncias. Em uma única chamada de API, uma frota pode executar vários tipos de instâncias em várias zonas de disponibilidade, usando as opções de compra de instância spot, instância sob demanda, instância reservada e Savings Plans juntos. Usando o Frota do EC2, você pode:

- Definir metas separadas de capacidade sob demanda e spot e a quantidade máxima que você deseja pagar por hora
- Especifique os tipos de instância que funcionam melhor para suas aplicações
- Especifique como o Amazon EC2 deve distribuir a capacidade da sua frota dentro de cada opção de compra

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e o Frota do EC2 executará instâncias até alcançar o valor máximo. Quando o valor máximo que você está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

A Frota do EC2 tenta executar o número de instâncias que são necessárias para atender à capacidade de destino especificada na sua solicitação. Se você tiver especificado um preço máximo total por hora, ele cumprirá a capacidade até alcançar a quantidade máxima que você está disposto a pagar. A frota também pode interromper a manutenção da capacidade Spot se as Instâncias spot forem interrompidas. Para obter mais informações, consulte Como as Instâncias spot funcionam.



Você pode especificar um número ilimitado de tipos de instâncias por Frota do EC2. Esses tipos de instância podem ser provisionados usando as opções de compra sob demanda e spot. Você também pode especificar várias zonas de disponibilidade, especificar preços spot máximos diferentes para cada instância e escolher opções spot adicionais para cada frota. O Amazon EC2 usa as opções especificadas para provisionar capacidade quando a frota é iniciada.

Enquanto a frota estiver em execução, se o Amazon EC2 recuperar uma instância spot devido a um aumento de preço ou uma falha na instância, a EC2 Fleet tentará substituir as instâncias por qualquer um dos tipos de instância que você especificar. Isso facilita recuperar a capacidade durante

um pico nos preços Spot. Você pode desenvolver uma estratégia flexível e elástica de alocação de recursos para cada frota. Por exemplo, dentro de frotas específicas, sua capacidade principal pode ser suplementada sob demanda com capacidade spot mais barata (se disponível).

Se você tiver Instâncias reservadas e especificar Instâncias on-demand na sua frota, a Frota do EC2 usará suas Instâncias reservadas. Por exemplo, se sua frota especificar instância sob demanda como `c4.large` e você tiver Instâncias reservadas para `c4.large`, receberá a definição de preço de Instância reservada. O mesmo se aplica ao usar um Savings Plans.

Não há cobrança adicional pelo uso do Frota do EC2. Você paga apenas pelas instâncias do EC2 que a frota executar.

Tópicos

- Limitações da Frota do EC2
- Instâncias expansíveis
- Tipos de solicitação da Frota do EC2
- Estratégias de configuração da Frota do EC2
- Trabalhar com Frotas do EC2

Limitações da Frota do EC2

As limitações a seguir se aplicam à Frota do EC2:

- A frota do EC2 está disponível apenas pela API do Amazon EC2, pela AWS CLI, pelos AWS SDKs e pelo AWS CloudFormation.
- Uma solicitação de EC2 Fleet não pode abranger regiões da AWS. Você precisa criar uma Frota do EC2 separada para cada região.
- Uma solicitação de Frota do EC2 não pode abranger sub-redes diferentes na mesma zona de disponibilidade.

Instâncias expansíveis

Se você executar as Instâncias spot usando um tipo de instância expansível e planeja usar as instâncias spot expansíveis imediatamente e por um breve período, sem tempo ocioso para acumular créditos de CPU, recomendamos executá-las no modo padrão para evitar pagar custos mais elevados. Se executar as Instâncias spot expansíveis no modo ilimitado e esgotar a CPU

imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para expansão. Caso contrário, pagar por créditos excedentes torna a as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para ter mais informações, consulte Quando usar o modo ilimitado versus CPU fixa.

Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o modo Ilimitado para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Tipos de solicitação da Frota do EC2

Existem três tipos de solicitações de Frota do EC2:

`instant`

Se você configurar o tipo de solicitação como `instant`, a Frota do EC2 incluirá uma solicitação síncrona única da capacidade desejada. Na resposta da API, as instâncias que foram executadas são retornadas, junto com os erros das instâncias que não puderam ser executadas. Para ter mais informações, consulte Usar uma EC2 Fleet do tipo 'instantâneo'.

`request`

Se você configurar o tipo de solicitação como `request`, a Frota do EC2 incluirá uma solicitação assíncrona única da capacidade desejada. Portanto, se a capacidade for reduzida devido a interrupções do spot, a frota não tentará reabastecer as Instâncias spot nem enviará solicitações em grupos de capacidade spot alternativos, se a capacidade não estiver disponível.

`maintain`

(Padrão) Se você configurar o tipo de solicitação como `maintain`, a Frota do EC2 incluirá uma solicitação assíncrona única da capacidade desejada e manterá a capacidade reabastecendo automaticamente quaisquer Instâncias spot interrompidas.

Todos os três tipos de solicitações se beneficiam com uma estratégia de alocação. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.

Usar uma EC2 Fleet do tipo 'instantâneo'

A EC2 Fleet do tipo instantâneo é uma solicitação síncrona única que faz apenas uma tentativa de iniciar a capacidade desejada. A resposta da API lista as instâncias que foram iniciadas juntamente com os erros das instâncias que não puderam ser iniciadas. Há vários benefícios de se usar uma EC2 Fleet do tipo Instantâneo, e eles são descritos neste artigo. Exemplos de configurações são fornecidos no fim do artigo.

Para workloads que precisam de uma API somente de inicialização para iniciar instâncias do EC2, você pode usar a API RunInstances. No entanto, com RunInstances, você só pode iniciar Instâncias sob demanda ou instâncias spot, mas não ambas na mesma solicitação. Além disso, quando você usa RunInstances para iniciar Instâncias spot, sua solicitação de Instância spot é limitada a um tipo de instância e a uma zona de disponibilidade. Isso visa um único grupo de capacidade spot (um conjunto de instâncias com o mesmo tipo de instância e zona de disponibilidade). Se o grupo de capacidade spot não tiver capacidade de instância spot suficiente para sua solicitação, a chamada RunInstances não tem sucesso.

Em vez de usar RunInstances para iniciar Instâncias spot, é recomendável usar a API CreateFleet com o parâmetro `type` definido como `instant` para obter os seguintes benefícios:

- Iniciar Instâncias sob demanda e instâncias spot em uma única solicitação. Uma EC2 Fleet pode iniciar Instâncias sob demanda, instâncias spot ou ambas. A solicitação das Instâncias spot é atendida se houver capacidade disponível e o preço máximo por hora para sua solicitação excede o preço Spot.
- Aumente a disponibilidade das instâncias spot. Usando uma EC2 Fleet do tipo `instant`, você pode iniciar instâncias spot seguindo as Práticas recomendadas para spot com os benefícios decorrentes disso:
  - Prática recomendada para spot: seja flexível sobre tipos de instância e zonas de disponibilidade.

    Benefício: especificando vários tipos de instância e zonas de disponibilidade, você aumenta o número de grupos de capacidade spot. Isso dá ao serviço de spot uma chance maior de encontrar e alocar sua capacidade computacional spot desejada. Uma boa regra geral é ser flexível em pelo menos 10 tipos de instância para cada workload e garantir que todas as zonas de disponibilidade estejam configuradas para uso na sua VPC.
  - Prática recomendada para spot: use a estratégia de alocação de price-capacity-optimized.

Benefício: a estratégia de alocação de `price-capacity-optimized` identifica instâncias nos grupos de capacidade spot com maior disponibilidade e provisiona as instâncias de menor preço desses grupos. Como a capacidade de instâncias spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam interrompidas quando o Amazon EC2 precisar recuperar capacidade.

- Tenha acesso a um conjunto mais amplo de recursos. Para workloads que precisam de uma API somente de lançamento e em que você prefere gerenciar o ciclo de vida de sua instância em vez de deixar a frota EC2 gerenciá-lo para você, use a EC2 Fleet do tipo `instant` em vez da API RunInstances. A EC2 Fleet fornece um conjunto mais amplo de recursos do que o RunInstances, conforme demonstrado nos exemplos a seguir. Para todas as outras workloads, você deve usar o Amazon EC2 Auto Scaling, porque ele fornece um conjunto de recursos mais abrangente para uma grande variedade de workloads, como aplicativos apoiados pelo ELB, workloads em contêineres e trabalhos de processamento de fila.

Você pode usar a Frota do EC2 do tipo instantânea para iniciar instâncias em blocos de capacidade. Para ter mais informações, consulte Tutorial : iniciar instâncias em blocos de capacidade.

Os serviços da AWS, como o Amazon EC2 Auto Scaling e o Amazon EMR, usam o tipo de EC2 Fleet instantâneo para iniciar instâncias do EC2.

Pré-requisitos para a EC2 Fleet do tipo instantâneo

Para obter os pré-requisitos para criar uma EC2 Fleet, consulte Pré-requisitos da Frota do EC2.

Como uma EC2 Fleet instantânea funciona

Ao trabalhar com uma EC2 Fleet do tipo `instant`, a sequência de eventos é a seguinte:

1. Configure o tipo de solicitação CreateFleet como `instant`. Para ter mais informações, consulte Criar uma Frota do EC2.. Observe que, após fazer a chamada de API, você não pode modificá-la.
2. Quando você faz uma chamada de API, a EC2 Fleet faz uma solicitação síncrona única da capacidade desejada.
3. A resposta da API lista as instâncias que foram iniciadas juntamente com os erros das instâncias que não puderam ser iniciadas.
4. Você pode descrever a EC2 Fleet, listar as instâncias associadas à EC2 Fleet e visualizar o histórico da EC2 Fleet.

5. Após a inicialização das instâncias, você poderá excluir a solicitação de frota. Ao excluir a solicitação de frota, você também pode optar por encerrar as instâncias associadas ou deixá-las em execução.
6. É possível encerrar as instâncias a qualquer momento.

Exemplos

Os exemplos a seguir mostram como usar a EC2 Fleet do tipo `instant` para diferentes casos de uso. Para obter mais informações sobre como usar os parâmetros da APICreateFleet do EC2, consulte Criar frota na Referência de API do Amazon EC2.

Exemplos

- Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade
- Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade
- Exemplo 3: iniciar uma frota spot usando pesos de instâncias
- Exemplo 4: iniciar instâncias spot dentro de uma única zona de disponibilidade
- Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade
- Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada
- Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade
- Exemplo 8: iniciar instâncias com vários modelos de lançamento
- Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda
- Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada
- Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized

Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo `instant`: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento.

- O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento.
- As 12 substituições do modelo de lançamento especificam 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. Cada combinação de tipo de instância e sub-rede define um grupo de capacidade spot, resultando em 12 pools de capacidade spot.
- A capacidade mínima pretendida para a frota é de 20 instâncias.
- A opção de compra padrão é `spot`, o que resulta na tentativa da frota de iniciar 20 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade

Você pode iniciar de forma ideal uma instância spot de cada vez fazendo várias chamadas de API da EC2 Fleet do tipo `instant`, definindo o TotalTargetCapacity como 1.

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 substituições do modelo de lançamento têm 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida da frota é 1 instância, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar uma instância spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação otimizada para capacidade, para iniciar uma instância spot a partir do grupo de capacidade mais disponível.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
```

```
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 3: iniciar uma frota spot usando pesos de instâncias

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância diferente e um peso diferente com base em quantas unidades da workload podem ser executadas na instância, pressupondo que uma unidade da workload requeira 15 GB de memória e 4 vCPUs. Por exemplo,

m5.xlarge (4 vCPUs e 16 GB de memória) pode executar uma unidade e tem peso 1, m5.2xlarge (8 vCPUs e 32 GB de memória) pode executar 2 unidades e tem peso 2, e assim por diante. A capacidade total pretendida é definida como 40 unidades. A opção de compra padrão é spot, e a estratégia de alocação é otimizada para capacidade, o que resulta em 40 m5.xlarge (40 dividido por 1), 20 m5.2xlarge (40 dividido por 2), 10 m5.4xlarge (40 dividido por 4), 5 m5.8xlarge (40 dividido por 8) ou uma combinação de tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

Para ter mais informações, consulte Peso de instâncias da Frota do EC2.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
```

```
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.8xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":8
         },
         {
            "InstanceType":"m5.8xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":8
         },
         {
            "InstanceType":"m5.8xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":8
         }
      ]
   }
],
"TargetCapacitySpecification":{
   "TotalTargetCapacity":40,
   "DefaultTargetCapacityType":"spot"
```

```
   },
   "Type":"instant"
}
```

Exemplo 4: iniciar instâncias spot dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias em uma única zona de disponibilidade definindo as opções de spot SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot, todas em uma única AZ, a partir dos grupos de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias do mesmo tipo de instância em uma única zona de disponibilidade definindo SpotOptions SingleInstanceType como true e SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot do mesmo tipo de instância, todas em uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada

Você pode configurar uma frota para iniciar as instâncias somente se a capacidade mínima pretendida puder ser iniciada, definindo as opções de spot MinTargetCapacity como a capacidade pretendida que você deseja iniciar em conjunto.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A Frota do EC2 inicia 20 instâncias spot a partir do grupo de capacidade spot com capacidade ideal usando as substituições do modelo de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
```

```
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade

Você pode configurar uma frota para iniciar as instâncias apenas se a capacidade mínima pretendida puder ser iniciada com um único tipo de instância em uma única zona de disponibilidade, definindo as opções de spot MinTargetCapacity como a capacidade mínima pretendida que você deseja iniciar ao mesmo tempo, juntamente com as opções SingleInstanceType e SingleAvailabilityZone.

As 12 especificações que substituem o modelo de lançamento têm diferentes tipos de instância e sub-redes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot, a estratégia de alocação spot é otimizada para capacidade, SingleInstanceType é true e SingleAvailabilityZone é true. A EC2 Fleet inicia 20 instâncias spot, todas do mesmo tipo de instância e todas em uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
```

```
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
       "TotalTargetCapacity": 20,
       "DefaultTargetCapacityType": "spot"
   },
```

```
    "Type": "instant"
}
```

Exemplo 8: iniciar instâncias com vários modelos de lançamento

Você pode configurar uma frota para iniciar instâncias com diferentes especificações de lançamento para diferentes tipos de instância ou um grupo de tipos de instância, especificando vários modelos de lançamento. Neste exemplo, queremos ter diferentes tamanhos de volume do EBS para diferentes tipos de instância e temos isso configurado nos modelos de lançamento ec2-fleet-lt-4xl, ec2-fleet-lt-9xl e ec2-fleet-lt-18xl.

Neste exemplo, usaremos 3 modelos de lançamento diferentes para os 3 tipos de instância, com base em seu tamanho. As especificação de lançamento faz a substituição em todos os modelos de lançamento que usam pesos de instância com base nas vCPUs no tipo de instância. A capacidade total pretendida é de 144 instâncias, a opção de compra padrão é spot e a estratégia de alocação de spot é otimizada para capacidade. A EC2 Fleet pode iniciar 9 c5n.4xlarge (144 dividido por 16) usando o modelo de lançamento ec2-fleet-4xl, ou 4 c5n.9xlarge (144 dividido por 36), usando o modelo de lançamento ec2-fleet-9xl, ou 2 c5n.18xlarge (144 dividido por 72), usando o modelo de lançamento ec2-fleet-18xl, ou uma combinação dos tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
```

```
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
```

```
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda

O exemplo a seguir especifica a capacidade total pretendida de 20 instâncias para a frota e uma capacidade pretendida de 5 Instâncias sob demanda. A opção de compra padrão é spot. A frota inicia 5 Instâncias sob demanda, conforme especificado, mas precisa iniciar mais 15 instâncias para atender à capacidade total pretendida. A opção de compra para a diferença é calculada como TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType, que resulta no lançamento pela frota de 15 Instâncias spot a partir de um dos 12 grupos de capacidade de spot com base na estratégia de alocação otimizada para capacidade.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
```

```
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias sob demanda com o tipo de capacidade pretendida padrão como spot, definindo a estratégia de uso para Reservas de Capacidade como use-capacity-reservations-first. E se vários grupos de instâncias tiverem Reservas de Capacidade não utilizadas, a estratégia de alocação sob demanda escolhida será aplicada. Neste exemplo, a estratégia de alocação sob demanda é priorizada.

Neste exemplo, há 6 Reservas de Capacidade não utilizadas disponíveis. Isso é menos que a capacidade sob demanda pretendida da frota de 10 Instâncias sob demanda.

A conta tem as seguintes 6 Reservas de Capacidade não utilizadas em 2 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
```

```
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A estratégia de alocação sob demanda é priorizada, e a estratégia de uso para Reservas de Capacidade é use-capacity-reservations-first. A estratégia de alocação spot é otimizada para capacidade. A capacidade total pretendida é de 20, a capacidade sob demanda pretendida é de 10 e o tipo de capacidade pretendida padrão é spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
```

```
            "Priority": 3.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 4.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 5.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 6.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 7.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 8.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 9.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 10.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 11.0
         },
         {
            "InstanceType":"m5d.large",
```

```
                "SubnetId":"subnet-49e41922",
                "Priority": 12.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Depois de criar a frota instantânea usando a configuração anterior, as 20 instâncias a seguir serão iniciadas para atender à capacidade pretendida:

- 7 Instâncias sob demanda c5.large em us-east-1a – c5.large em us-east-1a é priorizada, e há 3 Reservas de Capacidade c5.large não utilizadas disponíveis. As Reservas de Capacidade são usadas primeiro para iniciar 3 Instâncias sob demanda, e 4 Instâncias sob demanda adicionais são iniciadas de acordo com a estratégia de alocação sob demanda, que é priorizada neste exemplo.
- 3 Instâncias sob demanda m5.large em us-east-1a – m5.large em us-east-1a é priorizada em segundo lugar, e há 3 Reservas de Capacidade c3.large não utilizadas disponíveis
- 10 instâncias spot a partir de um dos 12 grupos de capacidade spot que tem a capacidade ideal, de acordo com a estratégia de alocação otimizada para capacidade.

Depois que a frota for lançada, você poderá executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade de c5.large e m5.large foram usadas.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
```

```
}
```

Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 especificações que substituem o modelo de lançamento têm 4 tipos de instância diferentes com uma prioridade atribuída e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida para a frota é de 20 instâncias, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar 20 instâncias spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação capacity-optimized-prioritized, que tenta ao máximo implementar as prioridades, mas otimiza a capacidade em primeiro lugar.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
```

```
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 2.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 4.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 4.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 4.0
         }
```

```
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Estratégias de configuração da Frota do EC2

Uma Frota do EC2 é um grupo de Instâncias on-demand e Instâncias spot. A Frota do EC2 também pode ser um grupo de instâncias de blocos de capacidade.

Instâncias sob demanda e instâncias spot

A Frota do EC2 tenta executar o número de instâncias necessárias para atender à capacidade de destino especificada na solicitação de frota. A frota pode incluir somente Instâncias on-demand, somente Instâncias spot ou uma combinação de Instâncias on-demand e Instâncias spot. A solicitação das Instâncias spot é atendida se houver capacidade disponível e o preço máximo por hora para sua solicitação excede o preço Spot. A frota também tenta manter sua capacidade alvo caso as Instâncias spot sejam interrompidas.

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e o Frota do EC2 executará instâncias até alcançar o valor máximo. Quando o valor máximo que você está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

Um Grupo de capacidade spot é um conjunto de instâncias do EC2 não utilizadas, com o mesmo tipo de instância e zona de disponibilidade. Ao criar uma Frota do EC2, você poderá incluir várias especificações de execução, que variam de acordo com o tipo de instância, a zona de disponibilidade, a sub-rede e o preço máximo. A frota seleciona os grupos de capacidade spot que são usados para atender à solicitação com base nas especificações de execução incluídas na sua solicitação e na configuração da solicitação. As Instâncias spot vêm dos grupos selecionados.

Com uma Frota do EC2, é possível provisionar muita capacidade do EC2. Isso é uma vantagem para aplicações com base no número de núcleos/instâncias ou na quantidade de memória. Por exemplo, você pode especificar uma Frota do EC2 para executar uma capacidade de destino de 200 instâncias, das quais 130 serão Instâncias on-demand e o restante Instâncias spot.

Instâncias de blocos de capacidade

Os blocos de capacidade para ML permitem que você reserve instâncias de GPU para uma data futura a fim de lidar com workloads de machine learning (ML) de curta duração. As instâncias que são executadas em um bloco de capacidade são automaticamente colocadas próximas umas das outras dentro dos UltraClusters do Amazon EC2. Para obter mais informações sobre blocos de capacidade, consulte Blocos de capacidade para ML.

Use as estratégias de configuração apropriadas para criar uma Frota do EC2 que atenda às suas necessidades.

Conteúdo

- Planejar uma EC2 Fleet
- Estratégias de alocação para Instâncias spot
- Seleção de tipo de instância baseada em atributos para frota do EC2
- Configurar Frota do EC2 para backup sob demanda
- Rebalanceamento de capacidade
- Sobreposições de preço máximo
- Controle de gastos
- Peso de instâncias da Frota do EC2

Planejar uma EC2 Fleet

Ao planejar sua Frota do EC2, recomendamos que você faça o seguinte:

- Determine se você deseja criar uma Frota do EC2 que envie uma solicitação síncrona ou assíncrona única da capacidade de destino desejada ou uma que mantenha uma capacidade de destino ao longo do tempo. Para obter mais informações, consulte Tipos de solicitação da Frota do EC2.
- Determine os tipos de instâncias que atendem aos requisitos da aplicação.
- Se você pretende incluir Instâncias spot na sua Frota do EC2, reveja as Melhores práticas de spot antes de criar a frota. Use essas melhores práticas ao planejar sua frota para que você possa provisionar as instâncias com o menor preço possível.
- Determine a capacidade de destino da sua Frota do EC2. Você pode definir a capacidade de destino em instâncias ou em unidades personalizadas. Para obter mais informações, consulte Peso de instâncias da Frota do EC2.

- Determine a parte da capacidade de destino da Frota do EC2 que deve ser de capacidade sob demanda e spot. Você pode especificar 0 para a capacidade sob demand, a capacidade spot ou ambas.
- Determine seu preço por unidade, se você estiver usando o peso de instância. Para calcular o preço por unidade, divida o preço por hora de instância pelo número de unidades (ou peso) que essa instância representa. Se você não estiver usando o peso de instância, o preço padrão por unidade será o preço por hora de instância.
- Determine a quantidade máxima por hora que você está disposto a pagar pela sua frota. Para obter mais informações, consulte Controle de gastos.
- Leia as opções possíveis para sua Frota do EC2. Para obter informações sobre os parâmetros da frota, consulte create-fleet na Referência de comandos da AWS CLI. Para exemplos de configuração da Frota do EC2, consulte Exemplos de configuração de Frota do EC2.

Estratégias de alocação para Instâncias spot

Sua configuração de inicialização determina todos os possíveis grupos de capacidade spot (tipos de instância e zonas de disponibilidade) nos quais a frota do EC2 pode iniciar instâncias spot. No entanto, ao iniciar instâncias, a frota do EC2 usa a estratégia de alocação que você especifica para escolher os grupos específicos de todos os seus grupos possíveis.

> **Note**
>
> (Somente para instâncias do Linux) Se você configurar a instância spot para iniciar com o AMD SEV-SNP ativado, será cobrada uma taxa de utilização por hora adicional equivalente a 10% da taxa horária sob demanda para o tipo de instância selecionado. Se a estratégia de alocação usar o preço como entrada, a frota do EC2 não incluirá essa tarifa adicional; somente o preço spot será usado.

Estratégias de alocação

Você pode especificar uma destas estratégias de alocação para instâncias spot:

`price-capacity-optimized` (recomendado)

A Frota do EC2 identifica os grupos com a maior disponibilidade de capacidade para o número de instâncias que estão sendo inicializadas. Isso significa que solicitaremos instâncias spot dos

grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo. Em seguida, a Frota do EC2 solicita instâncias spot do grupo com o menor preço entre os grupos.

A estratégia de alocação `price-capacity-optimized` é a ideal para a maioria das workloads spot, como aplicações conteinierizadas sem estado, microsserviços, aplicações da Web, trabalhos de dados e análise, e processamento em lote.

`capacity-optimized`

A Frota do EC2 identifica os grupos com a maior disponibilidade de capacidade para o número de instâncias que estão sendo inicializadas. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo. Opcionalmente, você pode definir uma prioridade para cada tipo de instância na frota usando o `capacity-optimized-prioritized`. A EC2 Fleet otimiza a capacidade primeiro, mas empenha-se em honrar as prioridades de tipo de instância.

Com as Instâncias spot, a definição de preço muda lentamente ao longo do tempo com base em tendências de longo prazo na oferta e na demanda, mas a capacidade oscila em tempo real. A estratégia `capacity-optimized` executa Instâncias spot automaticamente nos grupos mais disponíveis observando dados de capacidade em tempo real e prevendo quais são os mais disponíveis. Isso funciona bem para workloads que podem ter um custo de interrupção maior associado ao reinício do trabalho, como workloads de integração contínua (CI) longa, de renderização de imagens e mídia, de aprendizado profundo e de computação de alta performance (HPC). Ao oferecer a possibilidade de menos interrupções, a estratégia `capacity-optimized` pode reduzir o custo geral da workload.

Como alternativa, você pode usar a estratégia de alocação `capacity-optimized-prioritized` com um parâmetro de prioridade para ordenar os tipos de instância, da prioridade mais alta para a mais baixa. Você pode definir a mesma prioridade para diferentes tipos de instância. A EC2 Fleet otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades de tipo de instância (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da EC2 Fleet de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante. Observe que quando você define a prioridade para `capacity-optimized-prioritized`, a mesma prioridade também será aplicada às instâncias sob demanda se o `AllocationStrategy` sob demanda estiver definido como `prioritized`.

`diversified`

Os Instâncias spot são distribuídos em todos os grupos de capacidade spot.

`lowest-price` (não recomendado)

> **Warning**
>
> Não recomendamos a estratégia de alocação de `lowest-price` porque ela representa o maior risco de interrupção para as instâncias spot.

As instâncias spot vêm do grupo com o menor preço que tem capacidade disponível. Essa é a estratégia padrão. Porém, recomendamos que você substitua o padrão especificando a estratégia de alocação `price-capacity-optimized`.

Se o grupo com menor preço não tiver capacidade disponível, as instâncias spot virão do próximo grupo com menor preço que tiver capacidade disponível.

Se um grupo esgotar sua capacidade antes de atender a capacidade visada, a frota do EC2 continuará a atender à solicitação recorrendo ao próximo grupo com menor preço. Para garantir que a capacidade desejada seja atendida, é possível receber instâncias spot de vários grupos.

Como essa estratégia considera apenas o preço da instância e não a disponibilidade de capacidade, ela pode resultar em altas taxas de interrupção.

`InstancePoolsToUseCount`

O número de grupos spot para os quais alocar sua capacidade spot de destino. Válido apenas quando a estratégia de alocação está definida como `lowest-price`. A Frota do EC2 seleciona os grupos spot de menor preço e aloca uniformemente a capacidade spot visada pelo número de grupos spot que você especificar.

Observe que o EC2 Fleet tenta extrair instâncias spot a partir do número de pools que você especificar com base no melhor esforço. Se um pool esgotar sua capacidade spot antes de atender a capacidade visada, a Frota do EC2 atenderá a solicitação recorrendo ao próximo grupo de menor custo. Para garantir que sua capacidade de destino seja atendida, você pode receber Instâncias Spot de mais do que o número de pools especificado. Da mesma forma, se a maioria dos pools não tiver capacidade spot, você poderá receber sua capacidade de destino total de menos do que o número de pools que você especificou.

Escolher a estratégia de alocação apropriada

Você pode otimizar a frota para seu caso de uso escolhendo a estratégia apropriada de alocação spot. Para a capacidade visada da instância sob demanda, a Frota do EC2 sempre seleciona o tipo de instância de menor custo com base no preço público sob demanda e continua a seguir a estratégia de alocação (`price-capacity-optimized`, `capacity-optimized`, `diversified` ou `lowest-price`) para as instâncias spot.

Equilibrar menor preço e disponibilidade de capacidade

Para obter o equilíbrio entre os grupos de capacidade spot com menor preço e os grupos de capacidade spot com a maior disponibilidade de capacidade, recomendamos que você use a estratégia de alocação `price-capacity-optimized`. Essa estratégia toma decisões sobre quais grupos devem solicitar instâncias spot com base no preço dos grupos e na disponibilidade de capacidade de instâncias spot nesses grupos. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção em curto prazo, ao mesmo tempo que ainda levaremos o preço em consideração.

Se a frota executar workloads resilientes e sem estado, incluindo aplicações conteinerizadas, microsserviços, aplicações da Web, trabalhos de dados e análises, e processamento em lote, use a estratégia de alocação `price-capacity-optimized` para otimizar a economia de custos e a disponibilidade de capacidade.

Se a frota executar workloads que possam ter um custo de interrupção maior associado ao reinício do trabalho, você deverá implementar verificações para que as aplicações possam ser reiniciadas no ponto em que foram interrompidas. Usando verificações, você torna a estratégia de alocação `price-capacity-optimized` uma boa opção para essas workloads, pois ela aloca a capacidade dos grupos com menor preço que também oferecem uma baixa taxa de interrupção de instâncias spot.

Para ver um exemplo de configuração que usa a estratégia de alocação `price-capacity-optimized`, consulte Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade.

Quando as workloads têm um alto custo de interrupção

Opcionalmente, você pode usar a estratégia `capacity-optimized` se executar workloads que usem tipos de instância com preços semelhantes ou em que o custo da interrupção seja tão significativo que qualquer economia de custos será inadequada em comparação com um aumento marginal nas interrupções. Essa estratégia aloca capacidade dos grupos com capacidade spot mais

disponível que oferecem a possibilidade de menos interrupções, o que pode reduzir o custo geral da workload. Para ver um exemplo de configuração que usa a estratégia de alocação `capacity-optimized`, consulte Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade.

Quando a possibilidade de interrupções precisa ser minimizada, mas a preferência por determinados tipos de instância é importante, é possível expressar as prioridades do seu grupo usando a estratégia de alocação `capacity-optimized-prioritized` e definindo a ordem dos tipos de instância a serem usados por prioridade, da mais alta para a mais baixa. Para obter uma configuração de exemplo, consulte Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades.

Observe que quando você define as prioridades para `capacity-optimized-prioritized`, as mesmas prioridades também serão aplicadas às instâncias sob demanda se `AllocationStrategy` sob demanda estiver definido como `prioritized`.

Quando a workload é flexível em termos de tempo e a disponibilidade de capacidade não é um fator

Se a frota for pequena ou for executada por um período curto, você poderá usar `price-capacity-optimized` para maximizar a economia de custos, ainda levando em conta a disponibilidade de capacidade.

Quando sua frota é grande ou é executada por muito tempo

Se sua frota for grande ou estiver sendo executada há muito tempo, você poderá aprimorar a disponibilidade dela distribuindo as Instâncias spot por vários grupos, usando a estratégia `diversified`. Por exemplo, se a Frota do EC2 especificar 10 grupos e uma capacidade de destino de 100 instâncias, a frota executará 10 Instâncias spot em cada grupo. Se o preço spot para um grupo exceder seu preço máximo para esse mesmo grupo, somente 10% de sua frota será afetada. Usar essa estratégia também torna sua frota menos sensível a aumentos que ocorram com o tempo no preço spot em qualquer grupo específico. Com a estratégia `diversified`, a Frota do EC2 não executará Instâncias spot em nenhum grupo com um preço spot igual ou maior que o preço sob demanda.

Manter a capacidade de destino

Depois que as Instâncias spot são encerradas devido a uma alteração no preço spot ou na capacidade disponível de um grupo de capacidade spot, uma Frota do EC2 do tipo `maintain` executa a substituição de Instâncias spot. A estratégia de alocação determina os grupos dos quais as instâncias de substituição são iniciadas, da seguinte forma:

- Se a estratégia de alocação for `price-capacity-optimized`, a frota iniciará as instâncias de substituição nos grupos com maior disponibilidade de capacidade de instâncias spot, ao mesmo tempo que também levará em consideração o preço e identificará os grupos com menor preço com alta disponibilidade de capacidade.
- Se a estratégia de alocação for `capacity-optimized`, a frota iniciará as instâncias de substituição no grupo com a maior capacidade de instâncias spot disponível.
- Se a estratégia de alocação for `diversified`, a frota distribuirá a instância spot substituta entre os grupos restantes.

Seleção de tipo de instância baseada em atributos para frota do EC2

Ao criar uma frota do EC2, você deve especificar um ou mais tipos de instância para configurar as instâncias sob-demanda e as instâncias spot na frota. Como alternativa à especificação manual dos tipos de instância, você pode especificar os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos. Isso é conhecido como seleção de tipo de instância baseada em atributos. Por exemplo, você pode especificar o número mínimo e máximo de vCPUs necessárias para suas instâncias, e a frota do EC2 iniciará as instâncias usando todos os tipos de instância disponíveis que atendam a esses requisitos de vCPU.

A seleção de tipo de instância baseada em atributos é ideal para workloads e frameworks que possam ser flexíveis em relação a que tipos de instância elas usam, como ao executar contêineres ou frotas da Web, processar big data e implementar ferramentas de integração e implantação contínuas (CI/CD).

Benefícios

A seleção de tipo de instância baseada em atributos oferece os seguintes benefícios:

- Use facilmente os tipos de instâncias certos: com tantos tipos de instância disponíveis, encontrar os tipos de instância corretos para a workload pode ser demorado. Se você especificar os atributos de instância, os tipos de instância terão automaticamente os atributos necessários para sua workload.
- Configuração simplificada: para especificar manualmente vários tipos de instância para uma frota do EC2, crie uma substituição de modelo de lançamento separada para cada tipo de instância. Mas, com a seleção de tipo de instância baseada em atributos, para fornecer vários tipos de instância, você só precisa especificar os atributos das instâncias no modelo de lançamento ou em uma substituição de modelo de lançamento.

- Uso automático de novos tipos de instâncias: quando atributos de instância são especificados em vez de tipos de instância, sua frota pode usar tipos de instância de gerações mais novas à medida que são lançados, tornando a configuração da frota "à prova de obsolescência".
- Flexibilidade dos tipos de instâncias: quando atributos de instância são especificados em vez de tipos de instância, a frota do EC2 pode selecionar entre uma ampla variedade de tipos de instância para iniciar instâncias spot, o que atende à Prática recomendada para instâncias spot: flexibilidade de tipo de instância.

Tópicos

- Como funciona a seleção de tipo de instância baseada em atributos
- Proteção de preço
- Considerações
- Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos
- Exemplos de configurações que são válidas e não válidas
- Previsualizar os tipos de instância com os atributos especificados

Como funciona a seleção de tipo de instância baseada em atributos

Para usar a seleção de tipo de instância baseada em atributos na configuração de frota, substitua a lista dos tipos de instância por uma lista dos atributos de instância que suas instâncias requerem. A Frota do EC2 iniciará instâncias em todos os tipos de instância disponíveis que tenham os atributos de instância especificados.

Tópicos

- Tipos de atributos de instância
- Onde configurar a seleção de tipo de instância baseada em atributos
- Como a Frota do EC2 usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

Tipos de atributos de instância

Há vários atributos de instância que você pode especificar para expressar seus requisitos de computação, p. ex.:

- Contagem de vCPUs: o número mínimo e máximo de vCPUs por instância.

- Memória: o mínimo e o máximo de GiBs de memória por instância.
- Armazenamento local: se o sistema deve usar o EBS ou volumes de armazenamento de instâncias para armazenamento local.
- Desempenho intermitente: se o sistema deve usar a família de instâncias T, incluindo os tipos T4g, T3a, T3 e T2.

Para obter uma descrição de cada atributo e os valores padrão, consulte InstanceRequirements na Referência de API do Amazon EC2.

Onde configurar a seleção de tipo de instância baseada em atributos

Dependendo de você usar o console ou a AWS CLI, é possível especificar os atributos de instância para a seleção de tipo de instância baseada em atributos da seguinte forma:

No console, você pode especificar os atributos de instância no seguinte componente de configuração de frota:

- Em um modelo de inicialização, referencie o modelo de inicialização na solicitação da frota

Na AWS CLI, você pode especificar os atributos de instância em um ou ambos os componentes de configuração de frota a seguir:

- Em um modelo de inicialização, referencie o modelo de inicialização na solicitação da frota
- Em uma substituição de modelo de lançamento

  Se desejar uma combinação de instâncias que usam AMIs diferentes, você pode especificar atributos de instância em várias substituições de modelo de lançamento. Por exemplo, diferentes tipos de instância podem usar processadores baseados em x86 e Arm.

Como a Frota do EC2 usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

A Frota do EC2 provisiona uma frota da seguinte maneira:

- A Frota do EC2 identifica os tipos de instância que têm os atributos especificados.
- A Frota do EC2 usa proteção de preço para determinar quais tipos de instância excluir.

- A Frota do EC2 determina os grupos de capacidade dos quais considerará iniciar as instâncias com base nas regiões ou zonas de disponibilidade da AWS que têm os tipos de instância correspondentes.
- A Frota do EC2 aplica a estratégia de alocação especificada para determinar os grupos de capacidade dos quais as instâncias serão iniciadas.

  Observe que a seleção de tipo de instância baseada em atributos não escolhe os grupos de capacidade dos quais provisionar a frota; isso cabe às estratégias de alocação.

  Se você especificar uma estratégia de alocação, a Frota do EC2 iniciará as instâncias de acordo com a estratégia de alocação especificada.
  - Para instâncias spot, a seleção de tipo de instância baseada em atributos é compatível com as estratégias de alocação `price-capacity-optimized`, `capacity-optimized` e `lowest-price`. Não recomendamos a estratégia de alocação de spots `lowest-price` porque ela representa o maior risco de interrupção para as instâncias spot.
  - Para instâncias sob demanda, a seleção de tipo de instância baseada em atributos oferece suporte à estratégia de alocação de `lowest-price`.
- Se não houver capacidade para os tipos de instância com os atributos de instância especificados, nenhuma instância poderá ser iniciada e a frota retornará um erro.

Proteção de preço

A proteção de preços é um recurso que impede que sua Frota do EC2 use tipos de instância que você consideraria muito caros, mesmo que atendam aos atributos especificados. Para usar a proteção de preço, você define um limite de preço. Em seguida, quando o Amazon EC2 selecionar tipos de instância com seus atributos, ele excluirá os tipos de instância que tenham preços acima do limite.

A forma como o Amazon EC2 calcula o limite de preço é a seguinte:

- Primeiro, o Amazon EC2 identifica o tipo de instância com o menor preço dentre aqueles que correspondem aos seus atributos.
- Em seguida, o Amazon EC2 pegará o valor (expresso como uma porcentagem) que você especificou para o parâmetro de proteção de preço e o multiplicará pelo preço do tipo de instância identificado. O resultado é o preço usado como o limite de preço.

Há limites distintos de preço para instâncias sob demanda e instâncias spot.

Quando você cria uma frota com seleção de tipo de instância baseada em atributos, a proteção de preço é habilitada por padrão. É possível manter os valores padrão ou especificar seus próprios valores.

Você também pode desativar a proteção de preços. Para indicar que não há limite de proteção de preço, especifique um valor percentual alto, como 999999.

Tópicos

- Identificação do tipo de instância com o menor preço
- Proteção de preço de instância sob demanda
- Proteção de preço de instância spot
- Especificar o limite de proteção de preço

Identificação do tipo de instância com o menor preço

O Amazon EC2 determina o preço básico do limite de preço ao identificar o tipo de instância com o menor preço dentre aquelas que correspondem aos atributos especificados. Ele faz isso da seguinte maneira:

- Primeiro, ele analisa os tipos de instância C, M ou R da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.
- Se não houver uma correspondência, ele analisará os tipos de instância da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.
- Se não houver correspondência, ele examinará todos os tipos de instância da geração anterior que correspondam aos seus atributos e identificará o tipo de instância com o menor preço.

Proteção de preço de instância sob demanda

O limite de proteção de preço para tipos de instância sob demanda é calculado como uma porcentagem maior do que o tipo de instância sob demanda de menor preço identificado (`OnDemandMaxPricePercentageOverLowestPrice`). Você especifica maior a porcentagem que está disposto a pagar. Se você não especificar esse parâmetro, um valor padrão de `20` será usado para calcular um limite de proteção de preço 20% superior ao preço identificado.

Por exemplo, se o preço da instância sob demanda identificada for `0.4271`, e você especificar `25`, o limite de preço será 25% maior que `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 1.25 = 0.533875`. O preço calculado é o máximo que você está disposto a pagar por instâncias sob demanda e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância sob demanda com preço superior a `0.533875`.

Proteção de preço de instância spot

Por padrão, o Amazon EC2 aplicará automaticamente a proteção de preço de instância spot ideal para selecionar de forma consistente entre uma ampla variedade de tipos de instância. Você também pode definir manualmente a proteção de preço. No entanto, deixar que o Amazon EC2 faça isso por você pode aumentar a probabilidade de que sua capacidade de spot seja atendida.

É possível especificar manualmente a proteção de preço usando uma das opções a seguir. Se você definir manualmente a proteção de preço, recomendamos usar a primeira opção.

- Um percentual do tipo de instância sob demanda com o menor preço identificado [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Por exemplo, se o preço do tipo de instância sob demanda identificada for `0.4271`, e você especificar `60`, o limite de preço será 60% de `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 0.60 = 0.25626`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.25626`.
- Um percentual maior do que o tipo de instância spot com o menor preço identificado [`SpotMaxPricePercentageOverLowestPrice`]

  Por exemplo, se o preço do tipo de instância spot identificada for `0.1808`, e você especificar `25`, o limite de preço será 25% maior que `0.1808`. Isso é calculado da seguinte forma: `0.1808 * 1.25 = 0.226`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.266`. Não é recomendável usar esse parâmetro, pois os preço spot podem flutuar e, portanto, seu limite de proteção de preço também poderá flutuar.

Especificar o limite de proteção de preço

Para especificar o limite de proteção de preço

Ao criar a frota do EC2, configure a frota para seleção de tipo de instância baseada em atributos e então faça o seguinte:

- Para especificar o limite de proteção de preço da instância sob demanda, no arquivo de configuração JSON, em estrutura `InstanceRequirements`, para `OnDemandMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.
- Para especificar o limite de proteção de preço da instância spot, no arquivo de configuração JSON, na estrutura `InstanceRequirements`, especifique um destes parâmetros:
  - Para `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, insira o limite de proteção de preço como uma porcentagem.
  - Para `SpotMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.

Para obter mais informações sobre a criação de uma frota, consulte Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos.

> **Note**
>
> Ao criar a Frota do EC2, se você definir `TargetCapacityUnitType` para `vcpu` ou `memory-mib`, o limite de proteção de preço é aplicado com base no preço por VCPU ou por memória, em vez do preço por instância.

Considerações

- Você pode especificar tipos de instância ou atributos de instância em uma Frota do EC2, mas não ambos ao mesmo tempo.

  Ao usar a CLI, as substituições do modelo de lançamento prevalecerão sobre o modelo de lançamento. Por exemplo, se o modelo de lançamento contiver um tipo de instância e a substituição do modelo de lançamento contiver atributos de instância, as instâncias identificadas pelos atributos da instância prevalecerão sobre o tipo de instância no modelo de lançamento.

- Ao usar a CLI, quando você especifica atributos de instância como substituições, não pode especificar também pesos ou prioridades.
- Você pode especificar, no máximo, quatro estruturas de `InstanceRequirements` em uma configuração de solicitação.

Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos

Você pode configurar uma frota para usar a seleção de tipo de instância baseada em atributos usando a AWS CLI.

Para criar uma Frota do EC2 com a seleção de tipo de instância baseada nos atributos (AWS CLI)

Use o comando create-fleet (AWS CLI) para criar uma frota do EC2. Especifique a configuração da frota em um arquivo JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Exemplo de arquivo *file_name*`.json`

O exemplo a seguir contém os parâmetros que configuram uma Frota do EC2 para usar a seleção de tipo de instância baseada nos atributos e é seguido de um texto explicativo.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
```

```
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Os parâmetros para a seleção de tipo de instância baseada nos atributos são especificados na estrutura `InstanceRequirements`. Neste exemplo, dois atributos são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a Frota do EC2 provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

> **Note**
>
> Quando `InstanceRequirements` for incluído na configuração da frota, `InstanceType` e `WeightedCapacity` devem ser excluídos; eles não podem determinar a configuração da frota ao mesmo tempo que os atributos da instância.

O JSON também contém a seguinte configuração de frota:

- `"AllocationStrategy": "price-capacity-optimized"`: a estratégia de alocação para as instâncias spot na frota.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: o modelo de inicialização contém algumas informações de configuração da instância, mas se algum

tipo de instância for especificado, ele será substituído pelos atributos especificados em `InstanceRequirements`.

- `"TotalTargetCapacity": 20`: a capacidade visada é de 20 instâncias.
- `"DefaultTargetCapacityType": "spot"`: a capacidade padrão é instâncias spot.
- `"Type": "instant"`: o tipo de solicitação para a frota é `instant`.

Exemplos de configurações que são válidas e não válidas

Se você usar a AWS CLI para criar uma Frota do EC2, deve garantir que a configuração de frota seja válida. Exemplos de configurações que são válidas e não válidas.

As configurações são consideradas não válidas quando contiverem o seguinte:

- Uma única estrutura de `Overrides` com `InstanceRequirements` e `InstanceType`
- Duas estruturas de `Overrides`, uma com `InstanceRequirements` e outra com `InstanceType`
- Duas estruturas de `InstanceRequirements` com valores de atributo sobrepostos na mesma `LaunchTemplateSpecification`

Exemplos de configuração

- Configuração válida: modelo de lançamento único com substituições
- Configuração válida: modelo de lançamento único com vários InstanceRequirements
- Configuração válida: dois modelos de lançamento com substituições em cada
- Configuração válida: somente InstanceRequirements especificados, sem valores de atributo sobrepostos
- Configuração não válida: Overrides contémInstanceRequirements e InstanceType
- Configuração não válida: duas Overrides contêm InstanceRequirements e InstanceType
- Configuração não válida: valores de atributo sobrepostos

Configuração válida: modelo de lançamento único com substituições

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. A seguir está um texto explicativo do exemplo de configuração.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Para usar a seleção de instância baseada em atributos, você deve incluir a estrutura de `InstanceRequirements` na configuração de frota e especificar os atributos desejados para as instâncias da frota.

No exemplo anterior, os seguintes atributos de instância foram especificados:

- `VCpuCount`: os tipos de instância devem ter no mínimo 2 e no máximo 8 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no máximo 10.240 MiB de memória. Um mínimo de 0 indica que não há limite mínimo.
- `MemoryGiBPerVCpu`: os tipos de instância devem ter no máximo 10.000 GiB de memória. O parâmetro `Min` é opcional. Ao omiti-lo, você indica que não há limite mínimo.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs. A Frota do EC2 iniciará instâncias suficientes para que o número total de vCPUs na frota seja 5.000 vCPUs.

Configuração válida: modelo de lançamento único com vários InstanceRequirements

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo duas estruturas de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração válida: dois modelos de lançamento com substituições em cada

A configuração a seguir é válida. Ela contém dois modelos de lançamento, cada um deles com uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. Essa configuração é útil para oferecer suporte às arquiteturas `arm` e `x86` na mesma frota.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
```

```
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração válida: somente **`InstanceRequirements`** especificados, sem valores de atributo sobrepostos

A configuração a seguir é válida. Ela contém duas estruturas de `LaunchTemplateSpecification`, cada uma com um modelo de lançamento e uma estrutura `Overrides` contendo uma estrutura de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
        "LaunchTemplateConfigs": [
```

```
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
```

```
}
```

Configuração não válida: **`Overrides`** contém**`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. A estrutura de `Overrides` contém `InstanceRequirements` e `InstanceType`. Em `Overrides`, você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração não válida: duas **`Overrides`** contêm **`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. As estruturas `Overrides` contêm `InstanceRequirements` e `InstanceType`. Você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos, mesmo que estejam em estruturas de `Overrides` diferentes.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
```

```
    }
}
```

Configuração não válida: valores de atributo sobrepostos

A configuração a seguir não é válida. As duas estruturas de `InstanceRequirements` contêm `"VCpuCount": {"Min": 0, "Max": 2}`. Os valores desses atributos se sobrepõem, o que resultará em grupos de capacidade duplicados.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
```

```
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Previsualizar os tipos de instância com os atributos especificados

Você pode usar o comando get-instance-types-de-instance-requirements da AWS CLI para previsualizar os tipos de instância que correspondem aos atributos especificados por você. Isso é especialmente útil para determinar quais atributos especificar na configuração da solicitação sem iniciar nenhuma instância. Observe que o comando não considera a capacidade disponível.

Para previsualizar uma lista de tipos de instância especificando atributos usando a AWS CLI

1. (Opcional) Para gerar todos os atributos possíveis que podem ser especificados, use o comando get-instance-types-de-instance-requirements e o parâmetro `--generate-cli-skeleton`. Opcionalmente, você pode direcionar a saída para um arquivo e salvá-lo usando `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Saída esperada

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
               "Min": 0,
               "Max": 0
           },
           "MemoryMiB": {
               "Min": 0,
   ```

```
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
```

```
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Crie um arquivo de configuração JSON usando a saída da etapa anterior e configure-o da seguinte forma:

> **Note**
>
> Você deve fornecer valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Você pode omitir os outros atributos; quando omitidos, os valores padrão são usados.
> Para obter uma descrição de cada atributo e seus valores padrão, consulte get-instance-types-de-instance-requirements na Referência da linha de comando do Amazon EC2.

a. Em `ArchitectureTypes`, especifique um ou mais tipos de arquitetura de processador.

b. Em `VirtualizationTypes`, especifique um ou mais tipos de virtualização.

c. Em `VCpuCount`, especifique o número mínimo e máximo de vCPUs. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

d. Em `MemoryMiB`, especifique a quantidade mínima e máxima de memória em MiB. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

e. Opcionalmente, você pode especificar um ou mais dos outros atributos para restringir ainda mais a lista de tipos de instância retornados.

3. Para previsualizar os tipos de instância que têm os atributos que você especificou no arquivo JSON, use o comando get-instance-types-from-instance-requirements e especifique o nome e o caminho para seu arquivo JSON usando o parâmetro `--cli-input-json`. Opcionalmente, você pode formatar a saída para ser exibida em formato de tabela.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Exemplo de arquivo *attributes.json*

Neste exemplo, os atributos necessários estão incluídos no arquivo JSON. Eles são `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Além disso, o atributo opcional `InstanceGenerations` também está incluído. Observe que para `MemoryMiB`, o valor `Max` pode ser omitido para indicar que não há limite.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
```

```
    }
}
```

Exemplo de saída

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Após identificar os tipos de instância que atendem às suas necessidades, anote os atributos de instância usados para que poder usá-los ao configurar a solicitação de frota.

Configurar Frota do EC2 para backup sob demanda

Se houver a necessidade de escalas urgentes e imprevisíveis, como um site de notícias que deve ser dimensionado durante um grande evento de notícias ou execução de um jogo, recomendamos que você especifique tipos alternativos de instâncias para suas Instâncias on-demand, caso sua opção preferida não tenha capacidade disponível suficiente. Por exemplo, você pode preferir `c5.2xlarge` Instâncias on-demand, mas se não houver capacidade suficiente disponível, poderá usar algumas instâncias `c4.2xlarge` durante o pico de carga. Neste caso, a Frota do EC2 tenta atender a toda sua capacidade de destino usando instâncias `c5.2xlarge`, mas se não houver capacidade suficiente, ela executará automaticamente as instâncias `c4.2xlarge` para atender à capacidade de destino.

Tópicos

- Priorizar tipos de instâncias para capacidade sob demanda
- Use Reservas de Capacidade para Instâncias on-demand

Priorizar tipos de instâncias para capacidade sob demanda

Quando Frota do EC2 tenta atender à sua capacidade sob demanda, o padrão é iniciar primeiro o tipo de instância de menor preço. Se `AllocationStrategy` estiver definido como `prioritized`, Frota do EC2 usará a prioridade para determinar qual tipo de instância será o primeiro para atender a capacidade sob demanda. A prioridade é atribuída à substituição do modelo de ativação, e a prioridade mais alta é lançada primeiro.

Exemplo: priorizar tipos de instância

Neste exemplo, você configura três substituições de modelo de execução, cada uma com um tipo de instância diferente.

O preço sob demanda para os tipos de instância varia no preço. Estes são os tipos de instância usados neste exemplo, listados em ordem de preço, a partir do tipo de instância mais barato:

- `m4.large`: menor custo
- `m5.large`
- `m5a.large`

Se você não usar prioridade para determinar a ordem, a frota atenderá à capacidade sob demanda começando pelo tipo mais barato de instância.

No entanto, digamos que você tenha instâncias reservadas `m5.large` não utilizadas que deseja usar primeiro. É possível definir a prioridade de substituição do modelo de execução para que os tipos de instância sejam usados na ordem de prioridade, da seguinte forma:

- `m5.large`: prioridade 1
- `m4.large`: prioridade 2
- `m5a.large`: prioridade 3

Use Reservas de Capacidade para Instâncias on-demand

Com as Reservas de Capacidade sob demanda, você pode reservar capacidade computacional para suas Instâncias sob demanda em uma determinada zona de disponibilidade por qualquer duração. É possível configurar uma Frota do EC2 para usar as Reservas de Capacidade primeiro ao iniciar Instâncias sob demanda.

As Reservas de Capacidade são configuradas como `open` ou `targeted`. A frota EC2 pode iniciar Instâncias sob demanda nas Reservas de Capacidade `open` ou `targeted`, da seguinte forma:

- Se uma Reserva de capacidade é `open`, as Instâncias sob demanda que tiverem atributos correspondentes serão executadas automaticamente na capacidade reservada.
- Se uma Reserva de capacidade for `targeted`, as Instâncias sob demanda deverão usá-la como destino especificamente para executar na capacidade reservada. Isso é útil para usar Reservas de Capacidade específicas ou para controlar quando usar Reservas de Capacidade específicas.

Se você usar Reservas de Capacidade `targeted` em sua frota EC2, deve haver Reservas de Capacidade suficientes para atender à capacidade sob demanda de destino, caso contrário, o lançamento falhará. Para evitar uma falha no lançamento, adicione as Reservas de Capacidade `targeted` a um grupo de recursos e, em seguida, direcione o grupo de recursos. O grupo de recursos não precisa ter Reservas de Capacidade suficientes; se ficar sem Reservas de Capacidade antes que a capacidade sob demanda de destino seja atendida, a frota poderá iniciar a capacidade de destino restante na capacidade sob demanda regular.

Para usar Reservas de Capacidade com a frota EC2

1. Configurar a frota como tipo `instant`. Não é possível usar Reservas de Capacidade para frotas de outros tipos.
2. Configure a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`.
3. No modelo de lançamento, para Reserva de capacidade, escolha Aberto ou Destino por grupo. Se escolher Destino por grupo, especifique o ID do grupo de recursos de Reservas de Capacidade.

Quando a frota tenta atender à capacidade sob demanda, se descobrir que vários grupos de instâncias têm Reservas de Capacidade correspondentes não utilizadas, ela determina os grupos nos quais iniciar as Instâncias sob demanda com base na estratégia de alocação sob demanda (`lowest-price` ou `prioritized`).

Para obter exemplos de como configurar uma frota para usar Reservas de Capacidade para atender à capacidade sob demanda, consulte Exemplos de configuração de Frota do EC2, especificamente os Exemplos 5 a 7.

Para obter informações sobre configuração das Reservas de Capacidade, consulte On-Demand Capacity Reservations e as Perguntas frequentes sobre Reservas de Capacidade.

Rebalanceamento de capacidade

Você pode configurar a EC2 Fleet para iniciar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento para notificar que uma instância spot está em um risco elevado de interrupção. O rebalanceamento de capacidade ajuda a manter a disponibilidade da workload aumentando proativamente sua frota com uma nova instância spot antes que uma instância em execução seja interrompida por Amazon EC2. Para ter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.

Para configurar a frota do EC2 para executar uma instância spot de substituição, use o comando create-fleet (AWS CLI) e os parâmetros relevantes na estrutura de `MaintenanceStrategies`. Para obter mais informações, consulte o exemplo de configuração de execução.

Limitações

- O rebalanceamento de capacidade só está disponível para frotas do tipo `maintain`.
- Quando a frota estiver em execução, não é possível modificar a configuração de rebalanceamento de capacidade. Para alterar a configuração de rebalanceamento de capacidade, você deve excluir a frota e criar uma nova.

Opções de configuração

A `ReplacementStrategy` para Frota do EC2 oferece suporte a estes dois valores:

`launch-before-terminate`

O Amazon EC2 termina as Instâncias spot que recebem uma notificação de rebalanceamento após o lançamento de novas Instâncias spot de substituição. Se você especificar `launch-before-terminate`, também deverá especificar um valor para `termination-delay`. Depois que as novas instâncias de substituição são iniciadas, o Amazon EC2 aguarda o período de `termination-delay` e, em seguida, encerra as instâncias antigas. Em `termination-delay`, o mínimo é de 120 segundos (2 minutos) e o máximo é de 7.200 segundos (2 horas).

Recomendamos o uso de `launch-before-terminate` apenas se você puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento. Observe

que o Amazon EC2 pode interromper as instâncias antigas com um aviso dois minutos antes do período de `termination-delay`.

Recomendamos muito não usar a estratégia de alocação de `lowest-price` em combinação com `launch-before-terminate` para evitar ter instâncias spot substitutas que também apresentem risco elevado de interrupção.

`launch`

O Amazon EC2 inicia instâncias spot de substituição quando uma notificação de rebalanceamento é emitida para as instâncias spot existentes. O Amazon EC2 não termina automaticamente as instâncias que recebem uma notificação de rebalanceamento. Você pode terminar as instâncias antigas ou deixá-las em execução. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

Considerações

Se você configurar uma Frota do EC2 para rebalanceamento de capacidade, considere o seguinte:

Forneça o maior número possível de grupos de capacidade spot na solicitação

Configure sua Frota do EC2 para usar vários tipos de instância e zonas de disponibilidade. Isso oferece a flexibilidade para executar instâncias spot em vários grupos de capacidade spot. Para ter mais informações, consulte Ser flexível sobre tipos de instância e zonas de disponibilidade.

Evitar um risco elevado de interrupção das instâncias spot substitutas

As Instâncias spot substitutas podem apresentar um risco elevado de interrupção se você usar a estratégia de alocação de `lowest-price`. Isso ocorre porque o Amazon EC2 sempre iniciará instâncias no grupo de preços mais baixos que tenha capacidade disponível naquele momento, mesmo que exista a probabilidade de que as instâncias spot de substituição sejam interrompidas logo após serem iniciadas. Para evitar um risco elevado de interrupção, recomendamos muito não usar a estratégia de alocação de `lowest-price` e, em vez disso, recomendamos o uso da estratégia de `capacity-optimized` ou `capacity-optimized-prioritized`. Essas estratégias garantem que as instâncias spot substitutas sejam iniciadas nos grupos de capacidade spot ideais e, portanto, tenham menos probabilidade de serem interrompidas em futuro próximo. Para ter mais informações, consulte Usar a estratégia de alocação otimizada para preço e capacidade.

O Amazon EC2 Auto Scaling só iniciará uma nova instância se a disponibilidade for igual ou superior

Um dos objetivos do rebalanceamento de capacidade é melhorar a disponibilidade de uma instância spot. Se uma instância spot existente receber uma recomendação de rebalanceamento, o Amazon EC2 só iniciará uma nova instância caso a nova instância forneça uma disponibilidade igual ou superior a da instância existente. Se o risco de interrupção de uma nova instância for pior do que a instância existente, o Amazon EC2 não iniciará uma nova instância. No entanto, o Amazon EC2 continuará a avaliar os grupos de capacidade spot e iniciará uma nova instância se a disponibilidade melhorar.

Há uma chance de que a instância existente seja interrompida sem que o Amazon EC2 inicie proativamente uma nova instância. Quando isso acontecer, o Amazon EC2 tentará iniciar uma nova instância, independentemente de a nova instância ter um alto risco de interrupção.

O Rebalanceamento da capacidade não aumenta a taxa de interrupção de instâncias Spot

Quando o Rebalanceamento da capacidade é habilitado, ele não aumenta a Taxa de interrupção de instâncias Spot (o número de instâncias Spot que são recuperadas quando o Amazon EC2 precisa novamente de capacidade). Porém, se o rebalanceamento da capacidade detectar que uma instância está em risco de interrupção, o Amazon EC2 tentará iniciar imediatamente uma nova instância. O resultado é que pode haver a substituição de mais instâncias do que se você esperasse que o Amazon EC2 iniciasse uma nova instância depois que a instância em risco fosse interrompida.

Mesmo podendo substituir mais instâncias com o Rebalanceamento da capacidade habilitado, você se beneficia de ser proativo em vez de reativo, tendo mais tempo para agir antes que suas instâncias sejam interrompidas. Com um Aviso de interrupção de instâncias Spot, normalmente você só tem até dois minutos para encerrar sua instância sem problemas. Com o Rebalanceamento da capacidade iniciando uma nova instância com antecedência, os processos existentes têm maiores chances de serem concluídos na instância em risco. Além disso, você pode iniciar os procedimentos de desligamento da instância e impedir que novos trabalhos sejam agendados na instância em risco. Você também pode começar a preparar a instância recém-lançada para assumir o controle da aplicação. Com a substituição proativa do Rebalanceamento da capacidade, você se beneficia com uma continuidade tranquila.

Como exemplo teórico para demonstrar os riscos e benefícios do uso do Rebalanceamento da capacidade, considere o seguinte cenário:

- 14h: uma recomendação de rebalanceamento é recebida para a instância A, e o Amazon EC2 começa imediatamente a tentar iniciar uma instância B de substituição, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h30: uma recomendação de rebalanceamento é recebida para a instância-B, substituída pela instância-C, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h32: se o Rebalanceamento da capacidade não estivesse habilitado e um aviso de interrupção de instância Spot tivesse sido recebido às 14h32 para a instância-A, você teria apenas dois minutos para agir, mas a Instância-A estaria em execução até esse momento.

* Se `launch-before-terminate` for especificado, o Amazon EC2 encerrará a instância em risco depois que a instância de substituição ficar online.

O Amazon EC2 pode iniciar a nova Instâncias spot de substituição até que a capacidade atingida seja o dobro da capacidade visada

Quando uma Frota do EC2 é configurada para rebalanceamento de capacidade, a frota tenta executar uma nova instância spot de substituição para cada instância spot que recebe uma recomendação de rebalanceamento. Depois que uma instância spot recebe uma recomendação de rebalanceamento, ela deixa de ser contada como parte da capacidade atendida. Dependendo da estratégia de substituição, o Amazon EC2 termina a instância após um período espera para término pré-configurado ou a deixa em execução. Isso dá a você a oportunidade de executar ações de rebalanceamento na instância.

Se sua frota atingir o dobro da capacidade de destino, ela interrompe a execução de novas instâncias de substituição, mesmo que as próprias instâncias de substituição recebam uma recomendação de rebalanceamento.

Por exemplo, você cria uma Frota do EC2 com uma capacidade de destino de 100 instâncias spot. Todas as instâncias spot recebem uma recomendação de rebalanceamento, o que faz com que o Amazon EC2 inicie 100 instâncias spot de substituição. Isso eleva o número de instâncias spot atendidas para 200, o que é o dobro da capacidade de destino. Algumas das instâncias de substituição recebem uma recomendação de rebalanceamento, porém nenhuma instância de substituição é executada porque a frota não pode exceder o dobro da capacidade de destino.

Observe que você é cobrado por todas as instâncias durante a execução.

Recomendamos que você configure a Frota do EC2 para terminar instâncias spot que receberem uma recomendação de rebalanceamento

Se você configurar a Frota do EC2 para rebalanceamento de capacidade, recomendamos que só escolha `launch-before-terminate` com um período de espera de término apropriado se puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento.

Se escolher terminar as instâncias recomendadas para rebalanceamento você mesmo, recomendamos que monitore o aviso da recomendação de rebalanceamento recebido pelas instâncias spot na frota. Ao monitorar o sinal, você pode executar rapidamente ações de rebalanceamento nas instâncias afetadas, antes que o Amazon EC2 as interrompa e, em seguida, você pode encerrá-las manualmente. Se você não encerrar as instâncias, continuará pagando por elas enquanto estiverem em execução. O Amazon EC2 não encerra automaticamente as instâncias que recebem uma recomendação de rebalanceamento.

Você pode configurar notificações usando o Amazon EventBridge ou metadados da instância. Para ter mais informações, consulte Monitorar os sinais de recomendação de rebalanceamento.

A Frota do EC2 não conta as instâncias que recebem uma recomendação de rebalanceamento ao calcular a capacidade atendida durante o aumento ou a diminuição

Se a Frota do EC2 estiver configurada para rebalanceamento de capacidade e você alterar a capacidade de destino para aumento ou diminuição, a frota não contará as instâncias marcadas para rebalanceamento como parte da capacidade atendida, como a seguir:

- Reduzir a escala horizontalmente - Se você diminuir a capacidade visada, o Amazon EC2 encerrará instâncias que não estiverem marcadas para rebalanceamento até que a capacidade desejada seja atingida. As instâncias marcadas para rebalanceamento não são contabilizadas para a capacidade atingida.

  Por exemplo, você cria uma Frota do EC2 com uma capacidade visada de 100 instâncias spot, e 10 instâncias recebem uma recomendação de rebalanceamento, portanto, o Amazon EC2 inicia 10 novas instâncias de substituição, resultando em uma capacidade atingida de 110 instâncias. Em seguida, você reduz a capacidade visada para 50 (reduzir a escala horizontalmente), mas a capacidade de atendimento é, na verdade, 60 instâncias porque as 10 instâncias marcadas para rebalanceamento não são encerradas pelo Amazon EC2. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

- Aumentar a escala horizontalmente - Se você aumentar a capacidade visada, o Amazon EC2 iniciará novas instâncias até que a capacidade desejada seja atingida. As instâncias marcadas para reequilíbrio não são contabilizadas para a capacidade atendida.

  Por exemplo, você cria uma EC2 Fleet com uma capacidade planejada de 100 instâncias spot. 10 instâncias recebem uma recomendação de rebalanceamento, portanto, a frota inicia 10 novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você aumenta a capacidade de destino para 200 (aumento), mas a capacidade de atendimento é, na verdade, 210 instâncias porque as 10 instâncias marcadas para rebalanceamento não são contabilizadas pela frota como parte da capacidade de destino. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

Sobreposições de preço máximo

Cada Frota do EC2 pode incluir um preço máximo global ou usar o padrão (preço sob demanda). A frota usa esse preço como o preço máximo padrão em cada uma das suas especificações de execução.

É possível especificar um preço máximo em uma ou mais especificações de execução. Esse preço é específico da especificação de execução. Se uma especificação de execução incluir um preço específico, a Frota do EC2 usará esse preço máximo para substituir o preço máximo global. Qualquer outra especificação de execução que não inclua um preço máximo específico ainda usará o preço máximo global.

Controle de gastos

O Frota do EC2 interrompe as instâncias de lançamento quando atingir um dos seguintes parâmetros: `TotalTargetCapacity` ou `MaxTotalPrice` (a quantidade máxima que você está disposto a pagar). Para controlar a quantidade paga por hora da sua frota, especifique `MaxTotalPrice`. Quando o preço total máximo for alcançado, o Frota do EC2 para de iniciar instâncias mesmo que não tenha atingido a capacidade alvo.

Os exemplos a seguir mostram duas situações diferentes. Na primeira, o Frota do EC2 para de executar instâncias ao atingir a capacidade de destino. Na segunda, o Frota do EC2 para de abrir instâncias ao atingir o valor máximo que você está disposto a pagar (`MaxTotalPrice`).

Exemplo: parar de executar instâncias quando a capacidade de destino for atingida

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

O Frota do EC2 abre 10 Instâncias on-demand, porque o total de 1,00 USD (10 instâncias x 0,10 USD) não excede o `MaxTotalPrice` de 1,50 USD para Instâncias on-demand.

Exemplo: parar de executar instâncias quando o preço máximo total for atingido

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Se o Frota do EC2 executar a capacidade de destino (10 Instâncias on-demand), o custo total por hora será de 1,00 USD. Isso é mais que a quantidade (0,80 USD) especificada para `MaxTotalPrice` para Instâncias on-demand. Para evitar gastar mais do que você pretende, o Frota do EC2 abre somente 8 Instâncias on-demand (abaixo da capacidade de destino sob demanda), porque abrir mais excederia o `MaxTotalPrice` de Instâncias on-demand.

Peso de instâncias da Frota do EC2

Ao criar um Frota do EC2, você pode definir as unidades de capacidade com que cada tipo de instância contribuiria para a performance da aplicação. Você pode ajustar o preço máximo para cada especificação de lançamento usando peso de instâncias.

Por padrão, o preço que você especifica é por hora de instância. Ao usar o recurso de peso da instância, o preço que você especifica é por hora. Você pode calcular o preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A EC2 Fleet calcula o número de instâncias a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino. A frota pode selecionar qualquer grupo que você determinar na especificação de execução, mesmo que a capacidade das instâncias executadas ultrapasse a capacidade de destino solicitada.

A tabela a seguir inclui exemplos de cálculos para determinar o preço por unidade para uma Frota do EC2 com capacidade de destino igual a 10.

Tipo de instância	Peso da instância	Capacidade de destino	Número de instâncias executadas	Preço por hora de instância	Preço por hora
`r3.xlarge`	2	10	5 (10 dividido por 2)	0,05 USD	0,025 USD (0,05 dividido por 2)
`r3.8xlarge`	8	10	2 (10 dividido por 8, resultado arredondado para cima)	0,10 USD	0,0125 USD (0,10 dividido por 8)

Use o peso de instância do Frota do EC2 da maneira a seguir para provisionar a capacidade desejada de destino nos grupos com o menor preço por unidade no momento do atendimento:

1. Defina a capacidade de destino da Frota do EC2 em instâncias (o padrão) ou nas unidades de sua preferência, como CPUs virtuais, memória, armazenamento ou throughput.
2. Defina o preço por unidade.
3. Para cada especificação de execução, defina o peso, que é o número de unidades que o tipo de instância representa em relação à capacidade de destino.

Exemplo de peso da instância

Considere uma solicitação de Frota do EC2 com a seguinte configuração:

- Uma capacidade de destino de 24
- Uma especificação de execução com um tipo de instância `r3.2xlarge` e um peso de 6
- Uma especificação de execução com um tipo de instância `c3.xlarge` e um peso de 5

Os pesos representam o número de unidades que o tipo de instância representa em relação à capacidade de destino. Se a primeira especificação de execução fornecer o menor preço por unidade (preço de `r3.2xlarge` por hora de instância dividido por 6), a Frota do EC2 executará quatro dessas instâncias (24 dividido por 6).

Se a segunda especificação de execução fornecer o menor preço por unidade (preço de `c3.xlarge` por hora de instância dividido por 5), a Frota do EC2 executará cinco dessas instâncias (24 dividido por 5, resultado arredondado para cima).

Peso da instância e estratégia de alocação

Considere uma solicitação de Frota do EC2 com a seguinte configuração:

- Uma capacidade de destino de 30 Instâncias spot
- Uma especificação de execução com um tipo de instância `c3.2xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `m3.xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `r3.xlarge` e um peso de 8

A Frota do EC2 executará quatro instâncias (30 dividido por 8, resultado arredondado para cima). Com a estratégia `diversified`, a frota executa uma instância em cada um dos três grupos, e a quarta instância em qualquer um dos três grupos fornece o menor preço spot por unidade.

Trabalhar com Frotas do EC2

Para usar uma Frota do EC2, crie uma solicitação que inclua a capacidade total de destino, a capacidade sob demanda, a capacidade spot, uma ou mais especificações de execução para as instâncias e o preço máximo que você está disposto a pagar. O solicitação de frota deve incluir um modelo de lançamento que defina as informações de que a frota precisa para executar um instância, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade, e um ou mais grupos de segurança. É possível definir sobreposições de especificação de execução para o tipo de instância, a sub-rede, a zona de disponibilidade e o preço máximo que você está disposto a pagar, além de atribuir capacidade ponderada a cada sobreposição de especificação de execução.

A Frota do EC2 executa Instâncias on-demand quando há capacidade disponível e executa Instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível.

Se a frota incluir a Instâncias spot, o Amazon EC2 poderá tentar manter a capacidade de destino da frota à medida que os preços spot são alterados.

Uma solicitação de tipo de Frota do EC2 `maintain` ou `request` permanecerá ativa até que expire ou você a exclua. Ao excluir uma frota do tipo `maintain` ou `request`, você poderá especificar se a exclusão encerrará ou não as instâncias dessa frota. Caso contrário, as instâncias sob demanda são executadas até que você as encerre e as Instâncias spot são executadas até que sejam interrompidas ou encerradas.

Conteúdo

- Estados das solicitações da Frota do EC2
- Pré-requisitos da Frota do EC2
- Verificações de integridade da Frota do EC2
- Gerar um arquivo de configuração JSON da Frota do EC2
- Criar uma Frota do EC2.
- Marcar uma Frota do EC2
- Descrever a frota do EC2
- Modificar uma Frota do EC2
- Excluir uma Frota do EC2

Estados das solicitações da Frota do EC2

Uma solicitação de Frota do EC2 pode estar em um dos seguintes estados:

`submitted`

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias. A solicitação pode incluir Instâncias on-demand, Instâncias spot, ou ambos. Se uma solicitação for exceder os limites da frota, ela será excluída imediatamente.

`active`

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução. A solicitação permanece nesse estado até que seja alterada ou excluída.

`modifying`

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou que a solicitação seja excluída. Apenas um tipo `maintain` de frota pode ser modificado. Esse estado não se aplica a outros tipos de solicitação.

`deleted_running`

A solicitação de Frota do EC2 foi excluída e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas manualmente. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas. Apenas uma Frota do EC2 do tipo `maintain` ou `request` pode ter instâncias em execução após a solicitação de Frota do EC2 ser excluída. Não há suporte a uma frota `instant` excluída com instâncias em execução. Este estado não se aplica às frotas `instant`.

`deleted_terminating`

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`deleted`

A Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação foi excluída dois dias depois que as instâncias foram encerradas.

Pré-requisitos da Frota do EC2

Para criar uma Frota do EC2, observe os seguintes pré-requisitos:

- Modelo de execução
- Função vinculada ao serviço para Frota do EC2
- Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS
- Permissões para usuários da Frota do EC2

Modelo de execução

Um modelo de execução inclui informações sobre as instâncias a serem executadas, , por exemplo, o tipo de instância, a zona de disponibilidade e o preço máximo que você está disposto a pagar. Para ter mais informações, consulte Executar uma instância a partir de um modelo de execução.

Função vinculada ao serviço para Frota do EC2

O `AWSServiceRoleForEC2Fleet` concede à frota do EC2 permissão para solicitar, executar, encerrar e marcar instâncias em seu nome. O Amazon EC2 usa essa função vinculada ao serviço para concluir as seguintes ações:

- `ec2:RunInstances` – Executar instâncias
- `ec2:RequestSpotInstances` – Solicitação Instâncias spot.
- `ec2:TerminateInstances` – Encerrar instâncias
- `ec2:DescribeImages` – Descrever imagens de máquina da Amazon (AMIs) para Instâncias spot
- `ec2:DescribeInstanceStatus` – Descreva o status das Instâncias spot.
- `ec2:DescribeSubnets` – Descreva as sub-redes para Instâncias spot.
- `ec2:CreateTags` – Adicionar tags a Frota do EC2, instâncias e volumes.

Verifique se essa função está disponível antes de usar a AWS CLI ou uma API para criar uma frota do EC2.

> **Note**
>
> Uma Frota do EC2 `instant` não requer essa função.

Para criar a função, use o console do IAM da seguinte forma.

Para criar a função AWSServiceRoleForEC2Fleet para Frota do EC2

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Roles e Create role.
3. Na página Selecionar tipo da entidade confiável, faça o seguinte:
   a. Em Tipo de entidade confiável, escolha Serviços da AWS.
   b. Em Caso de uso, para Serviço ou caso de uso, escolha EC2 - Frota.

> **Tip**
>
> Certifique-se de escolher EC2 - Frota. Se você escolher EC2, o caso de uso EC2 - Frota não aparecerá na lista de Casos de uso. O caso de uso EC2 - Frota criará

automaticamente uma política com as permissões necessárias do IAM e sugerirá AWSServiceRoleForEC2Fleet como nome do perfil.

c. Escolha Próximo.

4. Na página Adicionar permissões, escolha Próximo.
5. Na página Nomear, revisar e criar, escolha Criar função.

Se você não precisar mais usar Frota do EC2, é recomendável excluir a função AWSServiceRoleForEC2Fleet. Depois que essa função for excluída na sua conta, você poderá criar a função novamente se criar outra frota.

Para obter mais informações, consulte Usar perfis vinculados ao serviço no Guia do usuário do IAM.

Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot criptografado do Amazon EBS na frota do EC2 e usar uma chave do AWS KMS para criptografia, será necessário conceder ao perfil AWSServiceRoleForEC2Fleet permissão para usar a chave gerenciada pelo cliente para que o Amazon EC2 possa iniciar instâncias em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Usar concessões e Usar políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder as permissões para a função AWSServiceRoleForEC2Fleet para usar a chave gerenciada pelo cliente

- Use o comando create-grant para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2Fleet) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é especificada pelo parâmetro `key-id` e o ARN da chave gerenciada pelo cliente. O principal é especificado pelo parâmetro `grantee-principal` e o ARN da função vinculada ao serviço AWSServiceRoleForEC2Fleet.

```
aws kms create-grant \
    --region us-east-1 \
```

```
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Permissões para usuários da Frota do EC2

Se os usuários pretenderem criar ou gerenciar uma Frota do EC2, certifique-se de conceder a eles as permissões necessárias.

Para criar uma frota do EC2

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Criar política.
4. Na página Create policy (Criar política), escolha a guia JSON, substitua texto pelo seguinte e escolha Review policy (Revisar política).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
```

```
}
```

O `ec2:*` concede a um usuário permissão para chamar todas as ações de API do Amazon EC2. Para limitar o usuário a ações de API do Amazon EC2, especifique essas ações.

O usuário deve ter permissão para chamar a ação `iam:ListRoles` para enumerar os perfis do IAM existentes, a ação `iam:PassRole` para especificar o perfil da frota do EC2 e a ação `iam:ListInstanceProfiles` para enumerar os perfis de instância existentes.

(Opcional) Para permitir que um usuário crie perfis ou perfis de instância usando o console do IAM, também é necessário adicionar as ações a seguir à política:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Na página Review policy (Revisar política), digite um nome e uma descrição para a política e escolha Create policy (Criar política).
6. Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

   - Usuários e grupos no AWS IAM Identity Center:

     Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

   - Usuários gerenciados no IAM com provedor de identidades:

     Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

   - Usuários do IAM:

     - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
     - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Verificações de integridade da Frota do EC2

A Frota do EC2 verifica o status de integridade das instâncias na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A Frota do EC2 determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. Uma instância é determinada como `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de status de integridade consecutivas. Para ter mais informações, consulte Verificações de status para as instâncias.

Você pode configurar a sua frota para substituir Instâncias spot não íntegras. Depois de configurar `ReplaceUnhealthyInstances` para `true`, uma instância spot é substituída ao ser reportada como `unhealthy`. A frota poderá ficar abaixo de sua capacidade de destino por alguns minutos enquanto uma instância spot não íntegra estiver sendo substituída.

Requisitos

- A substituição da verificação de integridade é compatível apenas para Frotas do EC2 que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para as frotas únicas do tipo `request` ou `instant`.
- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- Você pode configurar a Frota do EC2 para substituir instâncias não íntegras somente durante sua criação.
- Os usuários só poderão usar a substituição de verificação de integridade se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Para configurar um Frota do EC2 para substituir uma Instâncias spot não íntegra

1. Siga as etapas para criar um Frota do EC2. Para ter mais informações, consulte Criar uma Frota do EC2..
2. Para configurar a frota para substituir Instâncias spot não íntegras no arquivo JSON para `ReplaceUnhealthyInstances`, insira `true`.

Gerar um arquivo de configuração JSON da Frota do EC2

Para visualizar a lista completa de parâmetros de configuração de frota do EC2, você pode gerar um arquivo JSON. Para obter uma descrição de cada parâmetro, consulte create-fleet na Referência de comandos da AWS CLI.

Para gerar um arquivo JSON com todos os parâmetros de Frota do EC2 possíveis usando a linha de comando

- Use o comando create-fleet (AWS CLI) e o parâmetro `--generate-cli-skeleton` para gerar um arquivo JSON da Frota do EC2 e direcione a saída a um arquivo para salvá-la.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Exemplo de saída

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
```

```
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
                        "MemoryGiBPerVCpu": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
```

```
                        "ExcludedInstanceTypes": [
                            ""
                        ],
                        "InstanceGenerations": [
                            "previous"
                        ],
                        "SpotMaxPricePercentageOverLowestPrice": 0,
                        "OnDemandMaxPricePercentageOverLowestPrice": 0,
                        "BareMetal": "included",
                        "BurstablePerformance": "required",
                        "RequireHibernateSupport": true,
                        "NetworkInterfaceCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "LocalStorage": "excluded",
                        "LocalStorageTypes": [
                            "ssd"
                        ],
                        "TotalLocalStorageGB": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "BaselineEbsBandwidthMbps": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorTypes": [
                            "inference"
                        ],
                        "AcceleratorCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorManufacturers": [
                            "amd"
                        ],
                        "AcceleratorNames": [
                            "a100"
                        ],
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
```

```
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Criar uma Frota do EC2.

Para criar uma Frota do EC2, você precisa só especificar os seguintes parâmetros:

- `LaunchTemplateId` ou `LaunchTemplateName`: especifica o modelo de lançamento a ser usado (que contém os parâmetros das instâncias a serem iniciadas, por exemplo, o tipo de instância, a zona de disponibilidade e o preço máximo que você está disposto a pagar)
- `TotalTargetCapacity`: especifica a capacidade-alvo total para a frota
- `DefaultTargetCapacityType`: especifica se a opção de compra padrão é sob demanda ou spot

Você pode definir várias especificações de lançamento que substituem o modelo de lançamento. As especificações de execução podem variar por tipo de instância, zona de disponibilidade, sub-rede e preço máximo e podem incluir uma capacidade ponderada diferente. Como alternativa, especifique os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos. Para obter mais informações, consulte Seleção de tipo de instância baseada em atributos para frota do EC2.

Se você não especificar um parâmetro, a frota usará o valor padrão para o parâmetro.

Especifique os parâmetros da frota em um arquivo JSON. Para ter mais informações, consulte Gerar um arquivo de configuração JSON da Frota do EC2.

No momento, não há suporte de console para a criação de uma frota do EC2.

Para criar uma frota do EC2 (AWS CLI)

- Use o comando create-fleet (AWS CLI) para criar uma frota do EC2 e especificar o arquivo JSON que contém os parâmetros de configuração da frota.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Para obter arquivos de configuração de exemplo, consulte Exemplos de configuração de Frota do EC2.

A seguir está um exemplo de saída de uma frota do tipo `request` ou `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que executou a capacidade de destino.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que executou parte da capacidade de destino com erros em instâncias que não foram executadas.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
```

```
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que não executou nenhuma instância.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Marcar uma Frota do EC2

Para categorizar e gerenciar as solicitações de Frota do EC2, você pode marcá-las com metadados personalizados. Você pode atribuir uma tag a uma solicitação de Frota do EC2 ao criá-la ou posteriormente.

Quando você marca uma solicitação de frota, as instâncias e os volumes que são executados pela frota não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota. Você pode optar por atribuir tags somente à solicitação de frota, somente às instâncias executadas pela frota, somente aos volumes anexados às instâncias executadas pela frota ou aos todos os três.

> **Note**
>
> Para tipos de frota `instant`, é possível marcar volumes anexados a Instâncias on-demand e Instâncias spot. Para os tipos de frota `request` ou `maintain`, só é possível marcar volumes anexados a Instâncias on-demand.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Pré-requisito

Conceda ao usuário permissão para marcar recursos. Para ter mais informações, consulte Exemplo: marcar recursos.

Para conceder a um usuário permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Isso concede ao usuário permissão para criar tags.
- A ação `ec2:CreateFleet`. Isso concede ao usuário permissão para criar uma solicitação de Frota do EC2.
- Para `Resource`, recomendamos que você especifique `"*"`. Permite que os usuários marquem todos os tipos de recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

No momento, não oferecemos suporte para permissões no nível do recurso para o recurso `create-fleet`. Se especificar `create-fleet` como um recurso, você receberá uma exceção não autorizada quando tentar marcar a frota. O exemplo a seguir ilustra como não definir a política.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Como marcar uma nova solicitação de Frota do EC2

Para marcar uma solicitação de Frota do EC2 ao criá-la, especifique o par de valor-chave no arquivo JSON usado para criar a frota. O valor de `ResourceType` deve ser `fleet`. Se você especificar outro valor, ocorrerá falha na frota.

Como marcar instâncias e volumes executado por uma Frota do EC2

Para marcar instâncias e volumes ao serem executados pela frota, especifique as tags no modelo de execução mencionado na solicitação de Frota do EC2.

> **Note**
>
> Não é possível marcar volumes anexados a Instâncias spot que são executados por um tipo de frota `request` ou `maintain`.

Para marcar uma solicitação da frota do EC2, uma instância e um volume existentes (AWS CLI)

Use o comando create-tags para marcar os recursos existentes.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Descrever a frota do EC2

Você pode descrever a frota do EC2, relacionar as instâncias associadas à frota do EC2 e visualizar o histórico da frota do EC2.

Para descrever suas frotas do EC2 (AWS CLI)

Use o comando describe-fleets para descrever suas Frotas do EC2.

```
aws ec2 describe-fleets
```

> **Important**
>
> Se uma frota é do tipo `instant`, você deve especificar o ID da frota, caso contrário, ele não aparece na resposta. Inclua `--fleet-ids` da seguinte forma:

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Exemplo de saída

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
```

```
}
```

Use o comando describe-fleet-instances para descrever as instâncias da Frota do EC2 especificada. A lista retornada das instâncias em execução é atualizada periodicamente e pode estar desatualizada.

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Exemplo de saída

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Use o comando describe-fleet-history para descrever o histórico da Frota do EC2 especificada na hora determinada.

```
aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --
start-time 2018-04-10T00:00:00Z
```

Exemplo de saída

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
```

```
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```

Modificar uma Frota do EC2

Você pode modificar uma Frota do EC2 no estado `submitted` ou `active`. Quando você modifica uma frota, ela entra no estado `modifying`.

Só é possível modificar uma Frota do EC2 do tipo `maintain`. Você não pode modificar uma Frota do EC2 do tipo `request` nem do tipo `instant`.

Você pode modificar os seguintes parâmetros de uma Frota do EC2:

- `target-capacity-specification` – Aumentar ou diminuir a capacidade de destino de `TotalTargetCapacity`, `OnDemandTargetCapacity` e `SpotTargetCapacity`.
- `excess-capacity-termination-policy` – Se as instâncias em execução devem ser encerradas caso a capacidade total de destino da Frota do EC2 fique abaixo do tamanho atual da frota. Os valores válidos são `no-termination` e `termination`.

Quando você aumenta a capacidade de destino, a Frota do EC2 executa as instâncias adicionais de acordo com a opção de compra da instância especificada para `DefaultTargetCapacityType`, ou seja, Instâncias on-demand ou Instâncias spot.

Se `DefaultTargetCapacityType` for `spot`, a Frota do EC2 executará as Instâncias spot adicionais de acordo com sua respectiva estratégia de alocação.

Quando você diminui a capacidade de destino, a Frota do EC2 excluirá todas as solicitações abertas que excedem a nova capacidade de destino. Você pode solicitar que a frota encerre instâncias até o tamanho da frota atingir a nova capacidade de destino. Se a estratégia de alocação for `lowest-price`, a frota encerrará as instâncias com o preço mais alto por unidade. Se a estratégia de alocação for `diversified`, a frota encerrará as instâncias nos grupos. Como alternativa, você pode solicitar que a Frota do EC2 mantenha seu tamanho atual, mas não substitua as Instâncias spot interrompidas ou encerradas manualmente.

Quando uma EC2 Fleet encerra uma instância spot porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Para modificar uma frota do EC2 (AWS CLI)

Use o comando modify-fleet para atualizar a capacidade de destino da Frota do EC2 especificada.

```
aws ec2 modify-fleet \
```

```
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Se estiver diminuindo a capacidade de destino, mas quiser manter a frota com o tamanho atual, você poderá modificar o comando anterior da maneira a seguir.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

Excluir uma Frota do EC2

Caso não precise mais de uma Frota do EC2, você pode excluí-la. Depois que você exclui uma frota, todas as solicitações spot associadas à frota são caneladas, para que nenhuma nova instância spot seja iniciada.

Ao excluir uma Frota do EC2, você deve especificar se deseja encerrar todas as suas instâncias. Isso inclui tanto instâncias sob demanda quanto instâncias spot. Para frotas `instant`, a frota do EC2 deve encerrar as instâncias quando a frota for excluída. Não há suporte a uma frota `instant` excluída com instâncias em execução.

Se você especificar que as instâncias deverão ser encerradas quando a frota for excluída, a frota entrará no estado `deleted_terminating`. Caso contrário, ela entrará no estado `deleted_running` e as instâncias continuarão em execução até que sejam interrompidas ou encerradas manualmente.

Restrições

- Você pode excluir até 25 frotas do tipo `instant` com a mesma solicitação.
- Você pode excluir até 100 frotas do tipo `maintain` ou `request` com a mesma solicitação.
- Você pode excluir até 125 frotas em uma única solicitação, desde que não exceda a cota para cada tipo de frota, conforme especificado acima.
- Nenhuma frota será excluída se você exceder o número especificado de frotas a serem excluídas.
- Até 1000 instâncias podem ser encerradas em uma única solicitação para excluir frotas `instant`.

Para excluir uma frota do EC2 e encerrar as instâncias (AWS CLI)

Use o comando delete-fleets e o parâmetro `--terminate-instances` para excluir a Frota do EC2 especificada e encerrar as instâncias.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Exemplo de saída

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Para excluir uma Frota do EC2 sem encerrar as instâncias (AWS CLI)

Você pode modificar o comando anterior usando o parâmetro `--no-terminate-instances` para excluir a Frota do EC2 especificada sem encerrar as instâncias.

> **Note**
>
> Não há suporte a `--no-terminate-instances` para frotas `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Exemplo de saída

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
```

```
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

Solucionar problemas quando houver falha na exclusão da frota

Em caso de falha na exclusão da Frota do EC2, `UnsuccessfulFleetDeletions` retornará o ID da Frota do EC2, um código de erro e uma mensagem de erro.

Os códigos de erro são:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Solução de problemas de **`ExceededInstantFleetNumForDeletion`**

Se você tentar excluir mais de 25 frotas `instant` em uma única solicitação, o erro `ExceededInstantFleetNumForDeletion` será retornado. Veja a seguir um exemplo de saída deste erro.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
```

```
            "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
            "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
             }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Solução de problemas do **`NoTerminateInstancesNotSupported`**

Se você especificar que as instâncias em uma frota `instant` não devem ser encerradas quando você excluir a frota, o erro `NoTerminateInstancesNotSupported` será retornado. Não há suporte a `--no-terminate-instances` para frotas `instant`. Veja a seguir um exemplo de saída deste erro.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                        "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                        "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
```

Solução de problemas do **`UnauthorizedOperation`**

Se você não tiver permissão para encerrar instâncias, você obterá o erro `UnauthorizedOperation` ao excluir uma frota que deve encerrar suas instâncias. A seguir está a resposta de erro.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
```

```
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Para resolver o erro, você deve adicionar a ação `ec2:TerminateInstances` à política do IAM, conforme mostrado no exemplo a seguir.

```
{
       "Version": "2012-10-17",
       "Statement": [
            {
                "Sid": "DeleteFleetsAndTerminateInstances",
                "Effect": "Allow",
                "Action": [
                       "ec2:DeleteFleets"
                       "ec2:TerminateInstances"
                ],
                "Resource": "*"
            }
       ]
   }
```

Frota spot

A frota spot é um conjunto de instâncias spot e instâncias sob demanda opcionalmente executadas com base nos critérios especificados por você. A frota spot seleciona os grupos de capacidade spot que atendem às suas necessidades e executa instâncias spot para atender à capacidade prevista para a frota. Por padrão, as Frotas spot são definidas para manter a capacidade de destino executando instâncias de substituição depois que as Instâncias spot da frota são encerradas. Você pode enviar uma frota spot como uma solicitação única, que não persiste depois que as instâncias são encerradas. Você pode incluir solicitações de instância sob demanda em uma solicitação de frota spot.

> **Note**
>
> Se você quiser usar um console para criar uma frota que inclua instâncias spot, recomendamos usar um grupo do Auto Scaling em vez da frota spot. Para obter mais informações, consulte Grupos de Auto Scaling com vários tipos de instância e opções de compra no Manual do usuário do Amazon EC2 Auto Scaling.
> Se você quiser usar a AWS CLI para criar uma frota que inclua instâncias spot, recomendamos usar um grupo do Auto Scaling ou uma frota do EC2 em vez da frota spot. A API RequestSpotFleet, na qual a frota spot é baseada, é uma API herdada sem investimento planejado.
> Para obter mais informações sobre as APIs recomendadas a serem usadas, consulte Qual é o melhor método de solicitação spot para usar?

Tópicos

- Tipos de solicitação da frota spot
- Estratégias de configuração de frota spot
- Trabalhar com frotas spot
- Métricas do CloudWatch para frota spot
- Escalabilidade automátia para frota spot

Tipos de solicitação da frota spot

Há dois tipos de solicitações de frota spot:

`request`

Se você configurar o tipo de solicitação como `request`, a frota spot faz uma solicitação assíncrona única da capacidade desejada. Portanto, se a capacidade for reduzida devido a interrupções do spot, a frota não tentará reabastecer as Instâncias spot nem enviará solicitações em grupos de capacidade spot alternativos, se a capacidade não estiver disponível.

`maintain`

Se você configurar o tipo de solicitação como `maintain`, a frota spot faz uma solicitação assíncrona única da capacidade desejada e mantém a capacidade reabastecendo automaticamente quaisquer Instâncias spot interrompidas.

Para especificar o tipo de solicitação no console do Amazon EC2, faça o seguinte ao criar uma solicitação de frota spot:

- Para criar uma frota spot do tipo `request`, desmarque a caixa de seleção Manter a capacidade pretendida.
- Para criar uma frota spot do tipo `maintain`, marque a caixa de seleção Manter a capacidade pretendida.

Para ter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console).

Os dois tipos de solicitações se beneficiam com a estratégia de alocação. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.

Estratégias de configuração de frota spot

A frota spot é uma coleção, ou frota, de instâncias spot e, opcionalmente, instâncias sob demanda.

A frota spot tenta executar o número de instâncias spot e instâncias sob demanda para atender à capacidade desejada especificada na solicitação de frota spot. A solicitação de Instâncias spot será atendida se houver capacidade disponível e se o preço máximo especificado na solicitação exceder o preço spot atual. A frota spot também tenta manter sua frota de capacidade pretendida se as instâncias spot forem interrompidas.

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e a frota spot executará instâncias até alcançar o valor máximo. Quando o valor máximo que você

está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

Um Grupo de capacidade Spot é um conjunto de instâncias do EC2 não usadas com o mesmo tipo de instância (por exemplo `m5.large`), sistema operacional, zona de disponibilidade e plataforma de rede. Ao criar uma solicitação de frota spot, você poderá incluir várias especificações de execução, que variam de acordo com o tipo de instância, a AMI, a zona de disponibilidade ou a sub-rede. A frota spot seleciona os grupos de capacidade spot que são usados para atender à solicitação com base nas especificações de execução incluídas na sua solicitação de frota spot e na configuração da solicitação de frota spot. As Instâncias spot vêm dos grupos selecionados.

Conteúdo

- Planejar uma solicitação de frota spot
- Estratégias de alocação para Instâncias spot
- Seleção de tipo de instância baseada em atributos para frota spot
- Sob demanda na frota spot
- Rebalanceamento de capacidade
- Substituições do preço spot
- Controle de gastos
- Peso de instâncias de frotas spot

Planejar uma solicitação de frota spot

Antes de criar uma solicitação de frota spot, leia as Práticas recomendadas de spot. Use essas melhores práticas ao planejar a solicitação de frota spot para que você possa provisionar o tipo de instância desejado com o menor preço possível. Também recomendamos fazer o seguinte:

- Determine se você deseja criar uma frota spot que envie uma solicitação única para a capacidade de destino desejada ou uma frota spot que mantenha uma capacidade de destino ao longo do tempo.
- Determine os tipos de instâncias que atendem aos requisitos do aplicativo.
- Determine a capacidade de destino da solicitação de frota spot. Você pode definir a capacidade de destino em instâncias ou em unidades personalizadas. Para ter mais informações, consulte Peso de instâncias de frotas spot.

- Determine a parte da capacidade de destino da frota spot que deve ser sob demanda. Você pode especificar 0 para a capacidade sob demanda.
- Determine seu preço por unidade, se você estiver usando o peso de instância. Para calcular o preço por unidade, divida o preço por hora de instância pelo número de unidades (ou peso) que essa instância representa. Se você não estiver usando o peso de instância, o preço padrão por unidade será o preço por hora de instância.
- Leia as opções possíveis para a solicitação de frota spot. Para obter mais informações, consulte o comando request-spot-fleet na Referência de comandos da AWS CLI. Para obter exemplos adicionais, consulte Exemplos de configuração de frota spot.

Estratégias de alocação para Instâncias spot

Sua configuração de inicialização determina todos os possíveis grupos de capacidade spot (tipos de instância e zonas de disponibilidade) nos quais a frota spot pode iniciar instâncias spot. No entanto, ao iniciar instâncias, a frota spot usa a estratégia de alocação que você especifica para escolher os grupos específicos de todos os seus grupos possíveis.

> **Note**
>
> (Somente para instâncias do Linux) Se você configurar a instância spot para iniciar com o AMD SEV-SNP ativado, será cobrada uma taxa de utilização por hora adicional equivalente a 10% da taxa horária sob demanda para o tipo de instância selecionado. Se a estratégia de alocação usar o preço como entrada, a frota do EC2 não incluirá essa tarifa adicional; somente o preço spot será usado.

Estratégias de alocação

É possível especificar uma destas estratégias de alocação para suas instâncias spot:

`priceCapacityOptimized` (recomendado)

A frota spot identifica os grupos com maior disponibilidade de capacidade para o número de instâncias em execução. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo. Em seguida, a frota spot solicita instâncias spot do grupo com menor preço entre esses grupos.

A estratégia de alocação `priceCapacity0ptimized` é a ideal para a maioria das workloads spot, como aplicações conteinierizadas sem estado, microsserviços, aplicações da Web, trabalhos de dados e análise, e processamento em lote.

`capacity0ptimized`

A frota spot identifica os grupos com maior disponibilidade de capacidade para o número de instâncias em execução. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo. Opcionalmente, você pode definir uma prioridade para cada tipo de instância na frota usando o `capacity0ptimizedPrioritized`. A frota spot otimiza a capacidade primeiro, mas empenha-se em honrar as prioridades de tipo de instância.

Com as Instâncias spot, a definição de preço muda lentamente ao longo do tempo com base em tendências de longo prazo na oferta e na demanda, mas a capacidade oscila em tempo real. A estratégia `capacity0ptimized` executa Instâncias spot automaticamente nos grupos mais disponíveis observando dados de capacidade em tempo real e prevendo quais são os mais disponíveis. Isso funciona bem para workloads que podem ter um custo de interrupção maior associado ao reinício do trabalho, como workloads de integração contínua (CI) longa, de renderização de imagens e mídia, de aprendizado profundo e de computação de alta performance (HPC). Ao oferecer a possibilidade de menos interrupções, a estratégia `capacity0ptimized` pode reduzir o custo geral da workload.

Como alternativa, você pode usar a estratégia de alocação `capacity0ptimizedPrioritized` com um parâmetro de prioridade para ordenar os tipos de instância, da prioridade mais alta para a mais baixa. Você pode definir a mesma prioridade para diferentes tipos de instância. A frota spot otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades de tipo de instância (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da frota spot de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante. Só haverá suporte para o uso de prioridades se a frota usar um modelo de lançamento. Observe que quando você define a prioridade para `capacity0ptimizedPrioritized`, a mesma prioridade também será aplicada às instâncias sob demanda se o `AllocationStrategy` sob demanda estiver definido como `prioritized`.

`diversified`

As Instâncias spot são distribuídas por todos os grupos.

Escolher uma estratégia de alocação apropriada

Você pode otimizar a frota para seu caso de uso escolhendo a estratégia apropriada de alocação spot. Para a capacidade visada da instância sob demanda, a frota spot sempre seleciona o tipo de instância de menor preço com base no preço público sob demanda e continua a seguir a estratégia de alocação, `priceCapacityOptimized`, `capacityOptimized` ou `diversified`, para instâncias spot.

Equilibrar menor preço e disponibilidade de capacidade

Para obter o equilíbrio entre os grupos de capacidade spot com menor preço e os grupos de capacidade spot com a maior disponibilidade de capacidade, recomendamos que você use a estratégia de alocação `priceCapacityOptimized`. Essa estratégia toma decisões sobre quais grupos devem solicitar instâncias spot com base no preço dos grupos e na disponibilidade de capacidade de instâncias spot nesses grupos. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção em curto prazo, ao mesmo tempo que ainda levaremos o preço em consideração.

Se a frota executar workloads resilientes e sem estado, incluindo aplicações conteinerizadas, microsserviços, aplicações da Web, trabalhos de dados e análises, e processamento em lote, use a estratégia de alocação `priceCapacityOptimized` para otimizar a economia de custos e a disponibilidade de capacidade.

Se a frota executar workloads que possam ter um custo de interrupção maior associado ao reinício do trabalho, você deverá implementar verificações para que as aplicações possam ser reiniciadas no ponto em que foram interrompidas. Usando verificações, você torna a estratégia de alocação `priceCapacityOptimized` uma boa opção para essas workloads, pois ela aloca a capacidade dos grupos com menor preço que também oferecem uma baixa taxa de interrupção de instâncias spot.

Para ver um exemplo de configuração que usa a estratégia de alocação `priceCapacityOptimized`, consulte Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades.

Quando as workloads têm um alto custo de interrupção

Opcionalmente, você pode usar a estratégia `capacityOptimized` se executar workloads que usem tipos de instância com preços semelhantes ou em que o custo da interrupção seja tão significativo que qualquer economia de custos será inadequada em comparação com um aumento marginal nas interrupções. Essa estratégia aloca capacidade dos grupos com capacidade spot mais disponível

que oferecem a possibilidade de menos interrupções, o que pode reduzir o custo geral da workload. Para ver um exemplo de configuração que usa a estratégia de alocação `capacityOptimized`, consulte Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição.

Quando a possibilidade de interrupções precisa ser minimizada, mas a preferência por determinados tipos de instância é importante, é possível expressar as prioridades do seu grupo usando a estratégia de alocação `capacityOptimizedPrioritized` e definindo a ordem dos tipos de instância a serem usados por prioridade, da mais alta para a mais baixa. Para obter uma configuração de exemplo, consulte Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade.

Observe que só é possível usar prioridades se a frota usar um modelo de inicialização. Observe que, quando você define as prioridades para `capacityOptimizedPrioritized`, as mesmas prioridades também serão aplicadas às instâncias sob demanda se a `AllocationStrategy` sob demanda estiver definida como `prioritized`.

Quando a workload é flexível em termos de tempo e a disponibilidade de capacidade não é um fator

Se a frota for pequena ou for executada por um período curto, você poderá usar `priceCapacityOptimized` para maximizar a economia de custos, ainda levando em conta a disponibilidade de capacidade.

Quando sua frota é grande ou é executada por muito tempo

Se sua frota for grande ou estiver sendo executada há muito tempo, você poderá aprimorar a disponibilidade dela distribuindo as Instâncias spot por vários grupos, usando a estratégia `diversified`. Por exemplo, se a frota spot especificar 10 grupos e uma capacidade visada de 100 instâncias, a frota iniciará 10 Instâncias spot em cada grupo. Se o preço spot para um grupo exceder seu preço máximo para esse mesmo grupo, somente 10% de sua frota será afetada. Usar essa estratégia também torna sua frota menos sensível a aumentos que ocorram com o tempo no preço spot em qualquer grupo específico. Com a estratégia `diversified`, a frota spot não executará instâncias spot em nenhum grupo com um preço spot igual ou maior que o preço sob demanda.

Manter a capacidade de destino

Depois que as Instâncias spot são encerradas devido a uma alteração no preço spot ou na capacidade disponível de um grupo de capacidade spot, uma frota spot do tipo `maintain` executa as instâncias spot de substituição. A estratégia de alocação determina os grupos dos quais as instâncias de substituição são iniciadas, da seguinte forma:

- Se a estratégia de alocação for `priceCapacityOptimized`, a frota iniciará as instâncias de substituição nos grupos com maior disponibilidade de capacidade de instâncias spot, ao mesmo tempo que também levará em consideração o preço e identificará os grupos com menor preço com alta disponibilidade de capacidade.
- Se a estratégia de alocação for `capacityOptimized`, a frota iniciará as instâncias de substituição no grupo com a maior capacidade de instâncias spot disponível.
- Se a estratégia de alocação for `diversified`, a frota distribuirá a instância spot substituta entre os grupos restantes.

Seleção de tipo de instância baseada em atributos para frota spot

Ao criar uma frota spot, você deve especificar um ou mais tipos de instância para configurar as instâncias sob-demanda e as instâncias spot na frota. Como alternativa à especificação manual dos tipos de instância, você pode especificar os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos. Isso é conhecido como seleção de tipo de instância baseada em atributos. Por exemplo, você pode especificar o número mínimo e máximo de vCPUs necessárias para suas instâncias, e a frota spot iniciará as instâncias usando todos os tipos de instância disponíveis que atendam a esses requisitos de vCPU.

A seleção de tipo de instância baseada em atributos é ideal para workloads e frameworks que possam ser flexíveis em relação a que tipos de instância elas usam, como ao executar contêineres ou frotas da Web, processar big data e implementar ferramentas de integração e implantação contínuas (CI/CD).

Benefícios

A seleção de tipo de instância baseada em atributos oferece os seguintes benefícios:

- Use facilmente os tipos de instâncias certos: com tantos tipos de instância disponíveis, encontrar os tipos de instância corretos para a workload pode ser demorado. Se você especificar os atributos de instância, os tipos de instância terão automaticamente os atributos necessários para sua workload.
- Configuração simplificada: para especificar manualmente vários tipos de instância para uma frota spot, crie uma substituição de modelo de lançamento separada para cada tipo de instância. Mas, com a seleção de tipo de instância baseada em atributos, para fornecer vários tipos de instância, você só precisa especificar os atributos das instâncias no modelo de lançamento ou em uma substituição de modelo de lançamento.

- Uso automático de novos tipos de instâncias: quando atributos de instância são especificados em vez de tipos de instância, sua frota pode usar tipos de instância de gerações mais novas à medida que são lançados, tornando a configuração da frota "à prova de obsolescência".
- Flexibilidade dos tipos de instâncias: quando atributos de instância são especificados em vez de tipos de instância, a frota spot pode selecionar entre uma ampla variedade de tipos de instância para iniciar instâncias spot, o que atende à Prática recomendada para instâncias spot: flexibilidade de tipo de instância.

Tópicos

- Como funciona a seleção de tipo de instância baseada em atributos
- Proteção de preço
- Considerações
- Criar uma frota spot com seleção de tipo de instância baseada em atributos
- Exemplos de configurações que são válidas e não válidas
- Previsualizar os tipos de instância com os atributos especificados

Como funciona a seleção de tipo de instância baseada em atributos

Para usar a seleção de tipo de instância baseada em atributos na configuração de frota, substitua a lista dos tipos de instância por uma lista dos atributos de instância que suas instâncias requerem. A frota spot iniciará as instâncias em todos os tipos de instância disponíveis que tenham os atributos de instância especificados.

Tópicos

- Tipos de atributos de instância
- Onde configurar a seleção de tipo de instância baseada em atributos
- Como a frota spot usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

Tipos de atributos de instância

Há vários atributos de instância que você pode especificar para expressar seus requisitos de computação, p. ex.:

- Contagem de vCPUs: o número mínimo e máximo de vCPUs por instância.

- Memória: o mínimo e o máximo de GiBs de memória por instância.
- Armazenamento local: se o sistema deve usar o EBS ou volumes de armazenamento de instâncias para armazenamento local.
- Desempenho intermitente: se o sistema deve usar a família de instâncias T, incluindo os tipos T4g, T3a, T3 e T2.

Para obter uma descrição de cada atributo e os valores padrão, consulte InstanceRequirements na Referência de API do Amazon EC2.

Onde configurar a seleção de tipo de instância baseada em atributos

Dependendo de você usar o console ou a AWS CLI, é possível especificar os atributos de instância para a seleção de tipo de instância baseada em atributos da seguinte forma:

No console, você pode especificar os atributos de instância em um ou em ambos os componentes de configuração de frota a seguir:

- Em um modelo de inicialização, referencie o modelo de inicialização na solicitação da frota
- Na solicitação da frota

Na AWS CLI, você pode especificar os atributos de instância em um ou ambos os componentes de configuração de frota a seguir:

- Em um modelo de lançamento, e referencie o modelo de lançamento na solicitação da frota
- Em uma substituição de modelo de lançamento

  Se desejar uma combinação de instâncias que usam AMIs diferentes, você pode especificar atributos de instância em várias substituições de modelo de lançamento. Por exemplo, diferentes tipos de instância podem usar processadores baseados em x86 e Arm.
- Em uma especificação de lançamento

Como a frota spot usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

A frota spot provisiona uma frota da seguinte maneira:

- A frota spot identifica os tipos de instância que têm os atributos especificados.
- A frota spot usa proteção de preço para determinar quais tipos de instância excluir.

- A frota spot determina os grupos de capacidade que serão considerados ao definir de quais grupos as instâncias serão iniciadas, com base nas regiões ou zonas de disponibilidade da AWS que têm os tipos de instância correspondentes.
- A frota spot aplica a estratégia de alocação especificada para determinar os grupos de capacidade dos quais as instâncias serão iniciadas.

  Observe que a seleção de tipo de instância baseada em atributos não escolhe os grupos de capacidade dos quais provisionar a frota; isso cabe às estratégias de alocação. Pode haver um grande número de tipos de instância com os atributos especificados, e alguns deles podem ser caros.

  Se você especificar uma estratégia de alocação, a frota spot iniciará as instâncias de acordo com a estratégia de alocação especificada.
  - Para instâncias spot, a seleção de tipo de instância baseada em atributos oferece suporte às estratégias de alocação de `capacityOptimizedPrioritized` e `capacityOptimized`.
  - Para instâncias sob demanda, a seleção de tipo de instância baseada em atributos oferece suporte à estratégia de alocação `lowestPrice`, que garante que a frota spot iniciará as instâncias sob demanda dos grupos de capacidade menos dispendiosos.
- Se não houver capacidade para os tipos de instância com os atributos de instância especificados, nenhuma instância poderá ser iniciada e a frota retornará um erro.

Proteção de preço

A proteção de preços é um recurso que impede que sua frota spot use tipos de instância que você consideraria muito caros, mesmo que atendam aos atributos especificados. Para usar a proteção de preço, você define um limite de preço. Em seguida, quando o Amazon EC2 selecionar tipos de instância com seus atributos, ele excluirá os tipos de instância que tenham preços acima do limite.

A forma como o Amazon EC2 calcula o limite de preço é a seguinte:

- Primeiro, o Amazon EC2 identifica o tipo de instância com o menor preço dentre aqueles que correspondem aos seus atributos.
- Em seguida, o Amazon EC2 pegará o valor (expresso como uma porcentagem) que você especificou para o parâmetro de proteção de preço e o multiplicará pelo preço do tipo de instância identificado. O resultado é o preço usado como o limite de preço.

Há limites distintos de preço para instâncias sob demanda e instâncias spot.

Quando você cria uma frota com seleção de tipo de instância baseada em atributos, a proteção de preço é habilitada por padrão. É possível manter os valores padrão ou especificar seus próprios valores.

Você também pode desativar a proteção de preços. Para indicar que não há limite de proteção de preço, especifique um valor percentual alto, como 999999.

Tópicos

- Identificação do tipo de instância com o menor preço
- Proteção de preço de instância sob demanda
- Proteção de preço de instância spot
- Especificar o limite de proteção de preço

Identificação do tipo de instância com o menor preço

O Amazon EC2 determina o preço básico do limite de preço ao identificar o tipo de instância com o menor preço dentre aquelas que correspondem aos atributos especificados. Ele faz isso da seguinte maneira:

- Primeiro, ele analisa os tipos de instância C, M ou R da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.
- Se não houver uma correspondência, ele analisará os tipos de instância da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.
- Se não houver correspondência, ele examinará todos os tipos de instância da geração anterior que correspondam aos seus atributos e identificará o tipo de instância com o menor preço.

Proteção de preço de instância sob demanda

O limite de proteção de preço para tipos de instância sob demanda é calculado como uma porcentagem maior do que o tipo de instância sob demanda de menor preço identificado (`OnDemandMaxPricePercentageOverLowestPrice`). Você especifica maior a porcentagem que está disposto a pagar. Se você não especificar esse parâmetro, um valor padrão de `20` será usado para calcular um limite de proteção de preço 20% superior ao preço identificado.

Por exemplo, se o preço da instância sob demanda identificada for `0.4271`, e você especificar `25`, o limite de preço será 25% maior que `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 1.25 = 0.533875`. O preço calculado é o máximo que você está disposto a pagar por instâncias sob demanda e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância sob demanda com preço superior a `0.533875`.

Proteção de preço de instância spot

Por padrão, o Amazon EC2 aplicará automaticamente a proteção de preço de instância spot ideal para selecionar de forma consistente entre uma ampla variedade de tipos de instância. Você também pode definir manualmente a proteção de preço. No entanto, deixar que o Amazon EC2 faça isso por você pode aumentar a probabilidade de que sua capacidade de spot seja atendida.

É possível especificar manualmente a proteção de preço usando uma das opções a seguir. Se você definir manualmente a proteção de preço, recomendamos usar a primeira opção.

- Um percentual do tipo de instância sob demanda com o menor preço identificado [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Por exemplo, se o preço do tipo de instância sob demanda identificada for `0.4271`, e você especificar `60`, o limite de preço será 60% de `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 0.60 = 0.25626`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.25626`.
- Um percentual maior do que o tipo de instância spot com o menor preço identificado [`SpotMaxPricePercentageOverLowestPrice`]

  Por exemplo, se o preço do tipo de instância spot identificada for `0.1808`, e você especificar `25`, o limite de preço será 25% maior que `0.1808`. Isso é calculado da seguinte forma: `0.1808 * 1.25 = 0.226`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.266`. Não é recomendável usar esse parâmetro, pois os preço spot podem flutuar e, portanto, seu limite de proteção de preço também poderá flutuar.

Especificar o limite de proteção de preço

Para especificar o limite de proteção de preço

Ao criar a frota spot, configure a frota para seleção de tipo de instância baseada em atributos e então faça o seguinte:

- Console

  Para especificar o limite de proteção de preço da instância sob demanda, em Additional instance attribute (Atributo de instância adicional), escolha On-demand price protection (Proteção de preços sob demanda) e Add attribute (Adicionar atributo). Em On-Demand price protection percentage (Porcentagem de proteção de preço sob demanda), insira o limite de proteção de preço como uma porcentagem.

  Para especificar o limite de proteção de preço da Instância spot, em Additional instance attribute (Atributos de instância adicional), escolha Spot price protection (Proteção de preço spot) e Add attribute (Adicionar atributo). Escolha um parâmetro e insira o limite de proteção de preço como uma porcentagem.

- AWS CLI

  Para especificar o limite de proteção de preço da instância sob demanda, no arquivo de configuração JSON, em estrutura `InstanceRequirements`, para `OnDemandMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.

  Para especificar o limite de proteção de preço da instância spot, no arquivo de configuração JSON, na estrutura `InstanceRequirements`, especifique um destes parâmetros:

  - Para `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, insira o limite de proteção de preço como uma porcentagem.
  - Para `SpotMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.

Para obter mais informações sobre a criação de uma frota, consulte Criar uma frota spot com seleção de tipo de instância baseada em atributos.

> **Note**
>
> Ao criar a frota spot, se você definir o tipo Total target capacity (Capacidade total de destino) como vCPUs ou Memory (MiB) (Memória [MiB]) (console) ou `TargetCapacityUnitType` para `vcpu` ou `memory-mib` (AWS CLI), o limite de proteção de preço é aplicado com base no preço por VCPU ou por memória, em vez do preço por instância.

Considerações

- Você pode especificar tipos de instância ou atributos de instância em uma frota spot, mas não os dois ao mesmo tempo.

  Ao usar a CLI, as substituições do modelo de lançamento prevalecerão sobre o modelo de lançamento. Por exemplo, se o modelo de lançamento contiver um tipo de instância e a substituição do modelo de lançamento contiver atributos de instância, as instâncias identificadas pelos atributos da instância prevalecerão sobre o tipo de instância no modelo de lançamento.
- Ao usar a CLI, quando você especifica atributos de instância como substituições, não pode especificar também pesos ou prioridades.
- Você pode especificar, no máximo, quatro estruturas de `InstanceRequirements` em uma configuração de solicitação.

Criar uma frota spot com seleção de tipo de instância baseada em atributos

Você pode configurar uma frota para usar a seleção de tipo de instância baseada em atributos usando o console do Amazon EC2 ou a AWS CLI.

Tópicos

- Criar uma frota spot usando o console
- Crie uma frota spot usando a AWS CLI

Criar uma frota spot usando o console

Para configurar uma frota spot para seleção de tipo de instância baseada em atributos (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Spot Requests (Solicitações de spot) e escolha Request Spot Instances (Solicitar instâncias spot).
3. Siga as etapas para criar um frota spot. Para ter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console).

   Ao criar a frota spot, configure a frota para seleção de tipo de instância baseada em atributos da seguinte forma:

   a. Em Instance type requirements (Requisitos de tipo de instância), escolha Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação).
   b. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
   c. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
   d. (Opcional) Em Additional instance attributes (Atributos de instância adicionais), você pode, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais restrições à solicitação.
   e. (Opcional) Expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes) para visualizar os tipos de instância que têm os atributos especificados.

Crie uma frota spot usando a AWS CLI

Para configurar uma frota spot para seleção de tipo de instância baseada em atributos (AWS CLI)

Use o comando request-spot-fleet (AWS CLI) para criar uma solicitação de frota spot. Especifique a configuração da frota em um arquivo JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Exemplo de arquivo *file_name*.json

O exemplo a seguir contém os parâmetros que configuram uma frota spot para usar a seleção de tipo de instância baseada em atributos e é seguido de um texto explicativo.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Os parâmetros para a seleção de tipo de instância baseada nos atributos são especificados na estrutura `InstanceRequirements`. Neste exemplo, dois atributos são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a frota spot provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

> **Note**
>
> Quando `InstanceRequirements` for incluído na configuração da frota, `InstanceType` e `WeightedCapacity` devem ser excluídos; eles não podem determinar a configuração da frota ao mesmo tempo que os atributos da instância.

O JSON também contém a seguinte configuração de frota:

- `"AllocationStrategy": "priceCapacityOptimized"`: a estratégia de alocação para as instâncias spot na frota.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"`: o modelo de inicialização contém algumas informações de configuração da instância, mas se algum tipo de instância for especificado, ele será substituído pelos atributos especificados em `InstanceRequirements`.
- `"TargetCapacity": 20`: a capacidade visada é de 20 instâncias.
- `"Type": "request"`: o tipo de solicitação para a frota é `request`.

Exemplos de configurações que são válidas e não válidas

Se você usar a AWS CLI para criar uma frota spot, deverá se certificar de que a configuração da frota seja válida. Exemplos de configurações que são válidas e não válidas.

As configurações são consideradas não válidas quando contiverem o seguinte:

- Uma única estrutura de `Overrides` com `InstanceRequirements` e `InstanceType`
- Duas estruturas de `Overrides`, uma com `InstanceRequirements` e outra com `InstanceType`
- Duas estruturas de `InstanceRequirements` com valores de atributo sobrepostos na mesma `LaunchTemplateSpecification`

Exemplos de configuração

- Configuração válida: modelo de lançamento único com substituições
- Configuração válida: modelo de lançamento único com vários InstanceRequirements
- Configuração válida: dois modelos de lançamento com substituições em cada

- Configuração válida: somente InstanceRequirements especificados, sem valores de atributo sobrepostos
- Configuração não válida: Overrides contémInstanceRequirements e InstanceType
- Configuração não válida: duas Overrides contêm InstanceRequirements e InstanceType
- Configuração não válida: valores de atributo sobrepostos

Configuração válida: modelo de lançamento único com substituições

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. A seguir está um texto explicativo do exemplo de configuração.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
```

```
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Para usar a seleção de instância baseada em atributos, você deve incluir a estrutura de `InstanceRequirements` na configuração de frota e especificar os atributos desejados para as instâncias da frota.

No exemplo anterior, os seguintes atributos de instância foram especificados:

- `VCpuCount`: os tipos de instância devem ter no mínimo 2 e no máximo 8 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no máximo 10.240 MiB de memória. Um mínimo de 0 indica que não há limite mínimo.
- `MemoryGiBPerVCpu`: os tipos de instância devem ter no máximo 10.000 GiB de memória. O parâmetro `Min` é opcional. Ao omiti-lo, você indica que não há limite mínimo.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs. A frota spot executará instâncias suficientes para que o número total de vCPUs na frota seja de 5.000 vCPUs.

Configuração válida: modelo de lançamento único com vários InstanceRequirements

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo duas estruturas de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
    "SpotFleetRequestConfig": {
```

```
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração válida: dois modelos de lançamento com substituições em cada

A configuração a seguir é válida. Ela contém dois modelos de lançamento, cada um deles com uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. Essa configuração é útil para oferecer suporte às arquiteturas `arm` e `x86` na mesma frota.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração válida: somente **`InstanceRequirements`** especificados, sem valores de atributo sobrepostos

A configuração a seguir é válida. Ela contém duas estruturas de `LaunchTemplateSpecification`, cada uma com um modelo de lançamento e uma estrutura `Overrides` contendo uma estrutura de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: **`Overrides`** contém**`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. A estrutura de `Overrides` contém `InstanceRequirements` e `InstanceType`. Em `Overrides`, você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: duas **`Overrides`** contêm **`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. As estruturas `Overrides` contêm `InstanceRequirements` e `InstanceType`. Você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos, mesmo que estejam em estruturas de `Overrides` diferentes.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: valores de atributo sobrepostos

A configuração a seguir não é válida. As duas estruturas de `InstanceRequirements` contêm `"VCpuCount": {"Min": 0, "Max": 2}`. Os valores desses atributos se sobrepõem, o que resultará em grupos de capacidade duplicados.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
```

```
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Previsualizar os tipos de instância com os atributos especificados

Você pode usar o comando get-instance-types-de-instance-requirements da AWS CLI para previsualizar os tipos de instância que correspondem aos atributos especificados por você. Isso é especialmente útil para determinar quais atributos especificar na configuração da solicitação sem iniciar nenhuma instância. Observe que o comando não considera a capacidade disponível.

Para previsualizar uma lista de tipos de instância especificando atributos usando a AWS CLI

1. (Opcional) Para gerar todos os atributos possíveis que podem ser especificados, use o comando get-instance-types-de-instance-requirements e o parâmetro `--generate-cli-skeleton`. Opcionalmente, você pode direcionar a saída para um arquivo e salvá-lo usando `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Saída esperada

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
               "Min": 0,
               "Max": 0
           },
           "MemoryMiB": {
   ```

```
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
```

```
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Crie um arquivo de configuração JSON usando a saída da etapa anterior e configure-o da seguinte forma:

> **Note**
>
> Você deve fornecer valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Você pode omitir os outros atributos; quando omitidos, os valores padrão são usados.
> Para obter uma descrição de cada atributo e seus valores padrão, consulte get-instance-types-de-instance-requirements na Referência da linha de comando do Amazon EC2.

a. Em `ArchitectureTypes`, especifique um ou mais tipos de arquitetura de processador.

b. Em `VirtualizationTypes`, especifique um ou mais tipos de virtualização.

c. Em `VCpuCount`, especifique o número mínimo e máximo de vCPUs. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

d. Em `MemoryMiB`, especifique a quantidade mínima e máxima de memória em MiB. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

e. Opcionalmente, você pode especificar um ou mais dos outros atributos para restringir ainda mais a lista de tipos de instância retornados.

3. Para previsualizar os tipos de instância que têm os atributos que você especificou no arquivo JSON, use o comando get-instance-types-from-instance-requirements e especifique o nome e o caminho para seu arquivo JSON usando o parâmetro `--cli-input-json`. Opcionalmente, você pode formatar a saída para ser exibida em formato de tabela.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Exemplo de arquivo *attributes.json*

Neste exemplo, os atributos necessários estão incluídos no arquivo JSON. Eles são `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Além disso, o atributo opcional `InstanceGenerations` também está incluído. Observe que para `MemoryMiB`, o valor `Max` pode ser omitido para indicar que não há limite.

```
{
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
```

```
}
```

Exemplo de saída

```
----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+--------------------------------------+
||             InstanceTypes            ||
|+------------------------------------+|
||             InstanceType             ||
|+------------------------------------+|
||  c4.xlarge                         ||
||  c5.xlarge                         ||
||  c5a.xlarge                        ||
||  c5ad.xlarge                       ||
||  c5d.xlarge                        ||
||  c5n.xlarge                        ||
||  c6a.xlarge                         ||
...
```

4. Após identificar os tipos de instância que atendem às suas necessidades, anote os atributos de instância usados para que poder usá-los ao configurar a solicitação de frota.

Sob demanda na frota spot

Para garantir que você sempre tenha capacidade de instância, você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot. Na solicitação de frota spot, especifique a capacidade desejada de destino e a quantidade dessa capacidade que deve ser sob demanda. O saldo compromete a capacidade spot, que será executada se houver capacidade e disponibilidade do Amazon EC2 disponíveis. Por exemplo, se você especificar a capacidade pretendida como 10 e a capacidade sob demanda como 8 em sua solicitação de frota spot, o Amazon EC2 executará 8 unidades de capacidade como sob demanda e 2 unidades de capacidade (10 - 8 = 2) como spot.

Priorizar tipos de instâncias para capacidade sob demanda

Quando a frota spot tenta atender à sua capacidade sob demanda, o padrão é iniciar primeiro o tipo de instância de menor preço. Se `OnDemandAllocationStrategy` estiver definido como `prioritized`, a frota spot usará a prioridade para determinar qual tipo de instância será o primeiro a atender a capacidade sob demanda.

A prioridade é atribuída à substituição do modelo de ativação, e a prioridade mais alta é lançada primeiro.

Exemplo: priorizar tipos de instância

Neste exemplo, você configura três substituições de modelo de execução, cada uma com um tipo de instância diferente.

O preço sob demanda para os tipos de instância varia no preço. Os tipos de instância usados neste exemplo são apresentados a seguir, listados em ordem de preço, começando com o tipo de instância mais barato:

- `m4.large`: mais barato
- `m5.large`
- `m5a.large`

Se você não usar a prioridade para determinar a ordem, a frota atenderá à capacidade sob demanda começando pelo tipo mais barato de instância.

No entanto, digamos que você tenha instâncias reservadas `m5.large` não utilizadas que deseja usar primeiro. É possível definir a prioridade de substituição do modelo de execução para que os tipos de instância sejam usados na ordem de prioridade, da seguinte forma:

- `m5.large`: prioridade 1
- `m4.large`: prioridade 2
- `m5a.large`: prioridade 3

Rebalanceamento de capacidade

Você pode configurar a frota spot para iniciar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento para notificar que uma instância spot está em um risco elevado de interrupção. O rebalanceamento de capacidade ajuda a manter a disponibilidade da workload aumentando proativamente sua frota com uma nova instância spot antes que uma instância em execução seja interrompida por Amazon EC2. Para ter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.

Para configurar a frota spot para iniciar uma instância spot de substituição, você pode usar o console do Amazon EC2 ou a AWS CLI.

- Console do Amazon EC2: marque a caixa de seleção Capacity rebalance (Rebalancear capacidade) ao criar a frota spot. Para obter mais informações, consulte a etapa 6.d em Criar uma solicitação de frota spot usando parâmetros definidos (console).
- AWS CLI: use o comando request-spot-fleet e os parâmetros relevantes na estrutura da `SpotMaintenanceStrategies`. Para obter mais informações, consulte o exemplo de configuração de execução.

Limitações

- O rebalanceamento de capacidade só está disponível para frotas do tipo `maintain`.
- Quando a frota estiver em execução, não é possível modificar a configuração de rebalanceamento de capacidade. Para alterar a configuração de rebalanceamento de capacidade, você deve excluir a frota e criar uma nova.

Opções de configuração

A `ReplacementStrategy` para frota spot oferece suporte a estes dois valores:

`launch-before-terminate`

O Amazon EC2 termina as Instâncias spot que recebem uma notificação de rebalanceamento após o lançamento de novas Instâncias spot de substituição. Se você especificar `launch-before-terminate`, também deverá especificar um valor para `termination-delay`. Depois que as novas instâncias de substituição são iniciadas, o Amazon EC2 aguarda o período de `termination-delay` e, em seguida, encerra as instâncias antigas. Em `termination-delay`, o mínimo é de 120 segundos (2 minutos) e o máximo é de 7.200 segundos (2 horas).

Recomendamos o uso de `launch-before-terminate` apenas se você puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento. Observe que o Amazon EC2 pode interromper as instâncias antigas com um aviso dois minutos antes do período de `termination-delay`.

`launch`

O Amazon EC2 inicia instâncias spot de substituição quando uma notificação de rebalanceamento é emitida para as instâncias spot existentes. O Amazon EC2 não termina automaticamente as instâncias que recebem uma notificação de rebalanceamento. Você pode

terminar as instâncias antigas ou deixá-las em execução. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

Considerações

Se você configurar uma frota spot para rebalanceamento de capacidade, considere o seguinte:

Forneça o maior número possível de grupos de capacidade spot na solicitação

Configure sua frota spot para usar vários tipos de instância e zonas de disponibilidade. Isso oferece a flexibilidade para executar instâncias spot em vários grupos de capacidade spot. Para ter mais informações, consulte Ser flexível sobre tipos de instância e zonas de disponibilidade.

Evitar um risco elevado de interrupção das instâncias spot substitutas

Para evitar um alto risco de interrupção, recomendamos fortemente a estratégia de alocação `capacityOptimized` ou `capacityOptimizedPrioritized`. Essas estratégias garantem que as instâncias spot substitutas sejam iniciadas nos grupos de capacidade spot ideais e, portanto, tenham menos probabilidade de serem interrompidas em futuro próximo. Para ter mais informações, consulte Usar a estratégia de alocação otimizada para preço e capacidade.

O Amazon EC2 Auto Scaling só iniciará uma nova instância se a disponibilidade for igual ou superior

Um dos objetivos do rebalanceamento de capacidade é melhorar a disponibilidade de uma instância spot. Se uma instância spot existente receber uma recomendação de rebalanceamento, o Amazon EC2 só iniciará uma nova instância caso a nova instância forneça uma disponibilidade igual ou superior a da instância existente. Se o risco de interrupção de uma nova instância for pior do que a instância existente, o Amazon EC2 não iniciará uma nova instância. No entanto, o Amazon EC2 continuará a avaliar os grupos de capacidade spot e iniciará uma nova instância se a disponibilidade melhorar.

Há uma chance de que a instância existente seja interrompida sem que o Amazon EC2 inicie proativamente uma nova instância. Quando isso acontecer, o Amazon EC2 tentará iniciar uma nova instância, independentemente de a nova instância ter um alto risco de interrupção.

O Rebalanceamento da capacidade não aumenta a taxa de interrupção de instâncias Spot

Quando o Rebalanceamento da capacidade é habilitado, ele não aumenta a Taxa de interrupção de instâncias Spot (o número de instâncias Spot que são recuperadas quando o Amazon EC2 precisa novamente de capacidade). Porém, se o rebalanceamento da capacidade detectar que uma instância está em risco de interrupção, o Amazon EC2 tentará iniciar imediatamente uma nova instância. O resultado é que pode haver a substituição de mais instâncias do que se você

esperasse que o Amazon EC2 iniciasse uma nova instância depois que a instância em risco fosse interrompida.

Mesmo podendo substituir mais instâncias com o Rebalanceamento da capacidade habilitado, você se beneficia de ser proativo em vez de reativo, tendo mais tempo para agir antes que suas instâncias sejam interrompidas. Com um Aviso de interrupção de instâncias Spot, normalmente você só tem até dois minutos para encerrar sua instância sem problemas. Com o Rebalanceamento da capacidade iniciando uma nova instância com antecedência, os processos existentes têm maiores chances de serem concluídos na instância em risco. Além disso, você pode iniciar os procedimentos de desligamento da instância e impedir que novos trabalhos sejam agendados na instância em risco. Você também pode começar a preparar a instância recém-lançada para assumir o controle da aplicação. Com a substituição proativa do Rebalanceamento da capacidade, você se beneficia com uma continuidade tranquila.

Como exemplo teórico para demonstrar os riscos e benefícios do uso do Rebalanceamento da capacidade, considere o seguinte cenário:

- 14h: uma recomendação de rebalanceamento é recebida para a instância A, e o Amazon EC2 começa imediatamente a tentar iniciar uma instância B de substituição, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h30: uma recomendação de rebalanceamento é recebida para a instância-B, substituída pela instância-C, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h32: se o Rebalanceamento da capacidade não estivesse habilitado e um aviso de interrupção de instância Spot tivesse sido recebido às 14h32 para a instância-A, você teria apenas dois minutos para agir, mas a Instância-A estaria em execução até esse momento.

* Se `launch-before-terminate` for especificado, o Amazon EC2 encerrará a instância em risco depois que a instância de substituição ficar online.

O Amazon EC2 pode iniciar a nova Instâncias spot de substituição até que a capacidade atingida seja o dobro da capacidade visada

Quando uma frota spot é configurada para rebalanceamento de capacidade, o Amazon EC2 tenta iniciar uma nova instância spot de substituição para cada instância spot que recebe uma recomendação de rebalanceamento. Depois que uma instância spot recebe uma recomendação de rebalanceamento, ela deixa de ser contada como parte da capacidade atendida. Dependendo da estratégia de substituição, o Amazon EC2 termina a instância após um período espera para término pré-configurado ou a deixa em execução. Isso dá a você a oportunidade de executar ações de rebalanceamento na instância.

Se sua frota atingir o dobro da capacidade de destino, ela interrompe a execução de novas instâncias de substituição, mesmo que as próprias instâncias de substituição recebam uma recomendação de rebalanceamento.

Por exemplo, você cria uma frota spot com uma capacidade de destino de 100 instâncias spot. Todas as instâncias spot recebem uma recomendação de rebalanceamento, o que faz com que o Amazon EC2 inicie 100 instâncias spot de substituição. Isso eleva o número de instâncias spot atendidas para 200, o que é o dobro da capacidade de destino. Algumas das instâncias de substituição recebem uma recomendação de rebalanceamento, porém nenhuma instância de substituição é executada porque a frota não pode exceder o dobro da capacidade de destino.

Observe que você é cobrado por todas as instâncias durante a execução.

Recomendamos que você configure a frota spot para terminar as instâncias spot que receberem uma recomendação de rebalanceamento

Se você configurar a frota spot para rebalanceamento de capacidade, recomendamos que só escolha `launch-before-terminate` com um período de espera de término apropriado se puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento.

Se escolher terminar as instâncias recomendadas para rebalanceamento você mesmo, recomendamos que monitore o aviso da recomendação de rebalanceamento recebido pelas instâncias spot na frota. Ao monitorar o sinal, você pode executar rapidamente ações de rebalanceamento nas instâncias afetadas, antes que o Amazon EC2 as interrompa e, em seguida, você pode encerrá-las manualmente. Se você não encerrar as instâncias, continuará pagando por elas enquanto estiverem em execução. O Amazon EC2 não encerra automaticamente as instâncias que recebem uma recomendação de rebalanceamento.

Você pode configurar notificações usando o Amazon EventBridge ou metadados da instância. Para ter mais informações, consulte Monitorar os sinais de recomendação de rebalanceamento.

A frota spot não conta as instâncias que recebem uma recomendação de rebalanceamento ao calcular a capacidade atendida durante o aumento ou a redução da capacidade

Se a frota spot estiver configurada para rebalanceamento de capacidade e você alterar a capacidade de destino para aumento ou diminuição, a frota não contará as instâncias marcadas para rebalanceamento como parte da capacidade atendida, como a seguir:

- Reduzir a escala horizontalmente - Se você diminuir a capacidade visada, o Amazon EC2 encerrará instâncias que não estiverem marcadas para rebalanceamento até que a capacidade

desejada seja atingida. As instâncias marcadas para rebalanceamento não são contabilizadas para a capacidade atingida.

Por exemplo, você cria uma frota spot com uma capacidade visada de 100 instâncias spot, e 10 instâncias recebem uma recomendação de rebalanceamento, portanto, o Amazon EC2 inicia 10 novas instâncias de substituição, resultando em uma capacidade atingida de 110 instâncias. Em seguida, você reduz a capacidade visada para 50 (reduzir a escala horizontalmente), mas a capacidade de atendimento é, na verdade, 60 instâncias porque as 10 instâncias marcadas para rebalanceamento não são encerradas pelo Amazon EC2. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

- Aumentar a escala horizontalmente - Se você aumentar a capacidade visada, o Amazon EC2 iniciará novas instâncias até que a capacidade desejada seja atingida. As instâncias marcadas para rebalanceamento não são contabilizadas para a capacidade atingida.

  Por exemplo, você cria uma frota spot com uma capacidade visada de 100 instâncias spot, e 10 instâncias recebem uma recomendação de rebalanceamento, portanto, o Amazon EC2 inicia 10 novas instâncias de substituição, resultando em uma capacidade atingida de 110 instâncias. Em seguida, você aumenta a capacidade de destino para 200 (aumento), mas a capacidade de atendimento é, na verdade, 210 instâncias porque as 10 instâncias marcadas para rebalanceamento não são contabilizadas pela frota como parte da capacidade de destino. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

Substituições do preço spot

Cada solicitação de frota spot pode incluir um preço máximo global ou usar o padrão (preço sob demanda). A frota spot usa esse preço como o preço máximo padrão em cada uma das suas especificações de execução.

É possível especificar um preço máximo em uma ou mais especificações de execução. Esse preço é específico da especificação de execução. Se uma especificação de execução incluir um preço específico, a frota spot usará esse preço máximo para substituir o preço máximo global. Qualquer outra especificação de execução que não inclua um preço máximo específico ainda usará o preço máximo global.

Controle de gastos

A frota spot para de executar instâncias quando atinge a capacidade de destino ou o valor máximo que você está disposto a pagar. Para controlar a quantidade paga por hora da sua frota, especifique

o `SpotMaxTotalPrice` para o Instâncias spot e o `OnDemandMaxTotalPrice` para Instâncias on-demand. Quando o preço total máximo for alcançado, a frota spot para de iniciar instâncias mesmo que não tenha atingido a capacidade alvo.

Os exemplos a seguir mostram duas situações diferentes. Na primeira, a frota spot para de executar instâncias ao atingir a capacidade de destino. Na segunda, a frota spot para de executar instâncias ao atingir o valor máximo que você está disposto a pagar.

Exemplo: parar de executar instâncias quando a capacidade de destino for atingida

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 1,50 USD

A frota spot executa 10 instâncias sob demanda, porque o total de 1,00 USD (10 instâncias x 0,10 USD) não excede o `OnDemandMaxTotalPrice` de 1,50 USD.

Exemplo: parar de executar instâncias quando o preço máximo total for atingido

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 0,80 USD

Se a frota spot executar a capacidade planejada (10 Instâncias on-demand), o custo total por hora será de 1,00 USD. Isso é mais que a quantidade (0,80 USD) especificada para `OnDemandMaxTotalPrice`. Para evitar gastar mais do que você pretende, a frota spot abre somente oito instâncias sob demanda (abaixo da meta de capacidade sob demanda), porque abrir mais excederia o `OnDemandMaxTotalPrice`.

Peso de instâncias de frotas spot

Ao solicitar uma frota de Instâncias spot, você poderá definir as unidades de capacidade com que cada tipo de instância contribuirá para a performance da aplicação e poderá ajustar corretamente o preço máximo para cada grupo de capacidade spot usando o peso da instância.

Por padrão, o preço que você especifica é por hora de instância. Ao usar o recurso de peso da instância, o preço que você especifica é por hora. Você pode calcular o preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A frota spot calcula o número de instâncias spot a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota spot o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino. A frota spot pode selecionar qualquer grupo que você determinar na especificação de execução, mesmo que a capacidade das instâncias executadas ultrapasse a capacidade de destino solicitada.

As tabelas a seguir fornecem exemplos de cálculos para determinar o preço por unidade para uma solicitação de frota spot com capacidade de destino igual a 10.

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
`r3.xlarge`	2	0,05 USD	0,025 (0,05 dividido por 2)	5 (10 dividido por 2)

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
`r3.8xlarge`	8	0,10 USD	0,0125 (0,10 dividido por 8)	2 (10 dividido por 8, resultado arredondado para cima)

Use o peso de instância de frotas spot da maneira a seguir para provisionar a capacidade planejada nos grupos com o menor preço por unidade no momento do atendimento:

1. Defina a capacidade planejada da frota spot em instâncias (o padrão) ou nas unidades de sua preferência, como CPUs virtuais, memória, armazenamento ou throughput.

2. Defina o preço por unidade.
3. Para cada configuração de execução, especifique o peso, que é o número de unidades que o tipo de instância representa em relação à capacidade de destino.

Exemplo de peso da instância

Considere uma solicitação de frota spot com a seguinte configuração:

- Uma capacidade de destino de 24
- Uma especificação de execução com um tipo de instância `r3.2xlarge` e um peso de 6
- Uma especificação de execução com um tipo de instância `c3.xlarge` e um peso de 5

Os pesos representam o número de unidades que o tipo de instância representa em relação à capacidade de destino. Se a primeira especificação de execução fornecer o menor preço por unidade (preço de `r3.2xlarge` por hora de instância dividido por 6), a frota spot executará quatro dessas instâncias (24 dividido por 6).

Se a segunda especificação de execução fornecer o menor preço por unidade (preço de `c3.xlarge` por hora de instância dividido por 5), a frota spot executará cinco dessas instâncias (24 dividido por 5, resultado arredondado para cima).

Peso da instância e estratégia de alocação

Considere uma solicitação de frota spot com a seguinte configuração:

- Uma capacidade de destino de 30
- Uma especificação de execução com um tipo de instância `c3.2xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `m3.xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `r3.xlarge` e um peso de 8

A frota spot executará quatro instâncias (30 dividido por 8, resultado arredondado para cima). Com a estratégia `diversified`, a frota spot executa uma instância em cada um dos três grupos, e a quarta instância em qualquer grupo que forneça o menor preço por unidade.

Trabalhar com frotas spot

Para começar a usar uma frota spot, crie uma solicitação de frota spot que inclua a capacidade pretendida, uma parte opcional sob demanda, uma ou mais especificações de lançamento para as instâncias e o preço máximo que você está disposto a pagar. O solicitação de frota deve incluir um modelo de lançamento que defina as informações de que a frota precisa para iniciar uma instância, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade e um ou mais grupos de segurança.

Se a frota incluir a Instâncias spot, o Amazon EC2 poderá tentar manter a capacidade de destino da frota à medida que os preços spot são alterados.

Não é possível modificar a capacidade de destino de uma solicitação única depois que ela for enviada. Para alterar a capacidade de destino, cancele a solicitação e envie uma nova.

Uma solicitação de frota spot permanecerá ativa até que expire ou você a cancele. Ao cancelar uma solicitação de frota spot, você pode especificar se esse cancelamento da solicitação encerra as instâncias spot nessa frota spot.

Conteúdo

- Estados das solicitações de frota spot
- Verificações de integridade da frota spot
- Permissões de frota spot
- Criar uma solicitação de frota spot
- Marcar uma frota spot
- Descrever a frota spot
- Modificar uma solicitação de frota spot
- Cancelar uma solicitação de frota spot

Estados das solicitações de frota spot

Uma solicitação de frota spot pode estar em um dos seguintes estados:

- `submitted` – A solicitação da frota spot está sendo avaliada, e o Amazon EC2 está se preparando para executar o número pretendido de instâncias. Se uma solicitação for exceder os limites da frota spot, ela será cancelada imediatamente.

- `active` – A frota spot foi validada e o Amazon EC2 está tentando manter a meta do número de instâncias spot em execução. A solicitação permanece nesse estado até que seja alterada ou cancelada.
- `modifying` – A solicitação da frota spot está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou até que a frota spot seja cancelada. Uma `request` única não pode ser alterada, e esse estado não se aplica a essas solicitações spot.
- `cancelled_running` – A frota spot é cancelada e não executa instâncias spot adicionais. Suas Instâncias spot existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.
- `cancelled_terminating` – A frota spot é cancelada e suas instâncias spot estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.
- `cancelled` – A frota spot é cancelada e não tem instâncias spot em execução. A solicitação de frota spot foi excluída dois dias depois que as instâncias foram encerradas.

Verificações de integridade da frota spot

A frota spot verifica o status de integridade das instâncias spot na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A frota spot determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. É determinado que uma instância está `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema é `impaired` em três verificações de integridade consecutivas. Para ter mais informações, consulte Verificações de status para as instâncias.

Você pode configurar a sua frota para substituir Instâncias spot não íntegras. Depois de habilitar a substituição da verificação de integridade, uma instância spot é substituída ao ser relatada como `unhealthy`. A frota pode ficar abaixo de sua capacidade de destino por até alguns minutos enquanto uma instância spot não íntegra está sendo substituída.

Requisitos

- A substituição da verificação de integridade é compatível apenas para Frotas spot que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para Frotas spot únicas (frotas do tipo `request`).

- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- Você pode configurar a frota spot para substituir instâncias não íntegras somente durante sua criação.
- Os usuários só poderão usar a substituição de verificação de integridade se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Console

Para configurar uma frota spot para substituir instâncias spot não íntegras usando o console

1. Siga as etapas para criar um frota spot. Para ter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console).
2. Para configurar a frota para substituir Instâncias spot não íntegras para a Health check (Verificação de integridade) , selecione Replace unhealthy instances (Substituir instâncias não íntegras). Para habilitar essa opção, primeiramente você deve selecionar Maintain target capacity (Manter capacidade de destino).

AWS CLI

Para configurar uma frota spot para substituir instâncias spot não íntegras usando a AWS CLI

1. Siga as etapas para criar um frota spot. Para ter mais informações, consulte Crie uma frota spot usando a AWS CLI.
2. Para configurar a frota para substituir Instâncias spot não íntegras, para `ReplaceUnhealthyInstances`, insira `true`.

Permissões de frota spot

Se os usuários pretenderem criar ou gerenciar uma frota spot, será necessário conceder a eles as permissões necessárias.

Se você usar o console do Amazon EC2 para criar uma frota spot, ele criará duas funções vinculada ao serviço chamadas `AWSServiceRoleForEC2SpotFleet` e `AWSServiceRoleForEC2Spot`, além de uma função chamada `aws-ec2-spot-fleet-tagging-role` que concede à frota spot as permissões para solicitar, executar, encerrar e marcar recursos em seu nome. Se você usar a AWS CLI ou uma API, é necessário garantir que essas funções existam.

Use as instruções a seguir para conceder as permissões necessárias e criar as funções.

Permissões e funções

- Conceder aos usuários permissão para uma frota spot
- Função vinculada ao serviço para frota spot
- Função vinculada ao serviço para instâncias spot
- Função do IAM para marcar uma frota spot

Conceder aos usuários permissão para uma frota spot

Se os usuários pretenderem criar ou gerenciar uma frota spot, certifique-se de conceder a eles as permissões necessárias.

Para criar uma frota spot

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies, Create policy.
3. Na página Criar política, selecione JSON, e substitua o texto pelo indicado a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

A política de exemplo anterior concede a um usuário as permissões necessárias para a maioria dos casos de uso de frota spot. Para limitar o usuário a ações de API específicas, especifique somente essas ações de API.

APIs do EC2 e do IAM necessárias

As seguintes APIs devem ser incluídas na política:

- `ec2:RunInstances` – Necessária para executar instâncias em uma frota spot
- `ec2:CreateTags` – Necessária para marcar as solicitações, instâncias ou volumes da frota spot
- `iam:PassRole` – Necessária para especificar a função da frota spot
- `iam:CreateServiceLinkedRole` – Necessária para criar a função vinculada ao serviço
- `iam:ListRoles` – Necessária para enumerar funções do IAM existentes
- `iam:ListInstanceProfiles` – Necessária para enumerar perfis da instância existente

Important

Se você especificar um perfil para o perfil de instância do IAM na especificação ou no modelo de inicialização, deverá conceder ao usuário a permissão de passar o perfil para o serviço. Para fazer isso, na política do IAM inclua "`arn:aws:iam::*:role/`*`IamInstanceProfile-role`*" como um recurso para a ação `iam:PassRole`. Para obter mais informações, consulte Conceder permissões ao usuário para passar uma função a um produto da AWS no Guia do usuário do IAM.

APIs de frota spot

Adicione as seguintes ações da API de frota spot à política, conforme necessário:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

APIs opcionais do IAM

(Opcional) Para permitir que um usuário crie perfis ou perfis de instância usando o console do IAM, é necessário adicionar as seguintes ações à política:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Escolha Revisar política.
5. Na página Review policy (Revisar política), digite um nome e uma descrição para a política e escolha Create policy (Criar política).
6. Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

   - Usuários e grupos no AWS IAM Identity Center:

     Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

   - Usuários gerenciados no IAM com provedor de identidades:

Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Função vinculada ao serviço para frota spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões necessárias para chamar outros produtos da AWS em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculado diretamente a um serviço da AWS. As funções vinculadas a serviços oferecem uma maneira segura de delegar permissões a serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulte Usar perfis vinculados ao serviço no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço chamada AWSServiceRoleForEC2SpotFleet para executar e gerenciar instâncias em seu nome.

> **Important**
>
> Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado na frota spot, será necessário conceder ao perfil AWSServiceRoleForEC2SpotFleet permissão para usar a CMK para que o Amazon EC2 possa executar instâncias em seu nome. Para ter mais informações, consulte Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS.

Permissões concedidas por AWSServiceRoleForEC2SpotFleet

O Amazon EC2 usa AWSServiceRoleForEC2SpotFleet para concluir as ações a seguir:

- `ec2:RequestSpotInstances` - Solicitar Instâncias spot
- `ec2:RunInstances` - executar instâncias
- `ec2:TerminateInstances` - encerrar instâncias

- `ec2:DescribeImages` - descrever imagens de máquina da Amazon (AMIs) para as instâncias
- `ec2:DescribeInstanceStatus` - descrever o status das instâncias
- `ec2:DescribeSubnets` – descrever as sub-redes das instâncias
- `ec2:CreateTags` - adiciona etiquetas à solicitação, às instâncias e aos volumes da frota spot
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - adicionar as instâncias especificadas ao load balancer especificado.
- `elasticloadbalancing:RegisterTargets` - registrar os destinos especificados no grupo de destino especificado.

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2Spotleet vinculada ao serviço na primeira vez que você criar uma frota spot usando o console.

Se você tinha uma solicitação de frota spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2SpotFleet em sua conta da AWS. Para obter mais informações, consulte Uma nova função apareceu em minha conta da AWS no Guia do usuário do IAM.

Se você usar a AWS CLI ou uma API para criar uma frota spot, verifique se essa função existe.

Para criar AWSServiceRoleForec2SpotFleet usando o console

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Roles.
3. Selecione Create role.
4. Na página Select trusted entity (Selecionar entidade confiável), faça o seguinte:
    a. Em Tipo de entidade confiável, escolha Serviços da AWS.
    b. Em Caso de uso, para Serviço ou caso de uso, escolha EC2.
    c. Em Caso de uso, Escolha EC2 - Frota spot.
    d. Escolha Próximo.
5. Na página Adicionar permissões, escolha Próximo.
6. Na página Nomear, revisar e criar, escolha Criar função.

Para criar AWSServiceRoleForec2SpotFleet usando o AWS CLI

Use o comando create-service-linked-role da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Se você não precisar mais usar a frota spot, é recomendável excluir a função AWSServiceRoleForEC2SpotFleet. Depois que a função for excluída da conta, o Amazon EC2 criará a função novamente se você solicitar uma frota spot usando o console. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado na solicitação de frota spot e usar uma chave gerenciada pelo cliente para criptografia, será necessário conceder ao perfil AWSServiceRoleForEC2SpotFleet permissão para usar a CMK para que o Amazon EC2 possa executar instâncias em seu nome. Para isso, adicione uma concessão à CMK, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Uso de concessões e Uso de políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder à função AWSServiceRoleForEC2SpotFleet permissões para usar a CMK

- Use o comando create-grant para adicionar uma concessão à CMK e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2SpotFleet) que recebe permissão para executar as operações permitidas pela concessão. A CMK é especificada pelo parâmetro `key-id` e pelo ARN da CMK. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço AWSServiceRoleForEC2SpotFleet.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/
  AWSServiceRoleForEC2SpotFleet \
  ```

```
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
"GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
"ReEncryptTo"
```

Função vinculada ao serviço para instâncias spot

O Amazon EC2 usa a função vinculada ao serviço denominada AWSServiceRoleForEC2Spot para executar e gerenciar Instâncias spot em seu nome. Para ter mais informações, consulte Função vinculada ao serviço para solicitações de instâncias spot.

Função do IAM para marcar uma frota spot

A função do IAM `aws-ec2-spot-fleet-tagging-role` concede à frota spot permissão para marcar a solicitação, as instâncias e os volumes de frota spot. Para ter mais informações, consulte Marcar uma frota spot.

> **Important**
>
> Se você optar por marcar as instâncias na frota e também por manter a capacidade visada (a solicitação de frota spot é do tipo `maintain`), as diferenças nas permissões definidas para o usuário e a `IamFleetRole` poderão levar a um comportamento inconsistente de marcação de instâncias na frota. Se o `IamFleetRole` não incluir a permissão `CreateTags`, algumas das instâncias executadas pela frota não serão marcadas. Embora estejamos trabalhando para corrigir essa inconsistência, para garantir que todas as instâncias executadas pela frota sejam marcadas, recomendamos que você use a função `aws-ec2-spot-fleet-tagging-role` para `IamFleetRole`. Outra opção é para usar uma função existente, anexe a `AmazonEC2SpotFleetTaggingRole`Política gerenciada da AWS à função existente. Caso contrário, você precisará adicionar manualmente a permissão `CreateTags` à política existente.

Para criar uma função do IAM para marcar uma frota spot

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Roles.
3. Escolha Criar Perfil.
4. Na página Select trusted entity (Selecionar entidade confiável), em Trusted entity type (Tipo de entidade confiável), escolha AWS service (Serviço da).

5. Em Caso de uso, em Casos de uso para outros serviços da AWS, escolha EC2 e escolha EC2 - marcação de frota Spot.
6. Escolha Próximo.
7. Na página Adicionar permissões, escolha Próximo.
8. Na página Name, review, and create (Nomear, revisar e criar), para Role name (Nome da função), digite um nome para a função (por exemplo, **`aws-ec2-spot-fleet-tagging-role`**).
9. Revise as informações na página e escolha Create role (Criar função).

Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema “confused deputy” é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` na política de confiança `aws-ec2-spot-fleet-tagging-role` para limitar as permissões que a frota spot concede ao recurso para outro serviço.

Para adicionar as chaves de condição AWS:SourceArn e AWS:SourceAccount à política de confiança **`aws-ec2-spot-fleet-tagging-role`**

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Encontre o `aws-ec2-spot-fleet-tagging-role` que você criou anteriormente e escolha o link (não a caixa de seleção).
4. Em Summary (Resumo), escolha a guia Trust relationships (Relacionamentos de confiança) e, em seguida, escolha Edit trust policy (Editar política de confiança).
5. Na instrução JSON, adicione um elemento `Condition` que contenha suas chaves de contexto de condição global `aws:SourceAccount` e `aws:SourceArn` para evitar o problema confused deputy, como segue:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
```

```
      }
```

> **Note**
>
> Se você utilizar ambas as chaves de contexto de condição global, e o valor `aws:SourceArn` contiver o ID da conta, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

A política de confiança final será a seguinte:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Escolha Atualizar política.

A tabela a seguir fornece valores potenciais para `aws:SourceArn` para limitar o escopo do seu `aws-ec2-spot-fleet-tagging-role` em diferentes graus de especificidade.

Operação de API	Serviço chamado	Escopo	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para solicitações de frota spot na conta especificada.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para solicitações de frota spot na conta e na região especificada. Observe que essa função não será utilizável em outras regiões.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para apenas ações que afetam a frota sfr-11111111-1111-1111-1111-111111111111. Observe que essa função pode não ser utilizável para outras frotas spot. Além disso, essa função não pode ser	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

Operação de API	Serviço chamado	Escopo	**aws:SourceArn**
		usada para lançar novas frotas spot por meio de request-spot-fleet.	

Criar uma solicitação de frota spot

Usando o AWS Management Console, crie rapidamente uma solicitação de frota spot escolhendo apenas a aplicação ou tarefa necessária e as especificações mínimas de computação. O Amazon EC2 configura uma frota que melhor atenda às suas necessidades e siga a prática recomendada de spot. Para ter mais informações, consulte Criar uma solicitação de frota spot rapidamente (console). Caso contrário, você pode modificar qualquer uma das configurações padrão. Para ter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console) e Crie uma frota spot usando a AWS CLI.

Opções para criar uma frota spot

- Criar uma solicitação de frota spot rapidamente (console)
- Criar uma solicitação de frota spot usando parâmetros definidos (console)
- Crie uma frota spot usando a AWS CLI

Criar uma solicitação de frota spot rapidamente (console)

Siga estas etapas para criar rapidamente uma solicitação de frota spot.

Para criar uma solicitação de frota spot usando as configurações recomendadas (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Se você estiver começando a usar spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, selecione Solicitar Instâncias spot.
4. Em Launch parameters (Parâmetros de lançamento), escolha Manually configure launch parameters (Configurar parâmetros de lançamento manualmente).
5. Em AMI, escolha uma AMI.

6. Em Target capacity (Capacidade), especifique o número de unidades a serem solicitadas em Total target capacity (Capacidade-alvo total). Para o tipo de unidade, você pode escolher Instances (Instâncias), vCPUs ou Memory (MiB) [Memória (MiB)].
7. Em Your fleet request at a glance (Visão rápida da solicitação de frota), revise a configuração da frota e escolha Launch (Iniciar).

Criar uma solicitação de frota spot usando parâmetros definidos (console)

Você pode criar uma frota spot usando parâmetros definidos por você.

Para criar uma solicitação de frota spot usando parâmetros definidos (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Se você estiver começando a usar spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, selecione Solicitar Instâncias spot.
4. Em Launch parameters (Parâmetros de lançamento), faça o seguinte:

   a. Para definir os parâmetros de lançamento no console de Spot, escolha Manually configure launch parameters (Configurar parâmetros de lançamento manualmente).

   b. Em AMI, escolha uma das AMIs básicas fornecidas pela AWS ou escolha Search for AMI (Pesquisar por AMI) para usar uma AMI de nossa comunidade de usuários, do AWS Marketplace ou uma que você criou.

      > **Note**
      >
      > Se uma AMI especificada nos parâmetros de execução estiver descadastrada ou desabilitada, não será possível executar nenhuma instância nova com base na AMI. Para frotas configuradas para manter a capacidade de destino, a capacidade de destino não será mantida.

   c. (Opcional) Em Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie uma novo.

      [Par de chaves existente] Escolha o par de chaves.

[Novo par de chaves] Escolha Create new key pair (Criar novo par de chaves) para ir para a página Key Pairs (Pares de chaves). Ao concluir, volte para a página Spot Requests (Solicitações de spot) e atualize a lista.

d. (Opcional) Expanda Additional launch parameters (Parâmetros de lançamento adicionais) e faça o seguinte:

   i. (Opcional) Para habilitar a otimização para o Amazon EBS, para EBS-optimized (Otimizada para EBS), escolha Launch EBS-optimized instances (Iniciar instâncias otimizadas para EBS).

   ii. (Opcional) Para adicionar armazenamento temporário em nível de blocos para suas instâncias, em Instance store (Armazenamento de instâncias), escolha Attach at launch (Anexar na execução).

   iii. (Opcional) Para adicionar armazenamento, escolha Add new volume (Adicionar novo volume) e especifique volumes adicionais do armazenamento de instâncias ou do Amazon EBS, dependendo do tipo de instância.

   iv. (Opcional) Por padrão, o monitoramento básico está habilitado para suas instâncias. Para habilitar monitoramento detalhado, para Monitoring (Monitoramento), escolha Enable CloudWatch detailed monitoring (Habilitar monitoramento detalhado do CloudWatch).

   v. (Opcional) Para executar uma instância spot dedicada, em Tenancy (Locação), selecione em Dedicated - run a dedicated instance (Dedicada: executar uma instância dedicada).

   vi. (Opcional) Em Security groups (Grupos de segurança), escolha um ou mais grupos de segurança ou crie um novo.

   [Grupo de segurança existente] Escolha um ou mais grupos de segurança.

   [Novo grupo de segurança] Escolha Create a new security group (Criar um novo grupo de segurança) para ir para a página Security Groups (Grupos de segurança). Ao concluir, volte para Spot Requests (Solicitações de spot) e atualize a lista.

   vii. (Opcional) Para tornar as instâncias acessíveis na Internet, em Auto-assign IPv4 Public IP (Atribuir automaticamente IP público IPv4), escolha Enable (Habilitar).

   viii. (Opcional) Para executar as Instâncias spot com uma função do IAM, em IAM instance profile (Perfil de instância do IAM), escolha a função.

   ix. (Opcional) Para executar um script de startup, copie-o para User data.

x. (Opcional) Para adicionar uma tag, escolha Create tag (Criar tag), insira uma chave e valor da tag, e escolha Create (Criar). Repita esse procedimento para cada tag.

   Para cada tag, para marcar as instâncias e a solicitação de frota spot com a mesma tag, verifique se as opções Instances (Instâncias) e Fleet (Frota) estão selecionadas. Para marcar apenas as instâncias iniciadas pela frota, desmarque Frota. Para aplicar tag apenas na solicitação de frota spot, desmarque Instances (Instâncias).

5. Em Additional request details (Detalhes de configuração adicionais), faça o seguinte:

   a. Revise os detalhes de solicitação adicional. Para fazer alterações, desmarque Apply defaults (Aplicar padrões).

   b. (Opcional) Em IAM fleet role (Função de frota do IAM), você pode usar a função padrão ou especificar uma função diferente. Para usar a função padrão depois de ter alterado a função, escolha Use default role (Usar função padrão).

   c. (Opcional) Em Maximum price (Preço máximo), você pode usar o preço máximo padrão (preço sob demanda) ou especificar o preço máximo que você está disposto a pagar. Se o seu preço máximo for inferior ao preço spot dos tipos de instâncias selecionados por você, as Instâncias spot não serão executadas.

   d. (Opcional) Para criar uma solicitação que seja válida somente em um período específico, edite Request valid from e Request valid until.

   e. (Opcional) Por padrão, terminamos as Instâncias spot quando a solicitação de frota spot expira. Para mantê-las em execução depois que sua solicitação expirar, desmarque Terminate the instances when the request expires (Encerrar as instâncias na expiração da solicitação).

   f. (Opcional) Para registrar as Instâncias spot em um load balancer, escolha Receive traffic from one or more load balancers (Receber tráfego de um ou mais load balancers) e escolha um ou mais Classic Load Balancers ou grupos de destino.

6. Em Minimum compute unit (Unidade mínima de computação), escolha as especificações mínimas de hardware (vCPUs, memória e armazenamento) necessárias para a aplicação ou tarefa, as specs (como especificações) ou as an instance type (como um tipo de instância).

   - Em as specs (como especificações), especifique o número necessário de vCPUs e a quantidade de memória.
   - Em as an instance type (como um tipo de instância), aceite o tipo de instância padrão ou escolha Change instance type (Alterar tipo de instância) para escolher outro tipo de instância.

7. Em Modify target capacity (Modificar capacidade-alvo), faça o seguinte:

   a. Em Total target capacity (Capacidade-alvo total), especifique o número de unidades a serem solicitadas. Para o tipo de unidade, você pode escolher Instances (Instâncias), vCPUs ou Memory (MiB) [Memória (MiB)]. Para especificar uma capacidade de destino igual a 0 para que seja possível adicionar capacidade posteriormente, escolha Maintain target capacity (Manter a capacidade do destino).

   b. (Opcional) Em Include On-Demand base capacity (Incluir capacidade sob demanda de base), especifique o número de unidades sob demanda a serem solicitadas. O número deve ser menor queTotal target capacity (Capacidade total pretendida). O Amazon EC2 calcula e aloca a diferença às unidades spot a serem solicitadas.

   > **Important**
   >
   > Para especificar a capacidade sob demanda opcional, primeiro, escolha um modelo de lançamento.

   c. (Opcional) Por padrão, o Amazon EC2 encerra instâncias spot quando elas são interrompidas. Para manter a capacidade do destino, selecione Maintain target capacity (Manter a capacidade de destino). Em seguida, você poderá especificar se o Amazon EC2 vai encerrar, interromper ou hibernar as instâncias spot que forem interrompidas. Para fazer isso, escolha a opção correspondente em Interruption behavior.

   > **Note**
   >
   > Se uma AMI especificada nos parâmetros de execução estiver descadastrada ou desabilitada, não será possível executar nenhuma instância nova com base na AMI. Para frotas configuradas para manter a capacidade de destino, a capacidade de destino não será mantida.

   d. (Opcional) Para permitir que a frota spot inicie uma instância spot substituta quando uma notificação de rebalanceamento de instância for emitida para uma instância spot existente na frota, selecione Capacity rebalance (Rebalanceamento de capacidade) e escolha uma estratégia de substituição de instância. Se escolher Launch before terminate (Iniciar antes de terminar), especifique o atraso (em segundos) antes que a frota spot encerre as instâncias antigas. Para ter mais informações, consulte Rebalanceamento de capacidade.

e. (Opcional) Para controlar o valor pago por hora por todas as instâncias spot da sua frota, selecione Manter custo pretendido para instâncias spot e insira o valor total máximo que você está disposto a pagar por hora. Quando o valor total máximo for alcançado, a frota spot interromperá a execução de instâncias spot mesmo que a capacidade do destino ainda não tenha sido atingida. Para ter mais informações, consulte Controle de gastos.

8. Em Network (Rede), faça o seguinte:

   a. Em Rede, escolha uma VPC existente ou crie uma nova.

      [VPC existente] escolha a VPC.

      [VPC nova] Escolha Create new VPC (Criar nova VPC) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

   b. (Opcional) Em Availability Zones (Zonas de disponibilidade), deixe que a AWS escolha as zonas de disponibilidade para suas instâncias spot ou especifique uma ou mais zonas de disponibilidade.

      Se houver mais de uma sub-rede em uma zona de disponibilidade, escolha a sub-rede apropriada em Subnet (Sub-rede). Para adicionar sub-redes, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

9. Em Instance type requirements (Requisitos de tipo de instância), você pode especificar atributos de instância e deixar o Amazon EC2 identificar os tipos de instância com esses atributos ou pode especificar uma lista de instâncias. Para ter mais informações, consulte Seleção de tipo de instância baseada em atributos para frota spot.

   a. Se escolher Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação), especifique os atributos da instância da seguinte forma:

      i. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.

      ii. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.

iii. (Opcional) Em Additional instance attributes (Atributos de instância adicionais), você pode, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais uma restrição à solicitação. É possível omitir os atributos adicionais; quando omitidos, os valores padrão são usados. Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores na Referência da linha de comando do Amazon EC2.

iv. (Opcional) Para visualizar os tipos de instância com os atributos especificados, expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes). Para excluir tipos de instância dos tipos a serem usados na solicitação selecione as instâncias e escolha Exclude selected instance types (Excluir tipos de instância selecionados).

b. Se escolher Manually select instance types (Selecionar manualmente os tipos de instância), a frota spot fornecerá uma lista padrão de tipos de instância. Para selecionar mais tipos de instância, escolha Add instance types (Adicionar tipos de instância), selecione os tipos de instância a serem usados em sua solicitação e escolha Select (Selecionar). Para excluir tipos de instância, selecione os tipos de instância e escolha Delete (Excluir).

10. Em Allocation Strategy (Estratégia de alocação), escolha a estratégia que atenda às suas necessidades. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.
11. Em Your fleet request at a glance (Visão rápida da sua solicitação de frota), revise a configuração de frota e faça os ajustes necessários.
12. (Opcional) Para fazer download de uma cópia da configuração de execução para uso com a AWS CLI, escolha JSON config.
13. Escolha Executar.

O tipo de solicitação de frota spot é `fleet`. Quando a solicitação for atendida, as solicitações do tipo `instance` serão adicionadas, onde o estado será `active` e o status será `fulfilled`.

Crie uma frota spot usando a AWS CLI

Para criar uma solicitação de frota spot usando a AWS CLI

- Use o comando request-spot-fleet para criar uma solicitação de frota spot.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obter arquivos de configuração de exemplo, consulte Exemplos de configuração de frota spot.

A seguir está um exemplo de saída:

```
{
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Marcar uma frota spot

Para ajudar a categorizar e gerenciar as solicitações de frota spot, você pode marcá-las com metadados personalizados. Você pode atribuir uma tag a uma solicitação de frota spot ao criá-la ou posteriormente. Você pode atribuir tags usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Quando você marca uma solicitação de frota spot, as instâncias e os volumes que são executados pela frota spot não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota spot. Você pode optar por atribuir tags somente à solicitação de frota spot, somente às instâncias executadas pela frota, somente aos volumes anexados às instâncias executadas pela frota ou aos todos os três.

> **Note**
>
> As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Não é possível marcar volumes que estão anexados a Instâncias spot.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Conteúdo

- Pré-requisito
- Marcar uma nova frota spot
- Marcar uma nova frota spot e as instâncias e os volumes que ela executa
- Marcar uma frota spot existente
- Exibir tags de solicitações de frota spot

Pré-requisito

Conceda ao usuário permissão para marcar recursos. Para ter mais informações, consulte Exemplo: marcar recursos.

Para conceder a um usuário permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Isso concede ao usuário permissão para criar tags.
- A ação `ec2:RequestSpotFleet`. Concede ao usuário permissão para criar uma solicitação de frota spot.
- Para `Resource`, você deve especificar `"*"`. Permite que os usuários marquem todos os tipos de recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

No momento, não oferecemos suporte para permissões no nível do recurso para o recurso `spot-fleet-request`. Se especificar `spot-fleet-request` como um recurso, você receberá uma exceção não autorizada quando tentar marcar a frota. O exemplo a seguir ilustra como não definir a política.

```
{
    "Effect": "Allow",
```

```
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Marcar uma nova frota spot

Como marcar uma nova solicitação de frota spot usando o console

1. Siga o procedimento do Criar uma solicitação de frota spot usando parâmetros definidos (console).
2. Para adicionar uma tag, expanda Additional configurations (Configurações adicionais), escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag. Repita esse procedimento para cada tag.

   Para cada tag, você pode marcar a solicitação de frota spot e as instâncias com a mesma tag. Para marcar ambas, verifique se Instance tags (Tags de instância) e Fleet tags (Tags de frota) estão selecionados. Para marcar somente a solicitação de frota spot, desmarque Instance tags

(Tags de instância). Para marcar apenas as instâncias executadas pela frota, desmarque Fleet tags (Tags de frota).

3. Preencha os campos obrigatórios para criar uma solicitação de frota spot e escolha Launch (Executar). Para ter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos (console).

Para marcar uma nova solicitação de frota spot usando a AWS CLI

Para marcar uma solicitação de frota spot ao criá-la, defina-a da seguinte maneira:

- Especifique as etiquetas para a solicitação de frota spot em `SpotFleetRequestConfig`.
- Em `ResourceType`, especifique `spot-fleet-request`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

No exemplo a seguir, a solicitação de frota spot é marcada com duas tags: Key=Environment e Value=Production, e Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large"
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
```

```
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Marcar uma nova frota spot e as instâncias e os volumes que ela executa

Para marcar uma nova solicitação de frota spot e as instâncias e os volumes que ela executa usando a AWS CLI

Para marcar uma solicitação de frota spot ao criá-la e marcar as instâncias e os volumes quando elas são executadas pela frota, defina a configuração da solicitação de frota spot da seguinte maneira:

Tags de solicitações de frota spot:

- Especifique as etiquetas para a solicitação de frota spot em `SpotFleetRequestConfig`.
- Em `ResourceType`, especifique `spot-fleet-request`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

Tags de instância:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Em `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

  Como alternativa, você pode especificar as tags da instância no modelo de execução que é referenciado na solicitação de frota spot.

Tags de volume:

- Especifique as tags para os volumes no modelo de execução mencionado na solicitação de frota spot. A marcação de volume em `LaunchSpecifications` não é compatível.

No exemplo a seguir, a solicitação de frota spot é marcada com duas tags: Key=Environment e Value=Production, e Key=Cost-Center e Value=123. As instâncias executadas pela frota são marcadas com uma tag (que é a mesma que uma das tags da solicitação de frota spot): Keys=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
```

```
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Para marcar instâncias executadas por uma frota spot usando a AWS CLI

Para marcar instâncias quando elas são executadas pela frota, você pode especificar as tags no modelo de execução referenciado na solicitação de frota spot ou especificar as tags na configuração da solicitação de frota spot da seguinte maneira:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Em `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

No exemplo a seguir, as instâncias que são executadas pela frota são marcadas com uma tag: Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
```

```
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Para marcar volumes anexados a instâncias sob demanda executadas por uma frota spot usando a AWS CLI

Para marcar volumes ao serem criados pela frota, é necessário especificar as tags no modelo de execução mencionado na solicitação de frota spot.

> **Note**
>
> As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Não é possível marcar volumes que estão anexados a Instâncias spot.
> A marcação de volume em `LaunchSpecifications` não é compatível.

Marcar uma frota spot existente

Para marcar uma solicitação de frota spot existente usando o console

Depois de criar uma solicitação de frota spot, você pode adicionar tags à solicitação de frota usando o console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de frota spot existente usando a AWS CLI

Você pode usar o comando create-tags para marcar os recursos existentes. No exemplo a seguir, a solicitação de frota spot existente é marcada com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Exibir tags de solicitações de frota spot

Para visualizar tags de solicitação de frota spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e escolha a guia Tags.

Para descrever as tags de solicitação de frota spot

Use o comando describe-tags para visualizar as tags para o recurso especificado. No exemplo a seguir, você descreve as tags da solicitação de frota spot especificada.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
```

```
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Você também pode visualizar as tags de uma solicitação de frota spot descrevendo a solicitação de frota spot.

Use o comando describe-spot-fleet-requests para visualizar a configuração da solicitação de frota spot especificada, que inclui todas as tags especificadas para a solicitação de frota.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
```

```
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Descrever a frota spot

A frota spot executará instâncias spot quando o preço máximo exceder o preço spot e a capacidade estiver disponível. As Instâncias spot serão executadas até serem interrompidas ou até você as encerrar.

Para descrever sua frota spot (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot. Para ver os detalhes da configuração, escolha Description (Descrição).
4. Para listar as instâncias spot para a frota spot, escolha Instances (Instâncias).
5. Para visualizar o histórico da frota spot, escolha a guia History (Histórico).

Para descrever sua frota spot (AWS CLI)

Use o comando describe-spot-fleet-requests para descrever as solicitações de frota spot.

```
aws ec2 describe-spot-fleet-requests
```

Use o comando describe-spot-fleet-instances para descrever as instâncias spot da frota spot especificada.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Use o comando describe-spot-fleet-request-history para descrever o histórico da solicitação de frota spot especificada.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

Modificar uma solicitação de frota spot

Você pode modificar uma solicitação de frota spot ativa para executar as seguintes tarefas:

- Aumentar a capacidade de destino e a porção sob demanda
- Reduzir a capacidade de destino e a porção sob demanda

> **Note**
>
> Você não pode modificar uma solicitação única de frota spot. É possível modificar uma solicitação de frota spot ao selecionar a opção Maintain target capacity (Manter capacidade de destino) ao criar a solicitação de frota spot.

Quando você aumenta a capacidade pretendida, a frota spot executa instâncias spot adicionais. Quando você aumenta a parte sob demanda, a frota spot inicia Instâncias sob demanda adicionais.

Quando você aumenta a capacidade pretendida, a frota spot executará as Instâncias spot adicionais de acordo com a estratégia de alocação de solicitação de frota spot.

Quando você diminui a capacidade de destino, a frota spot cancela todas as solicitações abertas que excedem a nova capacidade pretendida. Você pode solicitar que a frota spot encerre instâncias spot até o tamanho da frota atingir a nova capacidade pretendida. Se a estratégia de alocação for `diversified`, a frota spot encerrará as instâncias nos grupos. Como alternativa, você pode solicitar que a frota spot mantenha seu tamanho atual, mas não substitua as instâncias spot interrompidas ou encerradas manualmente.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Para modificar uma solicitação de frota spot (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha Actions (Ações) e Modify target capacity (Modificar capacidade de destino).
5. Em Modify target capacity (Modificar capacidade de destino), faça o seguinte:
    a. Insira a nova capacidade de destino e a porção sob demanda
    b. (Opcional) Se você estiver reduzindo a capacidade de destino, mas deseja manter a frota no tamanho atual, desmarque Terminate instances (Encerrar instâncias).
    c. Selecione Enviar.

Para modificar uma solicitação de frota spot usando a AWS CLI

Use o comando modify-spot-fleet- request para atualizar a capacidade pretendida da solicitação de frota spot especificada.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

Você pode modificar o comando anterior da seguinte forma para diminuir a capacidade de destino da frota spot especificada sem encerrar instâncias spot como resultado.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

Cancelar uma solicitação de frota spot

Se não precisar mais de frota spot, você cancelar a solicitação de frota spot. Depois que você cancela uma solicitação de frota spot todas as solicitações spot associadas à frota são canceladas, para que nenhuma nova instância spot seja iniciada.

Ao canelar uma frota spot, você deve especificar se deseja encerrar todas as suas instâncias. Isso inclui tanto instâncias sob demanda quanto instâncias spot.

Se você especificar que as instâncias deverão ser encerradas quando a frota for cancelada, a frota entrará no estado `cancelled_terminating`. Caso contrário, a solicitação de frota entrará no estado `cancelled_running` e as instâncias continuarão em execução até que sejam interrompidas ou encerradas manualmente.

Restrições

- Você pode excluir até 100 frotas com a mesma solicitação. Nenhuma frota será excluída se você exceder o número especificado.

Para cancelar uma solicitação de frota spot (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha Ações, Cancelar solicitação.
5. Na caixa de diálogo Adicionar regiões para replicação, faça o seguinte:
   a. Para encerrar as instâncias associadas ao mesmo tempo que cancela a solicitação de frota spot, deixe a caixa de seleção Encerrar instâncias marcada. Para encerrar a solicitação de frota spot sem encerar as instâncias associadas, desmarque a caixa de seleção Encerrar instâncias.
   b. Selecione a opção Confirmar.

Para cancelar uma solicitação de frota spot e encerrar as suas instâncias usando a AWS CLI

Use o comando cancel-spot-fleet-requests para cancelar a solicitação de frota spot especificada e encerrar suas instâncias sob demanda e spot.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Exemplo de saída

```
{
    "SuccessfulFleetRequests": [
        {
```

```
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Para cancelar uma solicitação de frota spot sem encerrar as suas instâncias usando a AWS CLI

Você pode modificar o comando anterior usando o parâmetro `--no-terminate-instances` para cancelar a frota spot especificada sem encerrar suas instâncias sob demanda e spot.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Exemplo de saída

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Métricas do CloudWatch para frota spot

O Amazon EC2 fornece métricas do Amazon CloudWatch que você pode usar para monitorar sua frota spot.

> **Important**
>
> Para garantir uma precisão, recomendamos que você habilite o monitoramento detalhado para usar essas métricas. Para ter mais informações, consulte Habilitar ou desabilitar o monitoramento detalhado para instâncias.

Para obter mais informações sobre as métricas do CloudWatch fornecidas pelo Amazon EC2, consulte Monitorar instâncias usando o CloudWatch.

Métricas de frota spot

O namespace `AWS/EC2Spot` inclui as métricas a seguir, além das métricas do CloudWatch das Instâncias spot em sua frota. Para ter mais informações, consulte Métricas de instância.

Métrica	Descrição
`AvailableInstancePoolsCount`	Os grupos de capacidade spot especificados na solicitação de frota spot. Unidades: contagem
`BidsSubmittedForCapacity`	A capacidade para a qual o Amazon EC2 enviou solicitações de frota spot. Unidades: contagem
`EligibleInstancePoolCount`	Os grupos de capacidade spot especificados na solicitação de frota spot onde o Amazon EC2 pode atender às solicitações. O Amazon EC2 não atende a solicitações em grupos nos quais o preço máximo que você está disposto a pagar por instâncias spot é menor que o preço spot ou o preço spot é maior que o preço das instâncias sob demanda. Unidades: contagem
`FulfilledCapacity`	A capacidade preenchida pelo Amazon EC2. Unidades: contagem
`MaxPercentCapacityAllocation`	O valor máximo de `PercentCapacityAllocation` em todos os grupos de frota spot especificados na solicitação de frota spot.

Métrica	Descrição
	Unidades: percentual
PendingCapacity	A diferença entre TargetCapacity e FulfilledCapacity. Unidades: contagem
PercentCapacityAllocation	A capacidade alocada para o grupo de capacidade spot para as dimensões especificadas. Para obter o valor máximo registrado em todos os grupos de capacidade spot, use MaxPercentCapacityAllocation. Unidades: percentual
TargetCapacity	A capacidade pretendida da solicitação de frota spot. Unidades: contagem
TerminatingCapacity	A capacidade que está sendo encerrada, pois a capacidade provisionada é maior que a capacidade de destino. Unidades: contagem

Se a unidade de medida para uma métrica é Count, a estatística mais útil é Average.

Dimensões da frota spot

Para filtrar os dados da frota spot, use as dimensões a seguir.

Dimensões	Descrição
AvailabilityZone	Filtre os dados por zona de disponibilidade.
FleetRequestId	

Dimensões	Descrição
	Filtre os dados por solicitação de frota de spot.
`InstanceType`	Filtre os dados por tipo de instância.

Exibir as métricas do CloudWatch para sua frota spot

Você pode visualizar as métricas do CloudWatch para sua frota spot usando o console do Amazon CloudWatch. Essas métricas são exibidas como gráficos de monitoramento. Esses gráficos mostrarão pontos de dados se a frota spot estiver ativa.

As métricas são agrupadas primeiro pelo namespace e, em seguida, por várias combinações de dimensões dentro de cada namespace. Por exemplo, você pode visualizar todas as métricas da frota spot ou grupos de métricas de frota spot por ID de solicitação de frota spot, tipo de instância ou Zona de disponibilidade.

Para visualizar métricas de frota spot

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace do EC2 Spot.

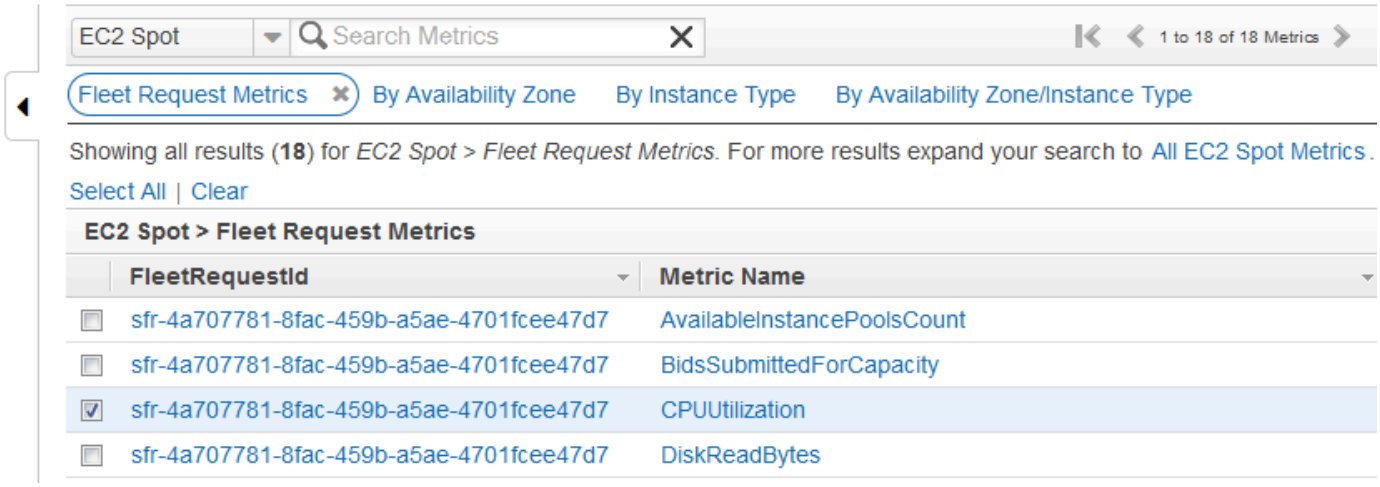
   > **Note**
   >
   > Se o namespace do EC2 Spot não for exibido, há dois motivos para isso. Você ainda não usou a frota spot, apenas os serviços da AWS em uso enviam métricas para o Amazon CloudWatch. Ou, se você não tiver usado a frota spot nas últimas duas semanas, o namespace não será exibido.

4. (Opcional) Para filtrar as métricas por dimensão, selecione uma das seguintes ações:

   - Fleet Request Metrics (Métricas de solicitação da frota): agrupar por solicitação de frota spot
   - By Availability Zone (Por zona de disponibilidade): agrupar por solicitação de frota spot e zona de disponibilidade
   - By Instance Type (Por tipo de instância): agrupar por solicitação de frota spot e tipo de instância

- By Availabiilty Zone/Instance Type (Por zona de disponibilidade/tipo de instância): agrupar por solicitação de frota spot, zona de disponibilidade e tipo de instância

5. Para visualizar os dados de uma métrica, marque a caixa de seleção ao lado da métrica.



Escalabilidade automátia para frota spot

A escalabilidade automática é a capacidade de aumentar ou diminuir a capacidade de destino de sua frota spot automaticamente com base na demanda. Uma frota spot pode executar instâncias (aumentar a escala na horizontal) ou encerrar instâncias (reduzir a escala na horizontal), no intervalo escolhido, em resposta a uma ou mais políticas de escalabilidade.

A frota spot oferece suporte aos seguintes tipos de escalabilidade automática:

- Escalabilidade do monitoramento do objetivo: aumenta ou diminui a capacidade atual da frota com base em um valor pretendido para uma métrica específica. Isso é semelhante à forma como o termostato mantém a temperatura da sua casa, ou seja, você seleciona a temperatura e o termostato faz o resto.
- Escalabilidade em etapas: aumenta ou diminui a capacidade atual da frota com base em um conjunto de ajustes de escalabilidade, conhecidos como ajustes em etapas, que variam com base no tamanho da ruptura do alarme.
- Escalabilidade programado: aumenta ou diminui a capacidade atual da frota com base em data e hora.

Se estiver usando peso da instância, lembre-se de que a frota spot pode exceder a capacidade de destino conforme necessário. A capacidade atendida pode ser um número de ponto flutuante,

mas a capacidade de destino deve ser um inteiro, portanto, a frota spot é arredondada para o próximo inteiro. Você deve levar em conta esses comportamentos ao ver o resultado de uma política de escalabilidade quando um alarme é acionado. Por exemplo, suponha que a capacidade de destino seja 30, a capacidade atendida seja 30,1 e a política de escalabilidade subtraia 1. Quando o alarme é acionado, o processo de escalabilidade automática subtrairá 1 de 30,1 para obter 29,1 e o arredondará para 30, portanto, nenhuma ação de escalabilidade é executada. Suponhamos também que você selecione os pesos de instância 2, 4 e 8 e uma capacidade de destino igual a 10, mas nenhuma instância de peso 2 esteja disponível. Sendo assim, a frota spot provisionou instâncias de pesos 4 e 8 para uma capacidade atendida igual a 12. Se a política de escalabilidade reduzir a capacidade de destino em 20% e um alarme for acionado, o processo de escalabilidade automática subtrairá 12*0,2 de 12 para obter 9,6 e o arredondará para 10, portanto, nenhuma ação de escalabilidade será executada.

As políticas de escalabilidade que podem ser criadas para a frota spot oferecem suporte a um período de desaquecimento. Esse é o número de segundos após o encerramento de uma ação de escalabilidade em que as atividades de escalabilidade anteriores, relacionadas ao acionamento, podem influenciar eventos futuros de escalabilidade. Para expandir as políticas enquanto o período do desaquecimento estiver em vigor, a capacidade que foi adicionada pelo evento de expansão anterior que iniciou o desaquecimento é calculada como parte da capacidade desejada para a expansão seguinte. A intenção é expandir de forma contínua (mas não excessivamente). Para políticas de redução, o período do desaquecimento é utilizado para bloquear a escala subsequente nas solicitações até que expire. A intenção é reduzir de forma conservadora para proteger a disponibilidade de sua aplicação. Contudo, se outro alarme acionar uma política de expansão durante o período do desaquecimento após uma redução, a escalabilidade automática expandirá seu destino dimensionável imediatamente.

Recomendamos que você defina a escalabilidade com base nas métricas da instância com intervalos de 1 minuto, pois isso garante resposta mais rápida às mudanças de utilização. Aumentar a escalabilidade com base em métricas com intervalos de cinco minutos pode resultar em tempo de resposta mais lento e na escalabilidade com base em dados de métricas obsoletos. Para enviar dados de métrica das instâncias ao CloudWatch em períodos de 1 minuto, você deve habilitar especificamente o monitoramento detalhado. Para ter mais informações, consulte Habilitar ou desabilitar o monitoramento detalhado para instâncias e Criar uma solicitação de frota spot usando parâmetros definidos (console).

Para obter mais informações sobre configuração de escalabilidade para a frota spot, consulte os recursos a seguir:

- Seção application-autoscaling da Referência de comandos da AWS CLI
- Referência à API do Application Auto Scaling
- Guia do usuário do Application Auto Scaling

Permissões do IAM obrigatórias para escalabilidade automática de frota spot

A escalabilidade automática para frota spot é possível por uma combinação das APIs do Amazon EC2, do Amazon CloudWatch e do Application Auto Scaling. As solicitações de frota spot são criadas com o Amazon EC2, os alarmes são criados com o CloudWatch e as políticas de escalabilidade são criadas com o Application Auto Scaling.

Além das permissões do IAM para frota spot e do Amazon EC2, o usuário que acessa as configurações de escala de frota deve ter as permissões adequadas para os serviços compatíveis com escalação dinâmica. Os usuários devem ter permissões para usar as ações mostradas no exemplo de política a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Também é possível criar suas próprias políticas do IAM que permitem permissões mais refinadas para chamadas à API do Application Auto Scaling. Para obter mais informações, consulte Controle de acesso e autenticação no Manual do usuário do Application Auto Scaling.

O serviço do Application Auto Scaling também precisa de permissão para descrever a frota spot e os alarmes do CloudWatch, além de permissões para modificar a capacidade de destino da frota spot em seu nome. Se você habilitar a escalabilidade automática para a frota spot, ela criará uma função vinculada ao serviço chamada `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Essa função vinculada ao serviço concede ao Application Auto Scaling permissão para descrever os alarmes das políticas, monitorar a capacidade atual da frota e modificar a capacidade da frota. A função de frota spot gerenciada original para o Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, mas ela não é mais necessária. Essa função vinculada ao serviço é a função padrão do Application Auto Scaling. Para obter mais informações, consulte Funções vinculadas ao serviço no Manual do usuário do Application Auto Scaling.

Alterar a escala da frota spot usando as políticas de monitoramento do objetivo

Com as políticas de dimensionamento com monitoramento do objetivo, você seleciona uma métrica e define um valor pretendido. A frota spot cria e gerencia os alarmes do CloudWatch que acionam a política de escalabilidade e calculam o ajuste de escalabilidade com base na métrica e no valor de destino. A política de escalabilidade adiciona ou remove capacidade conforme necessário para manter a métrica no valor de destino especificado ou próxima a ele. Além de manter a métrica próxima ao valor de destino, uma política de escalabilidade de rastreamento de destino também se ajusta às flutuações na métrica, devido a um padrão de carga de flutuação, e minimiza as flutuações rápidas na capacidade da frota.

Você pode criar várias políticas de dimensionamento com monitoramento do objetivo para uma frota spot, desde que cada uma delas use uma métrica diferente. A escalabilidade da frota se baseia na política que fornece a maior capacidade da frota. Com isso, é possível cobrir vários cenários e garantir que sempre haja capacidade suficiente para processar suas workloads de aplicações.

Para garantir a disponibilidade da aplicação, a frota se expande proporcionalmente à métrica o mais rápido possível, mas se retrai gradualmente.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Não edite ou exclua os alarmes do CloudWatch que a frota spot gerencia para uma política de dimensionamento com monitoramento do objetivo. A frota spot exclui os alarmes automaticamente quando você exclui a política de dimensionamento com monitoramento do objetivo.

Limitação

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalação automática não é compatível com solicitações do tipo `request`.

Para configurar uma política de rastreamento (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione a solicitação de frota spot e escolha Auto Scaling.
4. Se a escalabilidade automática não estiver configurada, escolha Configurar.
5. Use Escalar capacidade entre para definir a capacidade mínima e máxima para sua frota. A escalabilidade automática não dimensiona a frota abaixo da capacidade mínima ou acima da capacidade máxima.
6. Em Policy Name (Nome da política), digite um nome para a política.
7. Escolha uma Target metric.
8. Digite um Target value (Valor de destino) para a métrica.
9. Em Período de esfriamento, especifique um novo valor (em segundos) ou mantenha o padrão.
10. (Opcional) Selecione Disable scale-in para omitir a criação de uma política de redução baseada na configuração atual. Você pode criar uma política de redução usando uma configuração diferente.
11. Escolha Save (Salvar).

Para configurar uma política de rastreamento de destino usando a AWS CLI

1. Registre a solicitação de frota spot como um destino escalável usando o comando register-scalable-target.
2. Crie uma política de escalabilidade usando o comando put-scaling-policy.

Alterar a escala da frota spot usando políticas de escalabilidade em etapas

Com as políticas de escalabilidade em etapas, você especifica os alarmes do CloudWatch para acionamento do processo de escalabilidade. Por exemplo, se você deseja aumentar a escala quando a utilização de CPU atinge um determinado nível, crie um alarme usando a métrica `CPUUtilization` fornecida pelo Amazon EC2.

Ao criar uma política de escalabilidade em etapas, você deve especificar um dos seguintes tipos de ajuste de escalabilidade:

- Add (Adicionar): aumente a capacidade de destino da frota por um número específico de unidades de capacidade ou por uma porcentagem especificada da capacidade atual.
- Remove (Remover): reduza a capacidade de destino da frota por um número específico de unidades de capacidade ou por uma porcentagem especificada da capacidade atual.
- Set to (Definir como): defina a capacidade de destino da frota como o número especificado de unidades de capacidade.

Quando um alarme é acionado, o processo de escalabilidade automática calcula a nova capacidade de destino usando a capacidade atendida e as políticas de escalabilidade e, em seguida, atualiza a capacidade de destino corretamente. Por exemplo, suponha que a capacidade de destino e a capacidade atendida sejam 10 e a política de escalabilidade seja 1. Quando o alarme é acionado, o processo de escalabilidade automática adiciona 1 a 10 para obter 11, para que a frota spot execute uma instância.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Limitação

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações do tipo `request` nem blocos spot.

Pré-requisitos

- Considere quais métricas do CloudWatch são importantes para sua aplicação. Você pode criar alarmes do CloudWatch com base nas métricas fornecidas pela AWS ou nas suas próprias métricas personalizadas.
- Para as métricas da AWS que você usará em suas políticas de escalabilidade, habilite a coleta das métricas do CloudWatch se o serviço que fornece as métricas não for habilitado por padrão.

Criar um alarme do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Alarmes.
3. Selecione Create alarm (Criar alarme).
4. Na página Specify metric and conditions (Especificar métrica e condições), selecione Select metric (Selecionar métrica).
5. Escolha Spot do EC2, Métricas de solicitação de frota, selecione uma métrica (por exemplo, TargetCapacity) e escolha Selecionar métrica.

   A página Specify metric and conditions (Especificar métrica e condições) será exibida, mostrando um gráfico e outras informações sobre a métrica selecionada.
6. Em Period (Período), escolha o período de avaliação para o alarme, por exemplo, 1 minuto. Ao avaliar o alarme, todos os períodos são agregados em um único ponto de dados.

   > **Note**
   >
   > Um período mais curto cria um alarme mais sensível.
7. Em Conditions (Condições), defina o alarme definindo a condição do limite. Por exemplo, é possível definir um limite para acionar o alarme sempre que o valor da métrica for maior que ou igual a 80%.
8. Em Additional configuration (Configuração adicional), para Datapoints to alarm (Pontos de dados para alarme), especifique quantos pontos de dados (períodos de avaliação) devem estar no estado ALARM para acionar o alarme, por exemplo, 1 período de avaliação para 2 de 3 períodos de avaliação. Isso cria um alarme que passará para o estado ALARM se houver violação de muitos períodos consecutivos. Para obter mais informações, consulte Avaliar um alarme no Guia do usuário do Amazon CloudWatch.
9. Para Missing data treatment (Tratamento de dados ausentes), selecione uma das opções (ou mantenha o padrão como Treat missing data as missing (Tratar dados ausentes como ausentes)). Para obter mais informações, consulte Configuração da forma como os alarmes do CloudWatch tratam dados ausentes no Manual do usuário do Amazon CloudWatch.
10. Escolha Next (Próximo).
11. (Opcional) Para receber notificações de um evento de dimensionamento, para Notification (Notificação), é possível escolher ou criar o tópico do Amazon SNS que você deseja usar para

receber notificações. Caso contrário, você poderá excluir a notificação agora e adicionar uma posteriormente, quando necessário.

12. Escolha Next (Próximo).
13. Em Add a description (Adicionar uma descrição), insira um nome e uma descrição para o alarme e selecione Next (Próximo).
14. Selecione Create alarm (Criar alarme).

Para configurar uma política de escalabilidade para a frota spot (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione a solicitação de frota spot e escolha Auto Scaling.
4. Se a escalabilidade automática não estiver configurada, escolha Configurar.
5. Use Escalar capacidade entre para definir a capacidade mínima e máxima para sua frota. As políticas de ajuste de escala não escalam a frota abaixo da capacidade mínima ou acima da capacidade máxima.
6. Em Políticas de ajuste de escala, Tipo de política, escolha Política de ajuste de escala em etapas.
7. Inicialmente, a opção Políticas de ajuste de escala contém as políticas de ajuste de escala em etapas denominadas ScaleUp e ScaleDown. Você pode completar essas políticas ou escolher Remover política para excluí-las. Você também pode escolher Add policy (Adicionar política).
8. Para definir a política, faça o seguinte:

    a. Em Policy Name (Nome da política), digite um nome para a política.

    b. Em Gatilho de políticas, selecione um alarme atual ou escolha Criar alarme para abrir o console do Amazon CloudWatch e criar um alarme.

    c. Em Modificar capacidade, defina a quantidade do ajuste de escala e os limites inferior e superior do ajuste da etapa. É possível adicionar ou remover um número específico de instâncias ou uma porcentagem do tamanho da frota atual ou definir a frota para um tamanho exato.

    Por exemplo, para criar uma política de ajuste de escala em etapas que aumente a capacidade da frota em 30%, escolha `Add`, digite `30` no próximo campo e escolha `percent`. Por padrão, o limite inferior de uma política de adição é o limite do alarme e o

limite superior é mais (+) infinito. Por padrão, o limite superior de uma política de remoção é o limite do alarme e o limite inferior é menos (-) infinito.

d. (Opcional) Para adicionar outra etapa, escolha Adicionar etapa.

e. Em Período de esfriamento, especifique um novo valor (em segundos) ou mantenha o padrão.

9. Escolha Salvar.

Para configurar políticas de escalabilidade em etapas para sua frota spot usando a AWS CLI

1. Registre a solicitação de frota spot como um destino escalável usando o comando register-scalable-target.
2. Crie uma política de escalabilidade usando o comando put-scaling-policy.
3. Crie um alarme que acione as políticas de escalabilidade usando o comando put-metric-alarm.

Alterar a escala da frota spot usando a escalabilidade programada

A escalabilidade com base em uma programação permite que você dimensione sua aplicação em resposta a alterações de demanda. Para usar a escalabilidade programada, crie ações programadas que instruam a frota spot a executar ações de escalabilidade em momentos específicos. Ao criar uma ação programada, você especifica uma frota spot existente, quando a ação de escalabilidade deve ocorrer, a capacidade mínima e a capacidade máxima. É possível criar ações programadas para escalar uma única vez ou de forma programada.

Você só pode criar uma ação programada para Frotas spot que já existe. Não é possível criar uma ação programada ao mesmo tempo em que você cria uma frota spot.

Limitação

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações do tipo `request` nem blocos spot.

Para criar uma única ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.

4. Escolha Create Scheduled Action (Criar ação programada).
5. Em Name (Nome), especifique um nome para a ação programada.
6. Insira um valor para Minimum capacity (Capacidade mínima), Maximum capacity (Capacidade máxima), ou ambos.
7. Em Recurrence (Recorrência), escolha Once (Uma vez).
8. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
9. Selecione Enviar.

Para escalar em uma programação recorrente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Em Recurrence (Recorrência), escolha uma das programações predefinidas (por exemplo, Every day (Todos os dias)) ou escolha Custom (Personalizado) e digite uma expressão cron. Para obter mais informações sobre as expressões cron compatíveis com a escalabilidade programada, consulte Expressões cron no Guia do usuário do Amazon CloudWatch Events.
5. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
6. Selecione Enviar.

Para editar uma ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Selecione a ação programada e escolha Actions (Ações), Edit (Editar).
5. Faça as alterações necessárias e escolha Submit (Enviar).

Para excluir uma ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Selecione a ação programada e escolha Actions (Ações), Delete (Excluir).
5. Quando a confirmação for solicitada, escolha Excluir.

Para gerenciar a escalabilidade programada usando o AWS CLI

Use os seguintes comandos:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Monitorar eventos da frota usando o Amazon EventBridge

Quando o estado de uma Frota do EC2 é alterado, a Frota do EC2 emite uma notificação. A notificação é disponibilizada como um evento que é enviado para Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events). Eventos são emitidos com base no melhor esforço.

Com Amazon EventBridge, você pode criar regras que acionam ações programáticas em resposta a um evento. Por exemplo, você pode criar duas regras de EventBridge, uma que é acionada quando um estado da frota muda e uma que é acionada quando uma instância na frota é encerrada. Se o estado da frota for alterado, a primeira regra invocará um tópico do SNS para enviar uma notificação por e-mail para você. Se uma instância for encerrada, a segunda regra de invocará uma função do Lambda para executar uma nova instância.

Tópicos

- Tipos de evento de Frota do EC2
- Tipos de evento de frota spot
- Criar uma regra do Amazon EventBridge

Tipos de evento de Frota do EC2

> **Note**
>
> Apenas frotas do tipo `maintain` e `request` emitem eventos. As frotas do tipo `instant` não emitem eventos porque enviam solicitações únicas síncronas e o estado da frota é conhecido imediatamente na resposta.

Existem cinco tipos de eventos de Frota do EC2. Para cada tipo de evento, existem vários subtipos.

Os eventos são enviados para EventBridge no formato JSON. Os seguintes campos no evento formam o padrão de evento definido na regra e que acionam uma ação:

`"source": "aws.ec2fleet"`

Identifica que o evento é de Frota do EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica o tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica o subtipo de evento.

Tipos de evento

- Alteração do estado da EC2 Fleet
- Alteração da solicitação de instância spot da EC2 Fleet
- Alteração da instância da EC2 Fleet
- Informações da EC2 Fleet
- Erro de EC2 Fleet

Alteração do estado da EC2 Fleet

A Frota do EC2 envia um evento `EC2 Fleet State Change` para Amazon EventBridge quando um estado Frota do EC2 mudar.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução.

`deleted`

A solicitação de Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação de Frota do EC2 foi excluída dois dias depois que as instâncias foram encerradas.

`deleted_running`

A solicitação de Frota do EC2 foi excluída e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`deleted_terminating`

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`expired`

A solicitação de Frota do EC2 expirou. Se a solicitação tiver sido criada com conjunto `TerminateInstancesWithExpiration`, um evento `terminated` subsequente indicará que as instâncias estão encerradas.

`modify_in_progress`

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada.

`modify_succeeded`

A solicitação de Frota do EC2 foi modificada.

`submitted`

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`progress`

A solicitação de Frota do EC2 está em processo de ser atendida.

Alteração da solicitação de instância spot da EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Spot Instance Request Change` para Amazon EventBridge quando uma solicitação de Instância spot na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
```

```
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de instância spot foi atendida e tem uma instância spot associada.

`cancelled`

Você cancelou a solicitação de instância spot ou a solicitação de instância spot expirou.

`disabled`

Você interrompeu a instância spot.

`submitted`

A solicitação de instância spot foi enviada.

Alteração da instância da EC2 Fleet

O Frota do EC2 envia um evento de `EC2 Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
```

```
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Os possíveis valores para `sub-type` são:

`launched`

Uma nova instância foi executada.

`terminated`

A instância foi encerrada.

`termination_notified`

Uma notificação de encerramento de instância foi enviada quando uma instância spot foi encerrada pelo Amazon EC2 durante a redução da escala na vertical, quando a capacidade de destino da frota foi modificada para baixo, p. ex., de uma capacidade de destino de 4 para uma capacidade de destino de 3.

Informações da EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Information` para Amazon EventBridge quando há um erro durante a execução. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
```

```
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Os possíveis valores para `sub-type` são:

`fleetProgressHalted`

O preço em cada especificação de execução não é válido porque está abaixo do preço spot (todas as especificações de execução produziram `launchSpecUnusable` eventos). Uma especificação de execução pode se tornar válida se o preço spot mudar.

`launchSpecTemporarilyBlacklisted`

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`launchSpecUnusable`

O preço em uma especificação de execução não é válido porque está abaixo do preço spot.

`registerWithLoadBalancersFailed`

Falha na tentativa de registrar instâncias com balanceadores de carga. Para obter mais informações, consulte a descrição do evento.

Erro de EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Error` para Amazon EventBridge quando há um erro durante a execução. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
```

```
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Os possíveis valores para `sub-type` são:

`iamFleetRoleInvalid`

A frota do EC2 não tem as permissões necessárias para executar ou encerrar uma instância.

`allLaunchSpecsTemporarilyBlacklisted`

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`spotInstanceCountLimitExceeded`

Você atingiu o limite do número de Instâncias spot que você pode executar.

`spotFleetRequestConfigurationInvalid`

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

Tipos de evento de frota spot

Existem cinco tipos de eventos de frota spot. Para cada tipo de evento, existem vários subtipos.

Os eventos são enviados para EventBridge no formato JSON. Os seguintes campos no evento formam o padrão de evento definido na regra e que acionam uma ação:

`"source": "aws.ec2spotfleet"`

Identifica que o evento é da frota spot.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifica o tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica o subtipo de evento.

Tipos de evento

- Alteração do estado da frota spot do EC2
- Alteração da solicitação de instância spot da frota spot do EC2
- Alteração da instância da frota spot do EC2
- Informações sobre a frota spot do EC2
- Erro na frota spot do EC2

Alteração do estado da frota spot do EC2

A Frota spot envia um `EC2 Spot Fleet State Change` evento para Amazon EventBridge quando uma frota spot muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de frota spot foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução.

`cancelled`

A solicitação de frota spot foi cancelada e não há instâncias em execução. A frota spot será excluída dois dias após o encerramento das instâncias.

`cancelled_running`

A solicitação de frota spot foi cancelada e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`cancelled_terminating`

A solicitação de frota spot foi cancelada e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`expired`

A solicitação de frota spot expirou. Se a solicitação tiver sido criada com conjunto `TerminateInstancesWithExpiration`, um evento `terminated` subsequente indicará que as instâncias estão encerradas.

`modify_in_progress`

A solicitação de frota spot está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada.

`modify_succeeded`

A solicitação de frota spot foi modificada.

`submitted`

A solicitação de frota spot está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`progress`

A solicitação de frota spot está em processo de atendimento.

Alteração da solicitação de instância spot da frota spot do EC2

A Frota spot envia um evento de `EC2 Spot Fleet Spot Instance Request Change` para Amazon EventBridge quando uma solicitação de Instância spot da frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de instância spot foi atendida e tem uma instância spot associada.

`cancelled`

Você cancelou a solicitação de instância spot ou a solicitação de instância spot expirou.

`disabled`

Você interrompeu a instância spot.

`submitted`

A solicitação de instância spot foi enviada.

Alteração da instância da frota spot do EC2

A frota spot envia um evento de `EC2 Spot Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.


```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```


Os possíveis valores para `sub-type` são:

`launched`

Uma nova instância foi executada.

`terminated`

A instância foi encerrada.

`termination_notified`

Uma notificação de encerramento de instância foi enviada quando uma instância spot foi encerrada pelo Amazon EC2 durante a redução da escala na vertical, quando a capacidade de destino da frota foi modificada para baixo, p. ex., de uma capacidade de destino de 4 para uma capacidade de destino de 3.

Informações sobre a frota spot do EC2

A frota spot envia um evento do `EC2 Spot Fleet Information` para Amazon EventBridge quando há um erro durante o atendimento. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Os possíveis valores para `sub-type` são:

`fleetProgressHalted`

O preço em cada especificação de execução não é válido porque está abaixo do preço spot (todas as especificações de execução produziram `launchSpecUnusable` eventos). Uma especificação de execução pode se tornar válida se o preço spot mudar.

`launchSpecTemporarilyBlacklisted`

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`launchSpecUnusable`

O preço em uma especificação de execução não é válido porque está abaixo do preço spot.

`registerWithLoadBalancersFailed`

Falha na tentativa de registrar instâncias com balanceadores de carga. Para obter mais informações, consulte a descrição do evento.

Erro na frota spot do EC2

A frota spot envia um evento do `EC2 Spot Fleet Error` para Amazon EventBridge quando há um erro durante o atendimento. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Os possíveis valores para `sub-type` são:

`iamFleetRoleInvalid`

A frota spot não tem as permissões necessárias para executar ou encerrar uma instância.

`allLaunchSpecsTemporarilyBlacklisted`

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`spotInstanceCountLimitExceeded`

Você atingiu o limite do número de Instâncias spot que você pode executar.

`spotFleetRequestConfigurationInvalid`

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

Criar uma regra do Amazon EventBridge

Quando uma notificação de uma alteração de estado é emitida para uma EC2 Fleet ou frota spot, o evento da notificação é enviado para o Amazon EventBridge. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra.

Tópicos

- Use Amazon EventBridge para monitorar eventos de Frota do EC2
- Use o Amazon EventBridge para monitorar eventos de frota spot

Use Amazon EventBridge para monitorar eventos de Frota do EC2

Quando uma notificação de uma alteração de estado é emitida para uma EC2 Fleet, o evento da notificação é enviado para o Amazon EventBridge na forma de arquivo JSON. Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Os campos a seguir formam o padrão de evento definido na regra:

`"source": "aws.ec2fleet"`

Identifica que o evento é de Frota do EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica o tipo de evento.

```
"detail": { "sub-type": "submitted" }
```

Identifica o subtipo de evento.

Para obter a lista de eventos do EC2 Fleet e dados de eventos de exemplo, consultethe section called “Tipos de evento de Frota do EC2”.

Exemplos

- Criar uma regra de EventBridge para enviar uma notificação
- Criar uma regra de EventBridge para acionar uma função do Lambda

Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push móvel sempre que o Amazon EC2 emite uma notificação de Frota do EC2. O sinal neste exemplo é emitido como um evento de `EC2 Fleet State Change`, que aciona a ação definida pela regra.

Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para enviar uma notificação quando um estado de Frota do EC2 muda

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).

d. Escolha Próximo.

4. Em Build event pattern (Criar padrão de evento), faça o seguinte:

   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.

   b. Em Event pattern (Padrão de evento), nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

      Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

      i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

         A. Escolha Event pattern form (Formulário de evento).

         B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

         C. Para Service (Serviço da AWS), escolha EC2 Fleet (Frota do EC2).

         D. Em Event type (Tipo de evento), escolha EC2 Fleet Instance Change (Alteração da instância da frota do EC2).

         E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

      ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

         A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

         B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

   c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

   a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).
7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar Regra.

Para obter mais informações, consulte Amazon EventBridge rules (Regras do Amazon EventBridge) e Amazon EventBridge event patterns (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Guia do usuário do Amazon EventBridge).

Criar uma regra de EventBridge para acionar uma função do Lambda

O exemplo a seguir cria uma regra de EventBridge para acionar uma função do Lambda toda vez que Amazon EC2 emite uma notificação de Frota do EC2. O sinal neste exemplo é emitido como um evento de `EC2 Fleet Instance Change`, subtipo `launched`, que aciona a ação definida pela regra.

Antes de criar a regra de EventBridge, você deve criar a função do Lambda.

Como criar a função do Lambda a ser usada na regra EventBridge

1. Abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. Escolha Create function.
3. Digite um nome para sua função, configure o código e escolha Create function (Criar função).

Para obter mais informações sobre como usar o Lambda, consulte Criar uma função do Lambda com o console no Guia do desenvolvedor do AWS Lambda.

Para criar uma regra de EventBridge para acionar uma função do Lambda quando uma instância em um estado de Frota do EC2 muda

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   d. Escolha Próximo.
4. Em Build event pattern (Criar padrão de evento), faça o seguinte:
   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
   b. Em Event pattern (Padrão de evento) nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Fleet Instance Change` e ao subtipo `launched`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Para Service (Serviço da AWS), escolha EC2 Fleet (Frota do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Fleet Instance Change (Alteração da instância da frota do EC2).

E. Selecione Edit pattern (Editar padrão) e adicione `"detail": {"sub-type": ["launched"]` para corresponder ao padrão do evento de exemplo. Para o formato JSON adequado, insira uma vírgula (`,`) após o colchete anterior (`]`).

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Para Topic (Tópico), escolha a Lambda function (função Lambda) e, para Function (Função), escolha a função que você criou para responder quando o evento ocorrer.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar Regra.

Para obter um tutorial sobre como criar uma função do Lambda e uma EventBridge regra que executa a função do Lambda, consulte Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge (Tutorial: Registrar em log o estado de uma instância do Amazon EC2 usando o EventBridge) no AWS Lambda User Guide (Guia do usuário do Amazon EventBridge).

Use o Amazon EventBridge para monitorar eventos de frota spot

Quando uma notificação de alteração de estado é emitida para uma frota spot, o evento da notificação é enviado para o Amazon EventBridge na forma de arquivo JSON. Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Os campos a seguir formam o padrão de evento definido na regra:

```
"source": "aws.ec2spotfleet"
```

Identifica que o evento é da frota spot.

```
"detail-type": "EC2 Spot Fleet State Change"
```

Identifica o tipo de evento.

```
"detail": { "sub-type": "submitted" }
```

Identifica o subtipo de evento.

Para obter a lista de eventos Spot Fleet e dados de eventos de exemplo, consultethe section called “Tipos de evento de frota spot”.

Exemplos

- Criar uma regra de EventBridge para enviar uma notificação
- Criar uma regra de EventBridge para acionar uma função do Lambda

Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivos móveis sempre que Amazon EC2 emite uma notificação de frota spot. O sinal neste exemplo é emitido como um evento de `EC2 Spot Fleet State Change`, que aciona a ação definida pela regra. Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para enviar uma notificação quando o estado de uma Frota spot for alterado

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   d. Escolha Próximo.
4. Em Build event pattern (Criar padrão de evento), faça o seguinte:
   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
   b. Em Event pattern (Padrão de evento), nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Spot Fleet Instance Change`.

```
{
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Em AWS Service (Produto da), escolha EC2 Spot Fleet (Frota spot do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Spot Fleet Instance Change (Alteração da instância da frota spot do EC2).

E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar Regra.

Para obter mais informações, consulte Amazon EventBridge rules (Regras do Amazon EventBridge) e Amazon EventBridge event patterns (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Guia do usuário do Amazon EventBridge).

Criar uma regra de EventBridge para acionar uma função do Lambda

O exemplo a seguir cria uma regra de EventBridge para acionar uma função do Lambda sempre que Amazon EC2 emite uma notificação de frota spot. O sinal neste exemplo é emitido como um evento de `EC2 Spot Fleet Instance Change`, subtipo `launched`, que aciona a ação definida pela regra.

Antes de criar a regra de EventBridge, você deve criar a função do Lambda.

Como criar a função do Lambda a ser usada na regra EventBridge

1. Abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. Escolha Create function.
3. Digite um nome para sua função, configure o código e escolha Create function (Criar função).

   Para obter mais informações sobre como usar o Lambda, consulte Criar uma função do Lambda com o console no Guia do desenvolvedor do AWS Lambda.

Para criar uma regra de EventBridge para acionar uma função do Lambda quando uma instância de uma Frota spot muda de estado

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:

   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.

c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).

d. Escolha Próximo.

4. Em Build event pattern (Criar padrão de evento), faça o seguinte:

a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.

b. Em Event pattern (Padrão de evento) nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Spot Fleet Instance Change` e ao subtipo `launched`.

```
{
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Em AWS Service (Produto da), escolha EC2 Spot Fleet (Frota spot do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Spot Fleet Instance Change (Alteração da instância da frota spot do EC2).

E. Selecione Edit pattern (Editar padrão) e adicione `"detail": {"sub-type": ["launched"]` para corresponder ao padrão do evento de exemplo. Para o formato JSON adequado, insira uma vírgula (`,`) após o colchete anterior (`]`).

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Para Topic (Tópico), escolha a Lambda function (função Lambda) e, para Function (Função), escolha a função que você criou para responder quando o evento ocorrer.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

a. Revise os detalhes da regra e modifique-os conforme necessário.

b. Escolha Criar Regra.

Para obter um tutorial sobre como criar uma função do Lambda e uma EventBridge regra que executa a função do Lambda, consulte Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge (Tutorial: Registrar em log o estado de uma instância do Amazon EC2 usando o EventBridge) no AWS Lambda User Guide (Guia do usuário do Amazon EventBridge).

Tutoriais para EC2 Fleet e frota spot

Os tutoriais a seguir orientarão você pelos processos comuns de criação de frotas do EC2 e de frotas spot.

Tutoriais

- Tutorial: Usar a Frota do EC2 com ponderação de instâncias
- Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal
- Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas
- Tutorial : iniciar instâncias em blocos de capacidade
- Tutorial: Usar frota spot com ponderação de instâncias

Tutorial: Usar a Frota do EC2 com ponderação de instâncias

Este tutorial usa uma empresa fictícia chamada Example Corp para ilustrar o processo de solicitação de uma Frota do EC2 usando o peso da instância.

Objetivo

A Exemplo Corp, uma empresa farmacêutica, quer usar a capacidade computacional do Amazon EC2 para fazer a triagem dos compostos químicos que podem ser usados para combater o câncer.

Planejamento

Primeiro, a Exemplo Corp analisa as Melhores práticas de spot. Em seguida, a Exemplo Corp determina os requisitos para a Frota do EC2.

Tipos de instância

A Exemplo Corp tem uma aplicação de uso intenso de memória e recursos de computação que funciona melhor com, pelo menos, 60 GB de memória e oito CPUs virtuais (vCPUs). Eles querem maximizar esses recursos para a aplicação com o menor preço possível. A Exemplo Corp decide que qualquer um dos seguintes tipos de instância do EC2 atenderá às suas necessidades:

Tipo de instância	Memória (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Tipo de instância	Memória (GiB)	vCPUs

Capacidade de destino em unidades

Com o peso da instância, a capacidade de destino pode igualar um número de instâncias (o padrão) ou uma combinação de fatores, como núcleos (vCPUs), memória (GiB) e armazenamento (GB). Considerando a base para sua aplicação (60 GB de RAM e oito vCPUs) como uma unidade, a Exemplo Corp decide que 20 vezes essa quantidade atenderá às suas necessidades. Então, a empresa define a capacidade de destino da solicitação de Frota do EC2 como 20.

Pesos das instâncias

Depois de determinar a capacidade de destino, a Exemplo Corp calcula os pesos das instâncias. Para calcular o peso para cada tipo de instância, eles determinam as unidades de cada tipo de instância que são necessárias para atingir a capacidade de destino da seguinte forma:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 unidade de 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 unidades de 20

Portanto, a Exemplo Corp atribui os pesos de instância 1, 2 e 4 às respectivas configurações de execução na solicitação de Frota do EC2.

Preço por hora

A Exemplo Corp usa o Preço sob demanda por hora de instância como o ponto inicial de preço. Eles também podem usar os preços spot recentes ou uma combinação dos dois. Para calcular o preço por hora, eles dividem o preço inicial por hora de instância pelo peso. Por exemplo:

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.8xLarge	$2,8	4	0,7 USD

A Exemplo Corp pode usar um preço global por hora de 0,7 USD e ser competitiva para todos os três tipos de instância. Eles também podem usar um preço global por hora de 0,7 USD e um preço específico por hora de 0,9 USD na especificação de execução `r3.8xlarge`.

Verificar permissões

Antes de criar uma Frota do EC2, a Exemplo Corp verifica se ela tem uma função do IAM com as permissões necessárias. Para ter mais informações, consulte Pré-requisitos da Frota do EC2.

Criar um modelo de execução

Em seguida, a Exemplo Corp cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para ter mais informações, consulte Criar um modelo de inicialização.

Criar a Frota do EC2

A Example Corp cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2: No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
```

```
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A Example Corp cria a Frota do EC2 usando o seguinte comando create-fleet:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Para ter mais informações, consulte Criar uma Frota do EC2..

Atendimento

A estratégia de alocação determina de quais grupos de capacidade spot os Instâncias spot procedem.

Com a estratégia `lowest-price` (que é uma estratégia padrão), as Instâncias spot vêm do grupo com o menor preço spot por unidade no momento do atendimento. Para fornecer 20 unidades de capacidade, a Frota do EC2 executa 20 instâncias `r3.2xlarge` (20 dividido por 1), 10 instâncias `r3.4xlarge` (20 dividido por 2) ou 5 instâncias `r3.8xlarge` (20 dividido por 4).

Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A Frota do EC2 executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal

Este tutorial usa uma empresa fictícia chamada ABC Online para ilustrar o processo de solicitação de uma Frota do EC2 com opção sob demanda como capacidade principal e capacidade spot (se disponível).

Objetivo

A ABC Online, uma empresa de entrega para restaurantes, quer provisionar a capacidade do Amazon EC2 em todos os tipos de instâncias do EC2 e opções de compra para atingir a escala, a performance e o custo desejados.

Planejamento

A ABC Online requer uma capacidade fixa para operar durante períodos de pico, mas gostaria de se beneficiar do aumento da capacidade a um preço menor. A ABC Online determina os seguintes requisitos para suas Frota do EC2:

- Capacidade de instância sob demanda: a ABC Online requer 15 instâncias sob demanda para garantir a acomodação do tráfego em períodos de pico.
- Capacidade de instâncias spot: a ABC Online gostaria de aprimorar a performance, mas com preços mais baixos, com provisionamento de 5 instâncias spot.

Verificar permissões

Antes de criar uma Frota do EC2, a ABC Online verifica se ela tem uma função do IAM com as permissões necessárias. Para ter mais informações, consulte Pré-requisitos da Frota do EC2.

Criar um modelo de execução

A ABC Online cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para ter mais informações, consulte Criar um modelo de inicialização.

Criar a Frota do EC2

A ABC Online cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2. No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{
```

```
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A ABC Online cria a Frota do EC2 usando o seguinte comando create-fleet:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Para ter mais informações, consulte Criar uma Frota do EC2..

Atendimento

A estratégia de alocação determina que a capacidade sob demanda seja sempre cumprida, enquanto o saldo da capacidade de destino seja atendido como spot se houver capacidade e disponibilidade.

Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas

Este tutorial orienta você por todas as etapas que você deve executar para que sua Frota do EC2 inicie Instâncias sob demanda nas Reservas de Capacidade `targeted`.

Você aprenderá a configurar uma frota para usar as Reservas de Capacidade sob demanda `targeted` primeiro ao iniciar Instâncias sob demanda. Você também aprenderá a configurar a frota para que, quando a capacidade total de destino sob demanda exceder o número de Reservas de Capacidade não utilizadas disponíveis, a frota use a estratégia de alocação especificada para selecionar os grupos de instâncias nos quais iniciar a capacidade de destino restante.

Configuração da Frota do EC2

Nesse tutorial, a configuração da frota é a seguinte:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade `targeted` não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (`us-east-1a` e `us-east-1b`)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Para iniciar as Instâncias sob demanda em Reservas de Capacidade targeted, você deve executar uma série de etapas, da seguinte forma:

- Etapa 1: Criar Reservas de Capacidade
- Etapa 2: Criar um grupo de recursos de Reservas de capacidade
- Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade
- (Opcional) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos
- Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico
- (Opcional) Etapa 6: Descrever o modelo de inicialização
- Etapa 7: Criar uma Frota EC2
- (Opcional) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes

Etapa 1: Criar Reservas de Capacidade

Use o comando Create-capacity-reservation para criar as Reservas de Capacidade, três para `us-east-1a` e outras três para `us-east-1b`. Exceto para a Zona de disponibilidade, os outros atributos das Reservas de Capacidade são idênticos.

3 Reservas de Capacidade no **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-1234567890abcdef1
```

3 Reservas de Capacidade no **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-54321abcdef567890
```

Etapa 2: Criar um grupo de recursos de Reservas de capacidade

Use o serviço `resource-groups` e o comando create-group para criar um grupo de recursos de Reservas de capacidade. Neste exemplo, o grupo de recursos é chamado de `my-cr-group`. Para obter informações sobre por que você deve criar um grupo de recursos, consulte Use Reservas de Capacidade para Instâncias on-demand.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade

Use o serviço `resource-groups` e o comando group-resources para adicionar as Reservas de Capacidade que você criou na Etapa 1 para o grupo de recursos Reservas de Capacidade. Observe que você deve fazer referência às Reservas de Capacidade sob demanda por seus ARNs.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Exemplo de saída

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Opcional) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos

Use o serviço `resource-groups` e o comando list-group-resources para descrever opcionalmente o grupo de recursos para visualizar suas Reservas de Capacidade.

```
aws resource-groups list-group-resources --group my-cr-group
```

Exemplo de saída

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
```

```
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico

Use o comando create-launch-template para criar um modelo de execução no qual especifique as Reservas de Capacidade a serem usadas. Neste exemplo, a frota usará Reservas de Capacidade `targeted`, que foram adicionadas a um grupo de recursos. Portanto, os dados do modelo de inicialização especificam que a Reserva de Capacidade se destina a um grupo de recursos específico. Neste exemplo, o modelo de inicialização é chamado de `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Opcional) Etapa 6: Descrever o modelo de inicialização

Use o comando template describe-launch-template para descrever opcionalmente o modelo de lançamento para visualizar sua configuração.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Exemplo de saída

```
{
    "LaunchTemplateVersions": [
        {
```

```
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Etapa 7: Criar uma Frota EC2

Crie uma EC2 Fleet que especifique as informações de configuração para as instâncias que serão iniciadas. A configuração de frota EC2 a seguir mostra somente as configurações pertinentes a esse exemplo. O modelo de inicialização `my-launch-template` é o modelo de inicialização criado na Etapa 5. Há dois grupos de instâncias, cada um com o mesmo tipo de instância (`c5.xlarge`), mas com diferentes zonas de disponibilidade (`us-east-1a` e `us-east-1b`). O preço dos grupos de instâncias é o mesmo porque o preço é definido para a região, não para a Zona de Disponibilidade. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
```

```
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1a`
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1b`
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o

preço é por região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

(Opcional) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes

Depois que a frota for lançada, você poderá, opcionalmente, executar describe-capacity-reservations para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade foram usadas em todos os grupos.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial : iniciar instâncias em blocos de capacidade

Este tutorial mostra todas as etapas que você deve seguir para que a Frota do EC2 inicie Instâncias sob demanda em blocos de capacidade. Para obter mais informações sobre blocos de capacidade, consulte Blocos de capacidade para ML.

Você pode usar a Frota do EC2 do tipo instantânea para iniciar instâncias em blocos de capacidade. Para ter mais informações, consulte Usar uma EC2 Fleet do tipo 'instantâneo'.

Na maioria dos casos, a capacidade pretendida da solicitação de Frota do EC2 deve ser menor ou igual à capacidade disponível na reserva de bloco de capacidade pretendida. As solicitações de capacidade pretendida que excederem os limites da reserva de bloco de capacidade não serão atendidas. Se a solicitação de capacidade pretendida exceder os limites da reserva de bloco de capacidade, você receberá uma exceção de capacidade insuficiente para a capacidade que ultrapassar os limites da reserva de bloco de capacidade.

> **Note**
>
> Para blocos de capacidade, a Frota do EC2 não recorrerá à inicialização de instâncias sob demanda para atender ao restante da capacidade pretendida.

Se a Frota do EC2 não puder atender à capacidade pretendida solicitada em uma reserva de bloco de capacidade disponível, a Frota do EC2 atenderá ao máximo de capacidade possível e retornará as instâncias que não conseguiu iniciar. Você pode repetir a chamada para a Frota do EC2 até que todas as instâncias sejam provisionadas.

Depois de configurar a solicitação da Frota do EC2, você deve esperar até a data de início da reserva do bloco de capacidade. Se fizer solicitações à Frota do EC2 para iniciar um bloco de capacidade que ainda não foi iniciado, você receberá um erro de capacidade insuficiente.

Depois que a reserva de bloco de capacidade se tornar ativa, você poderá fazer chamadas à API da Frota do EC2 e provisionar as instâncias no bloco de capacidade segundo os parâmetros selecionados. As instâncias em execução no bloco de capacidade continuam em execução até que você as interrompa ou encerre por meio de uma outra chamada de API do Amazon EC2, ou que o Amazon EC2 encerre as instâncias quando a reserva do bloco de capacidade terminar.

Considerações

- Não é possível ter vários blocos de capacidade na mesma solicitação `CreateFleet`.
- Não é possível usar `OnDemandTargetCapacity` ou `SpotTargetCapacity` e, ao mesmo tempo, definir o `capacity-block` como `DefaultTargetCapacity`.
- Se o `DefaultTargetCapacityType` estiver definido como `capacity-block`, você não poderá fornecer `OnDemandOptions::CapacityReservationOptions`. Uma exceção ocorrerá.

Criar um modelo de inicialização

O ID do modelo de execução é usado na próxima etapa. Para ter mais informações, consulte Criar um modelo de inicialização.

Para configurar o modelo de inicialização, para `InstanceMarketOptionsRequest`, defina `MarketType` como `capacity-block`. Especifique o ID da reserva do bloco de capacidade pretendida, definindo o parâmetro `CapacityReservationID`.

Criar a Frota do EC2

Crie um arquivo, `config.json`, com a configuração de Frota do EC2 a seguir. No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

Use o comando create-fleet a seguir.

```
aws ec2 create-fleet \
     --cli-input-json file://config.json
```

Para ter mais informações, consulte Criar uma Frota do EC2..

Tutorial: Usar frota spot com ponderação de instâncias

Este tutorial usa uma empresa fictícia chamada Example Corp para ilustrar o processo de solicitação de uma frota spot usando o peso da instância.

Objetivo

A Exemplo Corp, uma empresa farmacêutica, quer impulsionar a capacidade computacional do Amazon EC2 para fazer a triagem dos compostos químicos que podem ser usados para combater o câncer.

Planejamento

Primeiro, a Exemplo Corp analisa as Melhores práticas de spot. Em seguida, a Exemplo Corp determina os seguintes requisitos para a frota spot.

Tipos de instância

A Exemplo Corp tem uma aplicação de uso intenso de memória e recursos de computação que funciona melhor com, pelo menos, 60 GB de memória e oito CPUs virtuais (vCPUs). Eles querem maximizar esses recursos para a aplicação com o menor preço possível. A Exemplo Corp decide que qualquer um dos seguintes tipos de instância do EC2 atenderá às suas necessidades:

Tipo de instância	Memória (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidade de destino em unidades

Com o peso da instância, a capacidade de destino pode igualar um número de instâncias (o padrão) ou uma combinação de fatores, como núcleos (vCPUs), memória (GiB) e armazenamento (GB). Considerando a base para sua aplicação (60 GB de RAM e oito vCPUs) como 1 unidade, a Exemplo Corp decide que 20 vezes essa quantidade atenderá às suas necessidades. Então, a empresa define a capacidade de destino da solicitação de frota spot como 20.

Pesos das instâncias

Depois de determinar a capacidade de destino, a Exemplo Corp calcula os pesos das instâncias. Para calcular o peso para cada tipo de instância, eles determinam as unidades de cada tipo de instância que são necessárias para atingir a capacidade de destino da seguinte forma:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 unidade de 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 unidades de 20

Portanto, a Exemplo Corp atribui os pesos de instância 1, 2 e 4 às respectivas configurações de execução na solicitação de frota spot.

Preço por hora

A Exemplo Corp usa o Preço sob demanda por hora de instância como o ponto inicial de preço. Eles também podem usar os preços spot recentes ou uma combinação dos dois. Para calcular o preço por hora, eles dividem o preço inicial por hora de instância pelo peso. Por exemplo:

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	$2,8	4	0,7 USD

A Exemplo Corp pode usar um preço global por hora de 0,7 USD e ser competitiva para todos os três tipos de instância. Eles também podem usar um preço global por hora de 0,7 USD e um preço específico por hora de 0,9 USD na especificação de execução `r3.8xlarge`.

Verificar permissões

Antes de criar uma solicitação de frota spot, a Exemplo Corp verifica se ela tem uma função do IAM com as permissões necessárias. Para ter mais informações, consulte Permissões de frota spot.

Criar a solicitação

A Exemplo Corp cria um arquivo, `config.json`, com a seguinte configuração para a solicitação da frota spot:

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
```

```
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 2
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.8xlarge",
      "SubnetId": "subnet-482e4972",
      "SpotPrice": "0.90",
      "WeightedCapacity": 4
    }
  ]
}
```

A Exemplo Corp cria a solicitação de frota spot usando o comando request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para ter mais informações, consulte Tipos de solicitação da frota spot.

Atendimento

A estratégia de alocação determina de quais grupos de capacidade spot os Instâncias spot procedem.

Com a estratégia `lowestPrice` (que é uma estratégia padrão), as Instâncias spot vêm do grupo com o menor preço spot por unidade no momento do atendimento. Para fornecer 20 unidades de capacidade, a frota spot executa 20 instâncias `r3.2xlarge` (20 dividido por 1), 10 instâncias `r3.4xlarge` (20 dividido por 2) ou 5 instâncias `r3.8xlarge` (20 dividido por 4).

Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A frota spot executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Exemplo de configurações para EC2 Fleet e frota spot

Os exemplos a seguir mostram configurações de execução que você pode usar para criar frotas do EC2 e frotas spot.

Tópicos

- Exemplos de configuração de Frota do EC2
- Exemplos de configuração de frota spot

Exemplos de configuração de Frota do EC2

Os exemplos a seguir mostram configurações de execução que você pode usar com o comando create-fleet para criar uma Frota do EC2. Para obter mais informações sobre os parâmetros, consulte create-fleet na Referência de comandos da AWS CLI.

Exemplos

- Exemplo 1: Executar Instâncias spot como a opção de compra padrão
- Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão
- Exemplo 3: Executar Instâncias on-demand como a capacidade principal
- Exemplo 4: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade
- Exemplo 5: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas
- Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas
- Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição
- Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade
- Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades
- Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade
- Exemplo 11: configurar a seleção de tipo de instância baseada em atributos

Exemplo 1: Executar Instâncias spot como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução

é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é `spot`. Isso faz com que a frota execute duas Instâncias spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é `on-demand`. Isso faz com que a frota execute duas Instâncias on-demand.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
```

```
}
```

Exemplo 3: Executar Instâncias on-demand como a capacidade principal

O exemplo a seguir especifica a capacidade total de destino de duas instâncias para a frota e uma capacidade de destino de uma instância sob demanda. A opção de compra padrão é `spot`. A frota executa uma instância sob demanda, conforme especificado, mas precisa executar mais uma instância para atender à capacidade total desejada. A opção de compra para a diferença é calculada como `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, o que resulta na frota executando uma instância spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemplo 4: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade

É possível configurar uma frota para usar Reservas de capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como a frota seleciona as Reservas de Capacidade a serem usadas quando há mais Reservas de Capacidade do que o necessário para atender à capacidade de destino.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 12 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (mais do que a capacidade de destino da frota de 12 Instâncias sob demanda)

- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando há várias Reservas de Capacidade não utilizadas em vários grupos de instâncias, a frota determina os grupos nos quais as Instâncias sob demanda serão iniciadas com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Reservas de capacidade

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
```

```
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 12 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- `m5.large` – 0,096 USD por hora
- `m4.xlarge` – 0,20 USD por hora
- `m4.2xlarge` – 0,40 USD por hora

> **Note**
>
> O tipo da frota deve ser do tipo `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
```

```
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 12 instâncias a seguir serão executadas para atender à capacidade de destino:

- 5 `m5.large` Instâncias sob demanda em `us-east-1a` – `m5.large` em `us-east-1a` é o preço mais baixo, e há 5 Reservas de Capacidade `m5.large` disponíveis não utilizadas
- 5 `m4.xlarge` Instâncias sob demanda em `m4.xlarge` – `us-east-1a` em us-east-1a é o próximo preço mais baixo, e há 5 Reservas de Capacidade `m4.xlarge` não utilizadas disponíveis
- 2 Instâncias sob demanda `m4.2xlarge` em us-east-1a – `m4.2xlarge` em `us-east-1a` é o terceiro preço mais baixo, e existem 5 Reservas de Capacidade `m4.2xlarge` não utilizadas disponíveis, das quais somente 2 são necessárias para atender à capacidade de destino

Depois que a frota for lançada, você poderá executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade `m5.large` e `m4.xlarge` foram usadas, com 3 Reservas de Capacidade `m4.2xlarge` restantes não utilizadas.

```
{
    "CapacityReservationId": "cr-111",
```

```
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Exemplo 5: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas

É possível configurar uma frota para usar Reservas de capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 16 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (menor que a capacidade de destino da frota de 16 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Reservas de capacidade

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 16 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- m5.large – 0,096 USD por hora
- m4.xlarge – 0,20 USD por hora
- m4.2xlarge – 0,40 USD por hora

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
```

```
            ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 16 instâncias a seguir serão executadas para atender à capacidade de destino:

- 6 Instâncias sob demanda `m5.large` em `us-east-1a` – `m5.large` em `us-east-1a` é o preço mais baixo, e há 5 Reservas de Capacidade `m5.large` disponíveis não utilizadas As Reservas de Capacidade são usadas primeiro para iniciar 5 Instâncias sob demanda. Depois das Reservas de Capacidade `m4.xlarge` e `m4.2xlarge` restantes serem usadas, para atender à capacidade de destino, uma instância sob demanda adicional é iniciada, de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo.
- 5 `m4.xlarge` Instâncias sob demanda em `us-east-1a` – `m4.xlarge` em `us-east-1a` é o próximo preço mais baixo, e há 5 Reservas de Capacidade `m4.xlarge` disponíveis não utilizadas
- 5 `m4.2xlarge` Instâncias sob demanda em `us-east-1a` – `m4.2xlarge` em `us-east-1a` é o terceiro preço mais baixo, e há 5 Reservas de Capacidade `m4.2xlarge` disponíveis não utilizadas

Depois que a frota for lançada, você poderá executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de capacidade foram usadas em todos os grupos.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas

É possível configurar uma frota para usar Reservas de Capacidade `targeted` sob demanda primeiro ao iniciar Instâncias sob demanda definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como iniciar Instâncias sob demanda nas Reservas de Capacidade `targeted`, com os atributos das Reservas de Capacidade sendo os mesmos, exceto para suas Zonas de Disponibilidade (`us-east-1a` e `us-east-1b`). Ele também demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade `targeted` não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (`us-east-1a` e `us-east-1b`)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Para obter uma demonstração dos procedimentos que você deve executar para realizar este exemplo, consulte Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas.

Reservas de capacidade

A conta tem as 6 Reservas de Capacidade não utilizadas a seguir em 2 grupos diferentes. Neste exemplo, os grupos diferem de acordo com suas Zonas de disponibilidade. O número de Reservas de capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda para `c5.xlarge` em `us-east-1` é 0,17 USD por hora.

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1a`
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1b`
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o preço é por região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

Depois que a frota for lançada, você poderá executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de capacidade foram usadas em todos os grupos.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a EC2 Fleet para executar uma Instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma Instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar o tempo de espera entre o lançamento das novas instâncias spot substitutas até a exclusão automática das instâncias spot antigas, para `termination-delay`, especifique um valor em segundos. Para ter mais informações, consulte Opções de configuração.

> **Note**
>
> Recomendamos só usar `launch-before-terminate` se você puder prever quanto tempo os procedimentos de desligamento da instância levarão, de modo que as instâncias antigas só sejam terminadas após a conclusão desses procedimentos. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de Frota do EC2. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy`especifique `capacity-optimized`. Para obter mais informações sobre o que você deve considerar ao configurar uma Frota do EC2 para rebalanceamento de capacidade, consulte Rebalanceamento de capacidade.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
```

```
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                            }
                        }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que otimiza a capacidade. Para otimizar a capacidade, você deve definir `AllocationStrategy` como `capacity-optimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
```

```
                    {
                        "InstanceType": "r4.2xlarge",
                        "Placement": {
                            "AvailabilityZone": "us-west-2a"
                        },
                    },
                    {
                        "InstanceType": "m4.2xlarge",
                        "Placement": {
                            "AvailabilityZone": "us-west-2b"
                        },
                    },
                    {
                        "InstanceType": "c5.2xlarge",
                        "Placement": {
                            "AvailabilityZone": "us-west-2b"
                        }
                    }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que otimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacity-optimized-prioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecê-los igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacity-optimized-prioritized`. A EC2 Fleet otimizará a capacidade primeiro, mas

se empenhará em honrar as prioridades (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da EC2 Fleet de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas otimiza a capacidade em primeiro lugar.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Priority": 2,
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Priority": 3,
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
```

```
                    }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade

O exemplo a seguir demonstra como configurar uma Frota EC2 com uma estratégia de alocação spot que otimize tanto para capacidade quanto por menor preço. Para otimizar para capacidade e levar em consideração o preço, você deve definir a `AllocationStrategy` de spot como `price-capacity-optimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota do EC2 tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas e, ao mesmo tempo, escolher o grupo com menor preço.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
```

```
                    },
                     {
                         "InstanceType": "m4.2xlarge",
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         },
                     },
                     {
                         "InstanceType": "c5.2xlarge",
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         }
                     }
                ]
            }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 11: configurar a seleção de tipo de instância baseada em atributos

O exemplo a seguir demonstra como configurar uma Frota do EC2 para usar a seleção de tipo de instância baseada em atributos para identificar tipos de instância. Para especificar os atributos de instância necessários, especifique os atributos na estrutura `InstanceRequirements`.

No exemplo a seguir, dois atributos de instância são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a Frota do EC2 provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Exemplos de configuração de frota spot

Os exemplos a seguir mostram configurações de execução que você pode usar com o comando request-spot-fleet para criar uma solicitação de frota spot. Para ter mais informações, consulte Criar uma solicitação de frota spot.

> **Note**
>
> Em frota spot, não é possível especificar um ID de interface de rede em uma especificação de execução. Omita o parâmetro `NetworkInterfaceID` no modelo ou na especificação de execução.

Exemplos

- Exemplo 1: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço da região
- Exemplo 2: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada
- Exemplo 3: executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada
- Exemplo 4. Cancelar o preço da solicitação
- Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada
- Exemplo 6: executar uma frota spot usando o peso da instância
- Exemplo 7: executar uma frota spot com capacidade sob demanda
- Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição
- Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade
- Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades
- Exemplo 11: iniciar instâncias spot em uma frota priceCapacityOptimized
- Exemplo 12: configurar a seleção de tipo de instância baseada em atributos

Exemplo 1: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço da região

O exemplo a seguir determina uma única especificação de execução sem uma zona de disponibilidade nem sub-rede. A frota spot executa as instâncias na zona de disponibilidade de menor preço que tem uma sub-rede padrão. O preço que você paga não excede o preço sob demanda.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "m3.medium",
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ]
}
```

Exemplo 2: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada

Os exemplos a seguir determinam duas especificações de execução com zonas de disponibilidade ou sub-redes diferentes, mas o mesmo tipo de instância e AMI.

Zonas de disponibilidade

A frota spot executa as instâncias na sub-rede padrão da zona de disponibilidade de menor preço especificada.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "m3.medium",
        "Placement": {
            "AvailabilityZone": "us-west-2a, us-west-2b"
        },
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
```

```
  ]
}
```

Subredes

Você pode especificar sub-redes padrão ou não padrão, e as sub-rede não padrão podem ser de uma VPC padrão ou não padrão. O serviço spot executa as instâncias em qualquer sub-rede na zona de disponibilidade de menor preço.

Você não pode especificar sub-redes diferentes da mesma zona de disponibilidade em uma solicitação de frota spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Se as instâncias forem executadas em uma VPC padrão, elas receberão um endereço IPv4 público por padrão. Se as instâncias forem executadas em uma VPC não padrão, elas não receberão um endereço IPv4 público por padrão. Use uma interface de rede na especificação de execução para atribuir um endereço IPv4 público às instâncias executadas em uma VPC não padrão. Ao especificar uma interface de rede, você deve incluir o ID da sub-rede e o ID do grupo de segurança usando a interface de rede.

```
  ...
```

```
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "InstanceType": "m3.medium",
        "NetworkInterfaces": [
            {
                "DeviceIndex": 0,
                "SubnetId": "subnet-1a2b3c4d",
                "Groups": [ "sg-1a2b3c4d" ],
                "AssociatePublicIpAddress": true
            }
        ],
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
        }
    }
...
```

Exemplo 3: executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada

Os exemplos a seguir determinam duas configurações de execução com tipos de instância diferentes, mas a mesma AMI e zona de disponibilidade ou sub-rede. A frota spot executa as instâncias spot usando o tipo de instância de menor preço especificado.

Zona de disponibilidade

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
        "ImageId": "ami-1a2b3c4d",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "c5.4xlarge",
        "Placement": {
          "AvailabilityZone": "us-west-2b"
        }
    },
```

```
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Sub-rede

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Exemplo 4. Cancelar o preço da solicitação

Recomendamos que você use o preço máximo padrão, que é o preço sob demanda. Se você preferir, poderá especificar um preço máximo para a solicitação da frota e os preços máximos para as especificações de execução individuais.

Os seguintes exemplos especificam um preço máximo para a solicitação da frota e preços máximos para duas das três especificações de execução. O preço máximo da solicitação da frota é utilizado para qualquer especificação de execução que não especifique um preço máximo. A frota spot executa as instâncias spot usando o tipo de instância de menor preço.

Zona de disponibilidade

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
```

```
}
```

Sub-rede

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada

O exemplo a seguir usa a estratégia de alocação `diversified`. As especificações de execução têm tipos de instância diferentes, mas a mesma AMI e zona de disponibilidade ou sub-rede. A frota spot distribui as 30 instâncias pelas três especificações de execução, de modo que haja 10 instâncias de cada tipo. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.

Zona de disponibilidade

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
```

```
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Sub-rede

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Para aumentar a chance de que uma solicitação spot possa ser atendida pela capacidade do EC2 no caso de uma interrupção em uma das zonas de disponibilidade, uma prática recomendada é diversificar entre zonas. Nesse cenário, inclua cada zona de disponibilidade possível para você na especificação de execução. E, em vez de usar sempre a mesma sub-rede, use três sub-redes exclusivas (cada mapeamento para uma zona de disponibilidade diferente).

Zona de disponibilidade

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
```

```
            }
        }
    ]
}
```

Sub-rede

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Exemplo 6: executar uma frota spot usando o peso da instância

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância e um peso diferentes. A frota spot seleciona o tipo de instância com o menor preço por hora de unidade. A frota spot calcula o número de instâncias spot a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota spot o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino.

Se a solicitação `r3.2xlarge` for feita com êxito, o spot provisionará 4 dessas instâncias. Divida 20 por 6 para um total de 3,33 instâncias, em seguida, arredonde para 4 instâncias.

Se a solicitação `c3.xlarge` for feita com êxito, o spot provisionará 7 dessas instâncias. Divida 20 por 3 para um total de 6,66 instâncias, em seguida, arredonde para 7 instâncias.

Para ter mais informações, consulte Peso de instâncias de frotas spot.

Zona de disponibilidade

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Sub-rede

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
```

```
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Exemplo 7: executar uma frota spot com capacidade sob demanda

Para garantir que você sempre tenha capacidade de instância, você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot. Se houver capacidade, a solicitação de sob demanda sempre será atendida. O equilíbrio da capacidade de destino será atendido como Spot se houver capacidade e disponibilidade.

O exemplo a seguir especifica a capacidade desejada de destino como 10, da qual 5 deve ser sob demanda. A capacidade spot não é especificada. Ela está implícita no saldo da capacidade pretendida menos a capacidade sob demanda. O Amazon EC2 executará cinco unidades de capacidade como sob demanda e cinco unidades de capacidade (10-5=5) como spot se houver disponibilidade e capacidade do Amazon EC2 disponíveis.

Para ter mais informações, consulte Sob demanda na frota spot.

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
```

```
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a frota spot para executar uma instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar o tempo de espera entre o lançamento das novas instâncias spot substitutas até a exclusão automática das instâncias spot antigas, para `termination-delay`, especifique um valor em segundos. Para ter mais informações, consulte Opções de configuração.

> **Note**
>
> Recomendamos só usar `launch-before-terminate` se você puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garante que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de frota spot. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy`especifique `capacityOptimized`. Para obter mais informações sobre o que você deve considerar ao configurar uma frota spot para rebalanceamento de capacidade, consulte Rebalanceamento de capacidade.

```
{
    "SpotFleetRequestConfig": {
```

```
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimiza a capacidade. Para otimizar a capacidade, você deve definir `AllocationStrategy` como `capacityOptimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       }
                ]
          }
      ]
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacityOptimizedPrioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecê-los igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacityOptimizedPrioritized`. A frota spot otimizará a capacidade em primeiro lugar, mas honrará as prioridades com o melhor esforço (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da frota spot de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas otimiza a capacidade em primeiro lugar.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
             "Overrides": [
                    {
                       "InstanceType": "r4.2xlarge",
                       "Priority": 1,
                       "AvailabilityZone": "us-west-2a"
```

```
                    },
                     {
                         "InstanceType": "m4.2xlarge",
                         "Priority": 2,
                         "AvailabilityZone": "us-west-2b"
                     },
                     {
                         "InstanceType": "c5.2xlarge",
                         "Priority": 3,
                         "AvailabilityZone": "us-west-2b"
                     }
                ]
            }
       ]
}
```

Exemplo 11: iniciar instâncias spot em uma frota priceCapacityOptimized

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimize tanto para capacidade quanto para o menor preço. Para otimizar para capacidade e levar em consideração o preço, você deve definir a `AllocationStrategy` de spot como `priceCapacityOptimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas e ao mesmo tempo, escolher o grupo com menor preço.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
```

```
                    {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                     },
                     {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     },
                     {
                          "InstanceType": "c5.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Exemplo 12: configurar a seleção de tipo de instância baseada em atributos

O exemplo a seguir demonstra como configurar uma frota spot para usar a seleção de tipo de instância baseada em atributos para identificar tipos de instância. Para especificar os atributos de instância necessários, especifique os atributos na estrutura `InstanceRequirements`.

No exemplo a seguir, dois atributos de instância são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a frota spot provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

```
{
```

```
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Quotas da frota

As cotas normais do Amazon EC2 (antes chamadas de limites) se aplicam a instâncias iniciadas por uma frota do EC2 ou uma frota spot, como limites de instância spot e limites de volume.

Além disso, as cotas a seguir são aplicáveis:

Descrição da cota	Quota
O número de frotas do EC2 e frotas spot por região dos tipos `maintain` e `request` nos estados `active`, `deleted_running` e `cancelled_running`	1.000 [1] [2] [3]
O número de frotas EC2 do tipo `instant`	Ilimitado
O número de grupos de capacidade spot (combinação exclusiva de tipo de instância e	300 [1]

Descrição da cota	Quota
sub-rede) para frotas do EC2 e frotas spot dos tipos `maintain` e `request`	
O número de grupos de capacidade spot (combinação exclusiva de tipo de instância e sub-rede) para frotas do EC2 do tipo `instant`	Ilimitado
O tamanho dos dados de usuário em uma especificação de inicialização	16 KB [2]
A capacidade pretendida por frota do EC2 ou frota spot	10.000
A capacidade de destino em todas as frotas do EC2 e frotas spot de uma região	100.000 [1]
Uma solicitação de EC2 Fleet ou de frota spot não pode abranger regiões.	
Uma solicitação de EC2 Fleet ou de frota spot não pode abranger sub-redes diferentes na mesma zona de disponibilidade.	

[1] Essas cotas aplicam-se a frotas do EC2 e frotas spot.

[2] Estas são cotas fixas. Não é possível solicitar o aumento dessas cotas.

[3] Depois de excluir uma frota do EC2 ou cancelar uma solicitação de frota spot, e se você especificou que a frota não deverá terminar suas instâncias spot quando excluiu ou cancelou a solicitação, a solicitação de frota inserirá o estado `deleted_running` (frota do EC2) ou `cancelled_running` (frota spot). As instâncias continuarão em execução até que sejam interrompidas ou terminadas manualmente. Se você terminar as instâncias, a solicitação de frota entrará no estado `deleted_terminating` (frota do EC2) ou `cancelled_terminating` (frota spot) e não contará para essa cota. Para ter mais informações, consulte Excluir uma Frota do EC2 e Cancelar uma solicitação de frota spot.

Solicitar um aumento de cota para a capacidade pretendida

Se precisar exceder a cota padrão da capacidade de destino, solicite um aumento de cota.

Como solicitar um aumento de cota para a capacidade pretendida

1. Abra o formulário Create case (Criar caso) no AWS Support Center.
2. Escolha Service limit increase (Aumento de limite do serviço).
3. Em Limit type (Tipo de limite), escolha EC2 Fleet (Frota do EC2).
4. Em Region (Região), escolha a região da AWS na qual solicitar o aumento da cota.
5. Em Limit (Limite), escolha Target Fleet Capacity per Fleet (in units) (Capacidade da frota de destino por frota [em unidades]) ou Target Fleet Capacity per Region (in units) (Capacidade da frota de destino por região [em unidades]), dependendo da cota que deseja aumentar.
6. Em New limit value (Novo valor de limite), insira o novo valor.
7. Para solicitar um aumento para outra cota, escolha Add another request (Adicionar outra solicitação) e repita as etapas de 4 a 6.
8. Em Use case description (Descrição do caso de uso), insira o motivo para solicitar um aumento de cota.
9. Em Contact options (Opções de contato), especifique o idioma de contato e o método de contato de sua preferência.
10. Selecione Enviar.

Monitorar o Amazon EC2

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e de outras soluções da AWS. É necessário coletar dados de monitoramento de todas as partes de suas soluções da AWS para facilitar a depuração de uma falha de vários pontos (caso ocorra). No entanto, antes de iniciar o monitoramento do Amazon EC2, crie um plano de monitoramento que deverá incluir:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Depois de definir seus objetivos de monitoramento e criar seu plano de monitoramento, a próxima etapa é estabelecer uma linha de base para a performance normal do Amazon EC2 em seu ambiente. É necessário medir a performance do Amazon EC2 em vários momentos e em condições diferentes de carga. Ao monitorar o Amazon EC2, é necessário armazenar um histórico dos dados de monitoramento que você reúne. Será possível comparar a performance atual do Amazon EC2 com esses dados históricos para ajudá-lo a identificar padrões de performance normais e anomalias de performance, e elaborar métodos para resolvê-los. Por exemplo, é possível monitorar a utilização da CPU, a E/S de disco e a utilização da rede para suas instâncias do EC2. Quando a performance estiver fora da linha de base estabelecida, talvez seja necessário reconfigurar ou otimizar a instância para reduzir a utilização da CPU, melhorar a E/S de disco ou reduzir o tráfego de rede.

Para estabelecer uma linha de base, é preciso, no mínimo, monitorar os seguintes itens:

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/CloudWatch Logs
Utilização da CPU	CPUUtilization	
Utilização da rede	NetworkIn	

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/CloudWatch Logs
	NetworkOut	
Performance do disco	DiskReadOps DiskWriteOps	
Leituras/gravações de disco	DiskReadBytes DiskWriteBytes	
Utilização de memória, utilização de troca de disco, utilização de espaço em disco, utilização de arquivo de páginas, coleção de logs		[Instâncias do Linux e Windows Server] Colecionar métricas e logs das instâncias do Amazon EC2 e servidores on-premises com o agente do CloudWatch [Migração de agentes anteriores do CloudWatch Logs em instâncias do Windows Server] Migrar coleção de logs da instância do Windows Server para o agente do CloudWatch

Monitoramento automático e manual

A AWS fornece várias ferramentas que é possível usar para monitorar o Amazon EC2. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual.

Ferramentas de monitoramento

- Ferramentas de monitoramento automatizadas
- Ferramentas de monitoramento manual

Ferramentas de monitoramento automatizadas

Use as seguintes ferramentas de monitoramento automatizadas para observar o Amazon EC2 e gerar relatórios quando algo estiver errado:

- System status checks (Verificações do status do sistema): monitore os sistemas da AWS necessários para usar a instância a fim de garantir que eles estejam funcionando corretamente. Essas verificações detectam problemas com sua instância que exigem a participação da AWS para corrigi-los. Quando ocorre uma falha em uma verificação de status do sistema, é possível optar por esperar a AWS corrigir o problema ou resolvê-lo por conta própria (por exemplo, interrompendo e reiniciando ou encerrando e substituindo uma instância). Exemplos de problemas que causam falha nas verificações de status do sistema incluem:
  - Perda de conectividade de rede
  - Perda de energia do sistema
  - Problemas de software no host físico
  - Problemas de hardware de host físico que afetam a acessibilidade de rede

  Para obter mais informações, consulte Verificações de status para as instâncias.
- Verificações do status da instância: monitore o software e a configuração de rede da instância individual. Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando ocorre uma falha em uma verificação de status da instância, normalmente, você precisará resolver o problema por conta própria (por exemplo, reinicializando a instância ou fazendo modificações no sistema operacional). Exemplos de problemas que podem causar falha nas verificações de status da instância incluem:
  - Verificações de status de sistema com falha
  - Configuração incorreta do startup ou da rede
  - Memória exaurida
  - Sistema de arquivos corrompido
  - Kernel incompatível

  Para obter mais informações, consulte Verificações de status para as instâncias.
- Alarmes do Amazon CloudWatch: observe uma única métrica ao longo de um período que você especificar e realize uma ou mais ações com base no valor da métrica em relação a determinado limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou por uma política do Amazon EC2 Auto Scaling. Os

alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocarão ações simplesmente porque estão em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.

- Amazon EventBridge: automatize os produtos da AWS e responde automaticamente a eventos do sistema. Os eventos dos produtos da AWS são entregues ao EventBridge em tempo quase real, e é possível especificar ações automáticas a serem executadas quando um evento corresponde a uma regra elaborada por você. Para obter mais informações, consulte O que é o Amazon EventBridge?.
- Amazon CloudWatch Logs: monitore, armazene e acesse os arquivos de log de instâncias do Amazon EC2, do AWS CloudTrail ou de outras origens. Para obter mais informações, consulte o Amazon CloudWatch Logs User Guide (Manual do usuário do Amazon CloudWatch Logs).
- Agente do CloudWatch: colete logs e métricas no nível do sistema de hosts e convidados nas instâncias do EC2 e nos servidores on-premises. Para obter mais informações, consulte Coletar métricas e logs de instâncias do Amazon EC2 e de servidores on-premises com o agente do CloudWatch no Guia do usuário do Amazon CloudWatch.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento do Amazon EC2 envolve o monitoramento manual desses itens que os scripts de monitoramento, verificações de status e alarmes do CloudWatch não abrangem. Os painéis do console do Amazon EC2 e do CloudWatch fornecem uma visão rápida do estado do ambiente do Amazon EC2.

- O painel do Amazon EC2 mostra:
  - Eventos de integridade e programados por região
  - Estado da instância
  - Verificações do status
  - Status do alarme
  - Detalhes da métrica da instância (no painel de navegação, escolha Instances (Instâncias), selecione uma instância e escolha a guia Monitoring (Monitoramento))
  - Detalhes da métrica de volume (no painel de navegação, escolha Volumes, selecione um volume e escolha a guia Monitoring (Monitoramento))
- O painel do Amazon CloudWatch mostra:

- Alertas e status atual
- Gráficos de alertas e recursos
- Estado de integridade do serviço

Além disso, é possível usar o CloudWatch para fazer o seguinte:

- Colocar em gráfico dados de monitoramento do Amazon EC2 para solucionar problemas e descobrir tendências
- Pesquisar e procurar todas as métricas de recursos da AWS
- Criar e editar alarmes para ser notificado sobre problemas
- Consulte as visões gerais rápidas dos alarmes e recursos da AWS

Melhores práticas de monitoramento

Use as melhores práticas de monitoramento a seguir para ajudá-lo com suas tarefas de monitoramento do Amazon EC2.

- Faça o monitoramento de uma prioridade para gerenciar problemas pequenos antes que eles se tornem grandes.
- Crie e implemente um plano de monitoramento que colete dados de monitoramento de todas as partes da solução da AWS para facilitar a depuração de uma falha de vários pontos (caso ocorra). Seu plano de monitoramento deve tratar, pelo menos, as seguintes questões:
  - Quais são seus objetivos de monitoramento?
  - Quais recursos você vai monitorar?
  - Com que frequência você vai monitorar esses recursos?
  - Quais ferramentas de monitoramento você usará?
  - Quem realizará o monitoramento das tarefas?
  - Quem deve ser notificado quando algo der errado?
- Automatize tarefas de monitoramento o máximo possível.
- Verifique os arquivos de log em suas instâncias do EC2.

Monitorar o status das instâncias

É possível monitorar o status de suas instâncias visualizando as verificações de status e os eventos programados para elas.

A verificação de status fornece as informações resultantes de verificações automáticas executadas pelo Amazon EC2. Essas verificações automáticas detectam se problemas específicos estão afetando as instâncias. As informações de verificação de status, em conjunto com os dados fornecidos pelo Amazon CloudWatch, oferecem visibilidade operacional detalhada sobre cada uma das instâncias.

Também é possível ver o status de eventos específicos programados para suas instâncias. O status de eventos fornece informações sobre as próximas atividades que estão programadas para suas instâncias, como reinicialização ou desativação. Ele também fornece os horários de início e término programados para cada evento.

Tópicos

- Verificações de status para as instâncias
- Eventos de alteração de estado das instâncias
- Eventos programados para instâncias

Verificações de status para as instâncias

Com o monitoramento de status de instâncias, por exemplo, é possível determinar rapidamente se o Amazon EC2 detectou problemas que possam impedir que as instâncias executem aplicações. O Amazon EC2 executa verificações automáticas em cada instância do EC2 em execução para identificar problemas de hardware e software. É possível visualizar os resultados dessas verificações de status para identificar problemas específicos e detectáveis. O status do evento expande as informações que o Amazon EC2 já fornece sobre o estado de cada instância (como `pending`, `running`, `stopping`) e as métricas de utilização que o Amazon CloudWatch monitora (utilização de CPU, tráfego de rede e atividade de disco).

As verificações de status são realizadas a cada minuto e elas retornam o status de aprovação e reprovação. Se todas as verificações forem aprovadas, o status geral da instância será OK. Se uma ou mais verificações falharem, o status geral será impaired. As verificações de status são integradas ao Amazon EC2, portanto elas não podem ser desabilitadas ou excluídas.

Quando uma verificação de status falha, a métrica do CloudWatch correspondente para as verificações de status é incrementada. Para obter mais informações, consulte Métricas de verificação de status. É possível usar essas métricas para criar alarmes do CloudWatch que são acionados com base no resultado das verificações de status. Por exemplo, é possível criar um alarme para avisá-lo se as verificações de status falharem em uma instância específica. Para obter mais informações, consulte Criar e editar alarmes de verificação de status.

Também é possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e recupere automaticamente a instância se ela for danificada devido a um problema subjacente. Para obter mais informações, consulte Resiliência de instância.

Tópicos

- Tipos de verificações de status
- Como trabalhar com verificações de status

Tipos de verificações de status

Existem três tipos de verificação de status.

- Verificações de status de sistema
- Verificações de status de instâncias
- Verificações de status do EBS anexado

Verificações de status de sistema

As verificações de status do sistema monitoram os sistemas da AWS nos quais a instância é executada. Essas verificações detectam problemas subjacentes na instância que exigem o envolvimento da AWS para a correção. Quando uma verificação de status do sistema falha, é possível esperar que a AWS corrija o problema ou pode corrigi-lo por conta própria. Para instâncias baseadas no Amazon EBS, é possível interrompê-las e iniciá-las por conta própria, o que, na maioria dos casos, faz com que a instância seja migrada para um novo host. Para instâncias do Linux com armazenamento de instância, é possível encerrar e substituir a instância. Para instâncias do Windows, o volume raiz deve ser um volume do Amazon EBS. O armazenamento de instâncias não é compatível com o volume raiz. Observe que os volumes de armazenamento de instâncias são efêmeros e todos os dados são perdidos quando a instância é interrompida.

A seguir, temos exemplos de problemas que podem causar falha nas verificações de status do sistema:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

Se uma verificação de status do sistema falhar, incrementamos a métrica StatusCheckFailed_System.

Instâncias bare metal

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status do sistema poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status do sistema deve retornar um status de aprovação.

Verificações de status de instâncias

Verificações do status da instância monitore o software e a configuração de rede da instância individual. O Amazon EC2 verifica a integridade da instância enviando uma solicitação de protocolo de resolução de endereço (ARP) para a interface de rede (NIC). Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando uma verificação de status de instância falha, geralmente você precisa lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância).

> **Note**
>
> As distribuições recentes do Linux que usam `systemd-networkd` para a configuração de rede podem relatar verificações de integridade de maneira diferente das distribuições anteriores. Durante o processo de inicialização, esse tipo de rede pode começar mais cedo e possivelmente terminar antes de outras tarefas de inicialização que também podem afetar a integridade da instância. As verificações de status que dependem da disponibilidade da rede podem relatar um status íntegro antes da conclusão de outras tarefas.

A seguir, temos exemplos de problemas que podem causar falhas nas verificações de status da instância:

- Verificações de status de sistema com falha
- Configuração incorreta de redes ou startup
- Memória exaurida
- Sistema de arquivos corrompido
- Kernel incompatível
- [Instâncias do Windows] Durante a reinicialização da instância ou enquanto uma instância baseada no armazenamento de instância do Windows está sendo empacotada, uma verificação de status da instância relata uma falha até que a instância fique disponível novamente.

Se uma verificação de status da instância falhar, incrementamos a métrica StatusCheckFailed_Instance.

Instâncias bare metal

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status da instância poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status dela deve retornar um status de aprovação.

Verificações de status do EBS anexado

As verificações de status do EBS anexado monitoram se os volumes do Amazon EBS anexados a uma instância estão acessíveis e são capazes de concluir operações de E/S. A métrica `StatusCheckFailed_AttachedEBS` é um valor binário que indica deficiência caso um ou mais dos volumes do EBS anexados à instância não sejam capazes de concluir operações de E/S. Essas verificações de status detectam problemas subjacentes com a computação ou a infraestrutura do Amazon EBS. Se ocorrer uma falha na métrica de verificação de status do EBS anexado, você pode esperar a AWS resolver o problema ou tomar medidas, como substituir os volumes afetados ou interromper e reiniciar a instância.

Veja abaixo alguns exemplos de problemas que podem causar falha nas verificações de status do EBS anexado:

- Problemas de hardware ou software nos subsistemas de armazenamento subjacentes aos volumes do EBS
- Problemas de hardware no host físico que afetam a acessibilidade dos volumes do EBS
- Problemas de conectividade entre a instância e os volumes do EBS

Você pode usar a métrica `StatusCheckFailed_AttachedEBS` para ajudar a melhorar a resiliência da sua workload. É possível usar essa métrica para criar alarmes do Amazon CloudWatch que são acionados com base no resultado das verificações de status. Por exemplo, você pode fazer o failover para uma instância secundária ou zona de disponibilidade ao detectar um impacto prolongado. Também é possível monitorar a performance de E/S de cada volume anexado usando as métricas do EBS CloudWatch para detectar e substituir o volume danificado. Se sua workload não estiver direcionando a E/S para nenhum dos volumes do EBS anexados à sua instância e a verificação de status do EBS anexado indicar uma deficiência, você pode interromper a instância e iniciá-la para resolver problemas com o host físico que estiverem afetando a acessibilidade dos volumes do EBS. Para obter mais informações, consulte Métricas de uso do Amazon CloudWatch para o Amazon EBS

> **Note**
>
> - A métrica de verificação de status do EBS anexado está disponível somente para instâncias do Nitro.
> - Você pode monitorar a métrica de verificação de status do EBS anexado criando um alarme do CloudWatch com base na métrica `StatusCheckFailed_AttachedEBS`. Não é possível visualizar essa verificação de status usando o comando describe-instance-status da AWS CLI.

Como trabalhar com verificações de status

Você pode trabalhar com verificações de status usando o console e as ferramentas de linha de comando, como a AWS CLI.

Tópicos

- Visualizar verificações de status
- Criar e editar alarmes de verificação de status

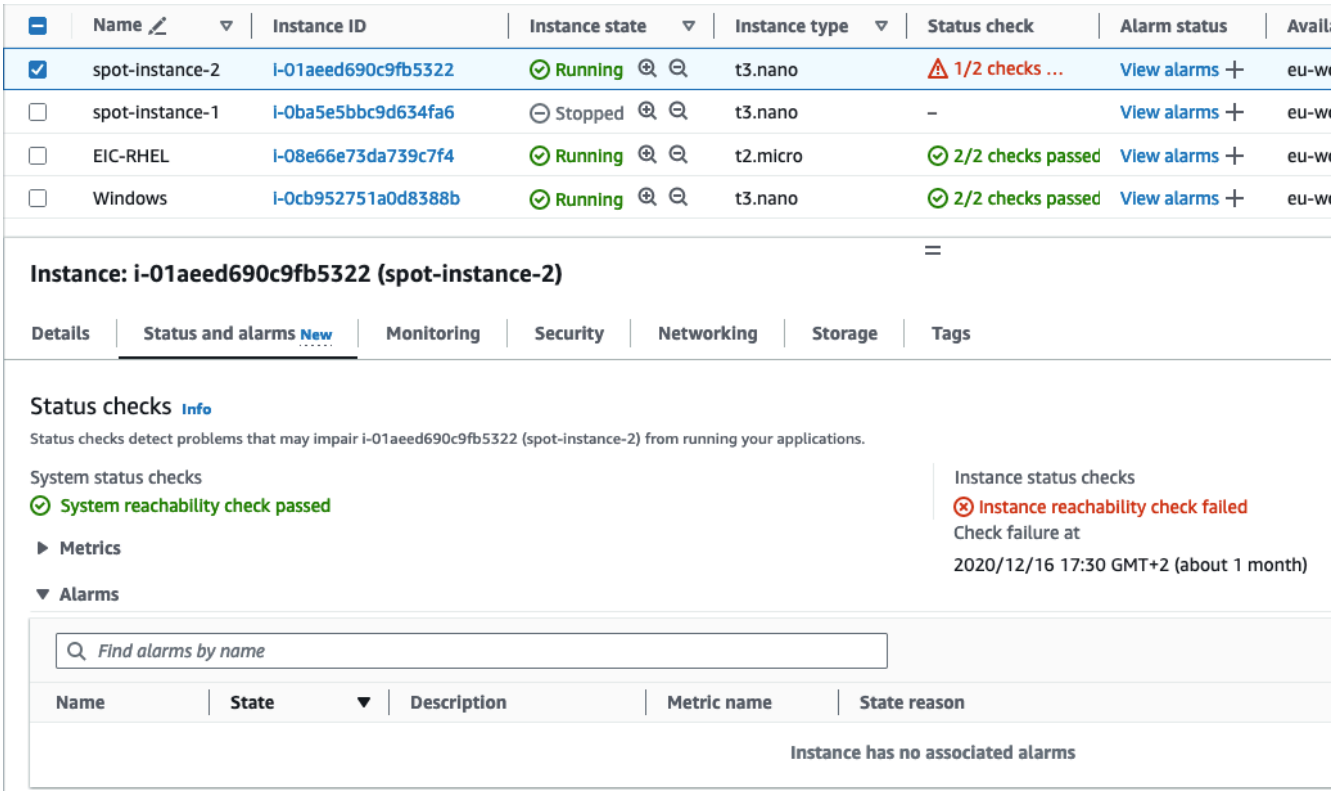
Visualizar verificações de status

Para ver as verificações de status, use um dos métodos a seguir.

Console

Para visualizar verificações de status

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na página Instances (Instâncias), a coluna Status check (Verificações de status) lista o status operacional de cada instância.
4. Para visualizar o status de uma instância específica, selecione a instância e escolha a guia Status e alarmes.



Se a verificação de status da instância falhar, você normalmente precisará lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância). Para solucionar problemas de falhas na verificação de status do sistema ou da instância em instâncias do Linux, consulte Solução de problemas de instâncias do Linux com falhas nas verificações de status.

5. Para revisar as métricas do CloudWatch para verificações de status, na guia Status e alarmes, expanda Métricas e veja os gráficos das seguintes métricas:

   - Falha na verificação de status do sistema

- Falha na verificação de status da instância

Para ter mais informações, consulte the section called “Métricas de verificação de status”.

Command line

É possível visualizar as verificações de status de instâncias em execução usando o comando describe-instance-status (AWS CLI).

Para visualizar o status de todas as instâncias, use o comando a seguir.

```
aws ec2 describe-instance-status
```

Para obter o status de todas as instâncias com um status de `impaired`, use o comando a seguir.

```
aws ec2 describe-instance-status \
    --filters Name=instance-status.status,Values=impaired
```

Para obter o status de uma única instância, use o comando a seguir.

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

Como alternativa, use os seguintes comandos do :

- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)
- DescribeInstanceStatus (API de consulta do Amazon EC2)

Se você tiver uma instância do Linux com falha na verificação de status, consulte Solução de problemas de instâncias do Linux com falhas nas verificações de status.

Criar e editar alarmes de verificação de status

É possível usar as métricas de verificação de status para criar alarmes do CloudWatch a fim de notificar você quando uma instância apresentou falha na verificação de status.

> **Important**
>
> As verificações de status e os alarmes de verificação de status podem entrar temporariamente em um estado de dados insuficiente se faltarem pontos de dados métricos. Embora raro, isso pode acontecer quando há uma interrupção nos sistemas de relatórios de métricas, mesmo quando uma instância está íntegra. Recomendamos que você trate esse estado como dados ausentes em vez de uma falha na verificação de status ou violação de alarme, especialmente ao executar ações de interrupção, encerramento, reinicialização ou recuperação na instância em resposta.

Para criar um alarme de verificação de status, use um dos seguintes métodos:

Console

Use o procedimento a seguir para configurar um alarme que envia uma notificação por e-mail ou que interrompe, encerra ou recupera uma instância quando ela apresenta falha em uma verificação de status.

Para criar um alarme de verificação de status (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status) e selecione Actions (Ações), Create status check alarm (Criar alarme de verificação de status).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar um alarme).
5. Em Alarm notification (Notificação de alarme), ative a opção para configurar notificações do Amazon Simple Notification Service (Amazon SNS). Selecione um tópico existente do Amazon SNS ou insira um nome para criar um tópico.

   Se você tiver adicionado um endereço de e-mail à lista de destinatários ou criado um novo tópico, o Amazon SNS enviará uma mensagem de e-mail de confirmação de assinatura para cada novo endereço. Cada destinatário deve confirmar a assinatura escolhendo o link contido na mensagem. As notificações de alerta são enviadas apenas para endereços confirmados.

6. Em Alarm action (Ação de alarme), ative a opção para especificar uma ação a ser executada quando o alarme for acionado. Selecione a ação.
7. Em Alarm thresholds (Limites de alarme), especifique a métrica e os critérios do alarme.

   É possível deixar as configurações padrão para Group samples by (Average) (Agrupar amostras por, Média) e Type of data to sample (Status check failed: either) (Tipo de dados para amostragem, Falha na verificação de status: qualquer), ou pode alterá-los para atender às suas necessidades.

   Para Consecutive Period (Período consecutivo), defina o número de períodos que deseja avaliar e, em Period (Período), insira a duração do período de avaliação antes de acionar o alarme e enviar um e-mail.
8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Criar.

Se você precisar fazer alterações em um alarme de status de instância, poderá editá-lo.

Para editar um alarme de verificação de status

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitoring (Monitoramento), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), escolha Edit an alarm (Editar um alarme).
5. Em Search for alarm (Procurar alarme), escolha o alarme.
6. Quando terminar de fazer alterações, escolha Update (Atualizar).

Command line

No exemplo a seguir, o alarme publica uma notificação para um tópico de SNS, `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, quando há falha da instância na verificação de instância ou na verificação de status de sistema por, pelo menos, dois períodos consecutivos. A métrica do CloudWatch usada é `StatusCheckFailed`.

Como criar um alarme de verificação de status usando a AWS CLI

1. Selecione um tópico de SNS existente ou crie um novo. Para obter mais informações, consulte Uso do Amazon SNS com a AWS CLI no Guia do usuário da AWS Command Line Interface.
2. Use o seguinte comando list-metrics para visualizar as métricas do Amazon CloudWatch disponíveis para o Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Use o seguinte comando put-metric-alarm para criar o alarme.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

O período é o intervalo de tempo, em segundos, no qual as métricas do Amazon CloudWatch são coletadas. Este exemplo usa 300, que são 60 segundos multiplicados por 5 minutos. O período de avaliação é o número de períodos consecutivos pelos quais o valor da métrica deve ser comparado ao limite. Este exemplo usa 2. As ações do alarme são as ações a serem executadas quando esse alarme é acionado. Este exemplo configura o alarme para enviar um e-mail usando Amazon SNS.

Eventos de alteração de estado das instâncias

O Amazon EC2 envia um evento `EC2 Instance State-change Notification` ao Amazon EventBridge quando o estado de uma instância é alterado.

A seguir estão dados de exemplo para esse evento. Neste exemplo, a instância inseriu o estado `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

Os possíveis valores para `state` são:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Quando você executa ou inicia uma instância, ela entra no estado `pending` e depois no estado `running`. Quando você interrompe uma instância, ela entra no estado `stopping` e depois no estado `stopped`. Quando você termina uma instância, ela entra no estado `shutting-down` e depois no estado `terminated`.

Receber uma notificação por e-mail quando o estado da instância for alterado

Para receber notificações por e-mail quando o estado de sua instância for alterado, crie um tópico do Amazon SNS e crie uma regra do EventBridge para o evento `EC2 Instance State-change Notification`.

Para criar um tópico do SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.

2. No painel de navegação, escolha Tópicos.
3. Escolha Criar tópico.
4. Em Tipo, escolha Padrão.
5. Em Name (Nome), digite um nome para o tópico.
6. Escolha Criar tópico.
7. Selecione Criar assinatura.
8. Em Protocolo, escolha Email.
9. Em Endpoint, insira o endereço de e-mail que receberá as notificações.
10. Selecione Criar assinatura.
11. Você receberá uma mensagem de e-mail com esta linha de assunto: AWS Notification - Subscription Confirmation. Siga as instruções para confirmar sua assinatura.

Para criar uma regra de EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Name (Nome), insira um nome para a regra.
4. Em Tipo de Regra, escolha Regra com Padrão de Evento.
5. Escolha Próximo.
6. Em Event pattern (Padrão de evento), faça o seguinte:
    a. Em Event source, escolha Serviços da AWS.
    b. Em AWS service (Serviço da AWS), escolha EC2.
    c. Para Event Type (Tipo de evento), escolha EC2 Instance State-change Notification (Notificação de alteração de estado da instância do EC2).
    d. Por padrão, enviamos notificações para qualquer alteração de estado de qualquer instância. Se você preferir, é possível selecionar estados específicos ou instâncias específicas.
7. Escolha Próximo.
8. Especifique um destino desta forma:
    a. Em Target types (Tipos de destino), escolha AWS service (Serviço da AWS).
    b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS).

c. Em Topic (Tópico), selecione o tópico do SNS que você criou no procedimento anterior.

9. Escolha Próximo.
10. (Opcional) Adicione etiquetas à regra.
11. Escolha Próximo.
12. Selecione Criar regra.
13. Para testar a regra, inicie uma alteração de estado. Por exemplo, inicie uma instância interrompida, interrompa uma instância em execução ou inicie uma instância. Você receberá mensagens de e-mail com esta linha de assunto: AWS Notification Message. O corpo do e-mail contém os dados do evento.

Eventos programados para instâncias

A AWS pode programar eventos para suas instâncias, como reinicialização, interrupção/início ou retirada. Esses eventos não ocorrem com frequência. Se uma de suas instâncias for afetada por um evento programado, a AWS enviará um e-mail ao endereço de e-mail que estiver associado à sua conta da AWS antes do evento programado. O e-mail fornece detalhes sobre o evento, incluindo as datas de início e de término. Dependendo do evento, é possível tomar providências para controlar sua duração. A AWS também envia um evento do AWS Health, que é possível monitorar e gerenciar usando o Amazon CloudWatch Events. Para obter mais informações sobre monitoramento de eventos do AWS Health com o CloudWatch, consulte Monitoramento de eventos do AWS Health com o CloudWatch Events.

Os eventos programados são gerenciados pela AWS. Você não pode programar eventos para suas instâncias. É possível visualizar os eventos programados pela AWS, personalizar notificações de eventos programados para incluir ou remover etiquetas da notificação por email, e executar ações quando uma instância estiver programada para ser reinicializada, desativada ou interrompida.

Para atualizar as informações de contato de sua conta a fim de ter certeza de que será notificado sobre os eventos agendados, acesse a página Configurações da conta.

> **Note**
>
> Quando uma instância for afetada por um evento agendado e fizer parte de um grupo do Auto Scaling, o Amazon EC2 Auto Scaling futuramente a substituirá como parte de suas verificações de integridade, e você não precisará realizar nenhuma outra ação. Para obter mais informações sobre as verificações de integridade realizadas pelo Amazon EC2 Auto

Scaling, consulte Verificações de integridade para instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Conteúdo

- Tipos de eventos programados
- Visualizar eventos agendados
- Personalizar notificações de eventos programados
- Trabalhar com instâncias programadas para interrupção ou retirada
- Trabalhar com instâncias programadas para reinicialização
- Trabalhar com instâncias programadas para manutenção
- Reagendar um evento programado
- Definir janelas de eventos para eventos programados

Tipos de eventos programados

O Amazon EC2 pode criar os seguintes tipos de eventos para suas instâncias, onde o evento ocorre em um horário programado:

- Instance stop (Interrupção de instância): na hora programada, a instância é interrompida. Quando você iniciá-la novamente, ela será migrada para um novo host. Aplica-se somente a instâncias baseadas no Amazon EBS.
- Instance retirement (Desativação da instância): na hora programada a instância é interrompida, se for baseada no Amazon EBS, ou encerrada, se for baseada no armazenamento de instâncias.
- Instance reboot (Reinicialização de instância): na hora programada, a instância é reinicializada.
- System reboot (Reinicialização do sistema): na hora programada, o host da instância é reinicializado.
- System maintenance (Manutenção do sistema): na hora programada, a instância pode ser temporariamente afetada pela manutenção de rede ou pela manutenção de energia.

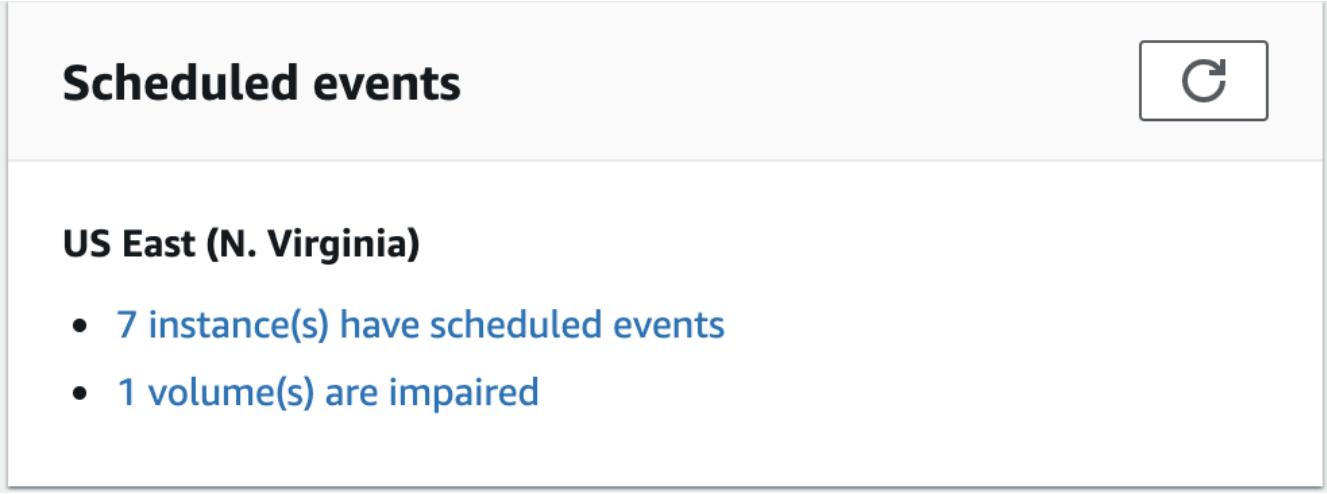
Visualizar eventos agendados

Além de receber a notificação de eventos agendados por e-mail, é possível verificar se há eventos programados usando um dos métodos a seguir.

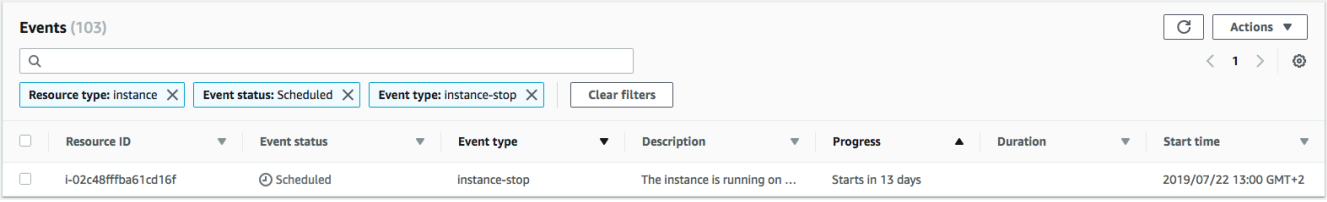
Console

Para visualizar eventos programados para suas instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. O painel exibe quaisquer recursos com um evento associado em Eventos agendados.



3. Para obter mais detalhes, escolha Eventos no painel de navegação. Todos os recursos com um evento associado serão exibidos. Você pode filtrar por características como tipo de evento, tipo de recurso e zona de disponibilidade.



AWS CLI

Para visualizar eventos programados para suas instâncias

Use o comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

O exemplo de saída a seguir mostra um evento de reinicialização.

```
[
```

```
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Para visualizar os eventos programados para suas instâncias usando a AWS Tools for Windows PowerShell

Use o seguinte comando Get-EC2InstanceStatus.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Para visualizar os eventos programados para suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos de manutenção ativos para suas instâncias dos metadados de instância usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema programado, no formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados das suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos concluídos ou cancelados para suas instâncias dos metadados de instância usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema que foi cancelado e um que foi concluído, no formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

É possível usar o AWS Health Dashboard para saber mais sobre eventos que podem afetar a instância. O AWS Health Dashboard organiza problemas em três grupos: ocorrências abertas, alterações programadas e outras notificações. O grupo de alterações programadas contém itens presentes e futuros.

Para obter mais informações, consulte Como iniciar o AWS Health Dashboard no Guia do usuário doAWS Health.

Personalizar notificações de eventos programados

É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail. Isso facilita a identificação do recurso afetado (instâncias ou Hosts dedicados) e priorizar ações para o próximo evento.

Ao personalizar notificações de eventos para incluir tags, é possível optar por incluir:

- Todas as tags associadas ao recurso afetado
- Somente tags específicas que estão associadas ao recurso afetado

Por exemplo, suponha que você atribua as tags `application`, `costcenter`, `project` e `owner` a todas as suas instâncias. É possível optar por incluir todas as tags nas notificações de eventos. Como alternativa, se você quiser ver apenas as tags `owner` e `project` nas notificações de eventos, poderá optar por incluir apenas essas tags.

Depois de selecionar as tags a serem incluídas, as notificações de evento incluirão o ID do recurso (ID da instância ou ID do Host dedicado) e os pares de chave de tag e valor associados ao recurso afetado.

Tarefas

- Incluir tags em notificações de eventos
- Remover tags de notificações de eventos
- Visualizar as tags a serem incluídas nas notificações de eventos

Incluir tags em notificações de eventos

As tags que você escolher incluir se aplicarão a todos os recursos (instâncias e Hosts dedicados) na região selecionada. Para personalizar notificações de eventos em outras regiões, primeiro selecione a região necessária e execute as etapas a seguir.

É possível incluir tags em notificações de eventos usando um dos métodos a seguir.

Console

Como incluir tags em notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.

3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Ative a opção Incluir tags em notificações de eventos.
5. Siga um destes procedimentos, dependendo das tags que você deseja incluir nas notificações de eventos:
   - Para incluir todas as tags associadas à instância afetada ou ao Host dedicado, selecione Incluir todas as tags.
   - Para selecionar as tags a serem incluídas, selecione Escolher as tags a serem incluídas e, em seguida, selecione ou insira as chaves de tag.
6. Escolha Salvar.

AWS CLI

Como incluir todas as tags em notificações de eventos

Use o comando register-instance-event-notification-attributes da AWS CLI e defina o parâmetro `IncludeAllTagsOfInstance` como `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Como incluir tags específicas em notificações de eventos

Use o comando register-instance-event-notification-attributes da AWS CLI e especifique as tags a serem incluídas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Remover tags de notificações de eventos

É possível remover tags de notificações de eventos usando um dos métodos a seguir.

Console

Como remover tags de notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Para remover todas as tags das notificações de eventos, desmarque Incluir tags nas notificações de eventos.
5. Para remover tags específicas das notificações de eventos, escolha o X para as chaves de tag correspondentes.
6. Escolha Salvar.

AWS CLI

Como remover todas as tags das notificações de eventos

Use o comando deregister-instance-event-notification-attributes da AWS CLI e defina o parâmetro `IncludeAllTagsOfInstance` como `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Como remover tags específicas de notificações de eventos

Use o comando deregister-instance-event-notification-attributes da AWS CLI e especifique as tags a serem removidas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Visualizar as tags a serem incluídas nas notificações de eventos

É possível visualizar as tags que devem ser incluídas nas notificações de eventos usando um dos métodos a seguir.

Console

Como visualizar as tags a serem incluídas nas notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).

AWS CLI

Como visualizar as tags a serem incluídas nas notificações de eventos

Use o comando describe-instance-event-notification-attributes da AWS CLI.

```
aws ec2 describe-instance-event-notification-attributes
```

Trabalhar com instâncias programadas para interrupção ou retirada

Quando a AWS detecta falha irreparável do host subjacente para sua instância, ela programa a instância para ser interrompida ou encerrada, dependendo do tipo de dispositivo raiz da instância. Se o dispositivo raiz for um volume do EBS, a instância será programada para ser interrompida. Se o dispositivo raiz for um volume de armazenamento de instância, a instância será programada para encerrar. Para ter mais informações, consulte Desativação da instância.

> **Important**
>
> Todos os dados armazenados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de instância anexados a uma instância que possui um volume do EBS como dispositivo raiz. Lembre-se de salvar os dados dos volumes do armazenamento de instâncias que poderão ser necessários mais tarde antes que a instância seja interrompida, hibernada ou encerrada.

Ações para instâncias baseadas no Amazon EBS

É possível esperar que a instância seja interrompida conforme programado. Como opção, é possível interromper e iniciar a instância por conta própria, o que a fará migrar para um novo host. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte Início e interrupção de instâncias do Amazon EC2.

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de interrupção de instância. Para obter mais informações, consulte Automating actions for Amazon EC2 instances no Guia do usuário do AWS Health.

Ações para instâncias com armazenamento de instâncias

Recomendamos que você execute uma instância de substituição da AMI mais recente e migre todos os dados necessários para a instância de substituição antes que a instância seja programada para encerrar. Depois, é possível encerrar a instância original ou esperar que ela seja encerrada conforme programado.

Trabalhar com instâncias programadas para reinicialização

Quando a AWS precisa realizar tarefas, como instalar atualizações ou manter o host subjacente, ela pode programar a reinicialização da instância ou do host subjacente. É possível reprogramar a maioria dos eventos de reinicialização para que a instância seja reinicializada em uma data e hora específicas que sejam adequadas para você.

Visualizar o tipo de evento de reinicialização

É possível ver se um evento de reinicialização é uma reinicialização de instância ou uma reinicialização do sistema usando um dos métodos a seguir.

Console

Para visualizar o tipo de evento de reinicialização programado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Resource type: instance (Tipo de recurso: instância) na lista de filtros.
4. Para cada instância, visualize o valor na coluna Event type (Tipo de evento). O valor é system-reboot ou instance-reboot.

AWS CLI

Para visualizar o tipo de evento de reinicialização programado

Use o comando describe-instance-status.

```
aws ec2 describe-instance-status \
```

```
    --instance-id i-1234567890abcdef0
```

Para eventos de reinicialização programados, o valor de `Code` é `system-reboot` ou `instance-reboot`. O seguinte exemplo de saída mostra um evento `system-reboot`.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

Ações para reinicialização de instância

É possível aguardar para que a reinicialização da instância ocorra dentro de sua janela de manutenção programada, reprogramar a reinicialização da instância para uma data e hora que sejam adequadas para você ou reinicializar a instância por conta própria em um momento conveniente.

Após a reinicialização da instância, o evento programado será apagado e a descrição dele será atualizada. A manutenção pendente do host subjacente será concluída e será possível começar a usar a instância novamente depois que ela tiver sido totalmente reinicializada.

Ações para a reinicialização do sistema

Você não pode reinicializar o sistema por conta própria. É possível aguardar para que a reinicialização do sistema ocorra durante a janela de manutenção programada, ou pode reprogramar a reinicialização do sistema para uma data e hora que sejam adequadas para você. Normalmente, uma reinicialização de sistema é concluída em questão de minutos. Depois que a reinicialização do sistema ocorre, a instância mantém o endereço IP e o nome de DNS, e qualquer dado nos volumes de armazenamento de instâncias locais é preservado. Depois que a reinicialização do sistema é concluída, o evento programado para a instância é apagado, e é possível verificar se o software da instância está operando conforme o esperado.

Como opção, se for necessário manter a instância em um horário diferente e você não puder reprogramar a reinicialização do sistema, não será possível interromper e iniciar a instância baseada no Amazon EBS, de modo que ela será migrada para um novo host. No entanto, os dados dos volumes de armazenamento de instâncias locais não são preservados. Também é possível automatizar uma interrupção e inicialização imediatas da instância em resposta a um evento programado de inicialização do sistema. Para obter mais informações, consulte Automatização de ações para instâncias do EC2 no Guia do usuário do AWS Health. Para uma instância baseada no armazenamento de instâncias, se não for possível reprogramar a reinicialização do sistema, será possível executar uma instância de substituição da AMI mais recente, migrar todos os dados necessários para a instância de substituição antes da janela de manutenção programada e encerrar a instância original.

Trabalhar com instâncias programadas para manutenção

Quando a AWS precisa manter o host subjacente de uma instância, ela programa a instância para manutenção. Há dois tipos de eventos de manutenção: manutenção de rede e manutenção de energia.

Durante a manutenção de rede, instâncias programadas perdem a conectividade de rede durante um breve período. A conectividade de rede normal com a instância é restaurada depois que a manutenção for concluída.

Durante a manutenção de energia, as instâncias programadas ficam offline durante um breve período e depois são reinicializadas. Quando uma reinicialização é realizada, todas as definições de configuração da instância são mantidas.

Depois que sua instância tiver sido reinicializada (isso geralmente leva alguns minutos), verifique se a aplicação está funcionando conforme o esperado. Nesse ponto, a instância não deve mais ter um evento associado a ela ou, se tiver, a descrição do evento programado começará com [Completed]. Às vezes, leva até 1 hora para que a descrição do status da instância seja atualizada. Eventos de manutenção concluídos são exibidos no painel do console do Amazon EC2 por até uma semana.

Ações para instâncias baseadas no Amazon EBS

É possível esperar que a manutenção ocorra conforme programado. Como opção, é possível interromper e iniciar a instância, o que a fará migrar para um novo host. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte Início e interrupção de instâncias do Amazon EC2.

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de manutenção. Para obter mais informações, consulte Automatização de ações para instâncias do EC2 no Guia do usuário do AWS Health.

Ações para instâncias com armazenamento de instâncias

É possível esperar que a manutenção ocorra conforme programado. Como alternativa, se quiser manter a operação normal durante a janela de manutenção programada, é possível iniciar uma instância de substituição da AMI mais recente, migrar todos os dados necessários para a instância de substituição antes da janela de manutenção programada e, então, encerrar a instância original.

Reagendar um evento programado

É possível reagendar um evento para que ele ocorra em uma data e hora específicas que forem convenientes. Somente eventos que tenham uma data de prazo podem ser reprogramados. Há outras limitações para reprogramar um evento.

É possível reagendar um evento usando um dos métodos a seguir.

Console

Para reprogramar um evento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Resource type: instance (Tipo de recurso: instância) na lista de filtros.
4. Escolha uma ou mais instâncias e selecione Actions (Ações), Schedule event (Programar evento).

   Somente eventos que têm uma data de prazo de evento, indicados por um valor para Deadline (Prazo), podem ser reprogramados. Se um dos eventos selecionados não tiver uma data de prazo, a opção Actions (Ações), Schedule event (Programar evento) será desativada.
5. Em New start time (Nova hora de início), insira uma nova data e hora para o evento. A nova data e hora devem ocorrer antes de Event deadline (Prazo do evento).
6. Escolha Salvar.

   Pode levar um ou dois minutos para a hora de início do evento atualizado ser refletida no console.

AWS CLI

Para reprogramar um evento

1. Somente eventos que têm uma data de prazo de evento, indicados por um valor para `NotBeforeDeadline`, podem ser reprogramados. Use o comando describe-instance-status para visualizar o valor do parâmetro `NotBeforeDeadline`.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

O seguinte exemplo de saída mostra um evento `system-reboot` que pode ser reprogramado, pois `NotBeforeDeadline` contém um valor.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

2. Para reprogramar o evento, use o comando modify-instance-event-start-time. Especifique a nova hora de início do evento usando o parâmetro `not-before`. A nova hora do evento deve ser antes de `NotBeforeDeadline`.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2019-03-25T10:00:00.000
```

O comando describe-instance-status poderá levar um ou dois minutos para retornar o valor do parâmetro `not-before` atualizado.

Limitações

- Somente eventos com uma data de prazo podem ser reprogramados. O evento pode ser reprogramado até a data de prazo do evento. A coluna Deadline (Prazo) do console e o campo `NotBeforeDeadline` da AWS CLI indicam se o evento tem uma data de prazo.
- Somente eventos ainda não iniciados podem ser reprogramados. A coluna Start time (Hora de início) do console e o campo `NotBefore` da AWS CLI indicam a hora de início do evento. Os eventos programados para início nos próximos cinco minutos não podem ser reprogramados.
- A nova hora de início do evento deve ser pelo menos 60 minutos a partir da hora atual.
- Se você reprogramar vários eventos usando o console, a data de prazo do evento será determinada pelo evento com a data de prazo do evento mais recente.

Definir janelas de eventos para eventos programados

É possível definir janelas de eventos personalizadas recorrentes semanalmente para eventos agendados que reinicializam, interrompem ou terminam suas instâncias do Amazon EC2. É possível associar uma ou mais instâncias a uma janela de eventos. Se um evento agendado para essas instâncias estiver planejado, a AWS irá programar os eventos na janela de eventos associada.

É possível usar janelas de eventos para maximizar a disponibilidade da workload especificando janelas de eventos que ocorrem durante períodos fora do pico para sua workload. Também é possível alinhar as janelas de eventos com suas programações de manutenção internas.

Você define uma janela de evento especificando um conjunto de intervalos de tempo. O intervalo de tempo mínimo é de duas horas. Os intervalos de tempo combinados devem totalizar pelo menos 4 horas.

É possível associar uma ou mais instâncias a uma janela de evento usando IDs de instância ou tags de instância. Também é possível associar hosts dedicados a uma janela de evento usando o ID do host.

> **Warning**
>
> As janelas de eventos são aplicáveis apenas para eventos agendados que param, reinicializam ou encerram instâncias.
> Janelas de eventos sãonãoaplicável para:
>
> - Eventos agendados e eventos de manutenção de rede acelerados.

- Manutenção não programada, como AutoRecovery e reinicializações não planejadas.

Trabalhar com janelas de eventos

- Considerações
- Visualizador de eventos do Windows
- Criar janelas de eventos
- Modificar janelas de
- Excluir janelas de eventos
- Marcar janelas de eventos

Considerações

- Todos os horários da janela de eventos são mostrados em UTC.
- A duração mínima da janela semanal de eventos é de quatro horas.
- Os intervalos de tempo dentro de uma janela de evento devem ser de pelo menos 2 horas.
- Apenas um tipo de destino (ID de instância, ID de host dedicado ou tag de instância) pode ser associado a uma janela de evento.
- Um destino (ID de instância, ID de host dedicado ou tag de instância) só pode ser associado a uma janela de evento.
- Um máximo de 100 IDs de instância, ou 50 IDs de host dedicados ou 50 tags de instância podem ser associados a uma janela de evento. As tags de instância podem ser associadas a qualquer número de instâncias.
- Um máximo de 200 janelas de eventos podem ser criadas por AWS região:
- Várias instâncias associadas a janelas de eventos podem potencialmente ter eventos agendados ocorrem ao mesmo tempo.
- Se a AWS já agendou um evento, modificar uma janela de evento não alterará a hora do evento agendado. Se o evento tiver uma data limite, é possívelreprogramar o evento.
- É possível interromper e iniciar uma instância antes do evento agendado, que migra a instância para um novo host, e o evento agendado não ocorrerá mais.

Visualizador de eventos do Windows

É possível reagendar um evento usando um dos métodos a seguir.

Console

Para visualizar janelas de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. SelecioneAções,Gerenciar janelas de eventos.
4. Selecione uma janela de eventos para visualizar seus detalhes.

AWS CLI

Para descrever todas as janelas de eventos

Usar adescribe-instance-event-windowscomando.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Saída esperada

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }
```

```
        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Para descrever uma janela de eventos específica

Usar adescribe-instance-event-windowscom o comando`--instance-event-window-id`para descrever uma janela de evento específica.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Para descrever janelas de eventos que correspondam a um ou mais filtros

Usar adescribe-instance-event-windowscom o comando`--filters`parâmetro . No exemplo a seguir, o filtro `instance-id` é usado para descrever todas as janelas de eventos que estão associadas à instância especificada.

Quando um filtro é usado, ele executa uma correspondência direta. No entanto, o`instance-id`é diferente. Se não houver correspondência direta com o ID da instância, ele voltará para associações indiretas com a janela de eventos, como tags da instância ou ID de host dedicado (se a instância estiver em um host dedicado).

Para obter a lista de filtros compatíveis, consulte describe-instance-event-windows na Referência da AWS CLI.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

Saída esperada

No exemplo a seguir, a instância está em um Host Dedicado, que está associado à janela de evento.

```
{
```

```
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

Criar janelas de eventos

É possível criar uma ou mais janelas de eventos. Para cada janela de evento, você especifica um ou mais blocos de tempo. Por exemplo, é possível criar uma janela de evento com blocos de tempo que ocorrem todos os dias às 4h por duas horas. Ou é possível criar uma janela de evento com blocos de tempo que ocorrem aos domingos, das 2h às 4h, e às quartas-feiras, das 3h às 5h.

Para ver as restrições da janela de eventos, consulteConsideraçõesAnteriormente neste tópico.

Janelas de eventos repetem semanalmente até que você as exclua.

Use um dos métodos a seguir para criar uma janela de eventos.

Console

Para criar uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Events.
3. SelecioneAções,Gerenciar janelas de eventos.
4. SelecioneJanela Criar evento de instância.
5. para oNome da janela de eventos, insira um nome descritivo para a janela de eventos.
6. para oAgendamentos de janelas, escolha especificar os blocos de tempo na janela de eventos usando o construtor de cron ou especificando intervalos de tempo.

   - Se escolher oConstrutor de cron, especifique o seguinte:
     1. para oDias (UTC), especifique os dias da semana em que a janela de eventos ocorre.
     2. para oHora de início (UTC), especifique a hora em que a janela de evento começa.
     3. para oDuration (Duração), especifique a duração dos blocos de tempo na janela do evento. A duração mínima por bloco de tempo é de 2 horas. A duração mínima da janela do evento deve ser igual ou superior a 4 horas no total. Todos os horários são em UTC.
   - Se escolher Intervalos de tempo, escolha Adicione um novo intervalo de tempo e especifique o dia e a hora de início e o dia e a hora de término. Repita para cada intervalo de tempo. A duração mínima por intervalo de tempo é de 2 horas. A duração mínima para todos os intervalos de tempo combinados deve ser igual ou superior a 4 horas no total.
7. (Opcional) ParaDetalhes do alvo, associe uma ou mais instâncias à janela de evento para que, se as instâncias estiverem agendadas para manutenção, o evento agendado ocorra durante a janela de evento associada. É possível associar uma ou mais instâncias a uma janela de evento usando IDs de instância ou tags de instância. É possível associar hosts dedicados a uma janela de evento usando o ID do host.

   É possível criar a janela de evento sem associar um destino à janela. Posteriormente, é possível modificar a janela para associar um ou mais alvos.
8. (Opcional) ParaTags da janela, escolhaAdicionar tag(Opcional) e insira a chave e o valor da tag. Repita esse procedimento para cada tag.
9. SelecioneJanela Criar eventos.

AWS CLI

Para criar uma janela de eventos usando a AWS CLI, crie primeiro a janela de evento e associe um ou mais destinos à janela de eventos.

Criar uma janela de eventos

É possível definir um conjunto de intervalos de tempo ou uma expressão cron ao criar a janela de evento, mas não ambos.

Para criar uma janela de eventos com um intervalo de tempo

Usar a`create-instance-event-window`e especifique o`--time-range`parâmetro . Você também deve especificar o parâmetro `--cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para criar uma janela de eventos com uma expressão cron

Usar a`create-instance-event-window`e especifique o`--cron-expression`parâmetro . Você também deve especificar o parâmetro `--time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Associar um alvo a uma janela de evento

É possível associar apenas um tipo de destino (IDs de instância, IDs de host dedicado ou tags de instância) a uma janela de evento.

Para associar tags de instância a uma janela de eventos

Usar aassociar-instance-event-windowe especifique o`instance-event-window-id`parâmetro para especificar a janela de evento. Para associar tags de instância, especifique o`--association-targete` para os valores de parâmetro, especifique uma ou mais tags.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para associar uma ou mais instâncias a uma janela de eventos

Usar aassociar-instance-event-windowe especifique o`instance-event-window-id`parâmetro para especificar a janela de evento. Para associar instâncias, especifique o`--association-target`e para os valores de parâmetro, especifique um ou mais IDs de instância.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
```

```
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para associar um host dedicado a uma janela de eventos

Usar aassociar-instance-event-windowe especifique o`instance-event-window-id`parâmetro para especificar a janela de evento. Para associar um Host Dedicado, especifique o`--association-targete`, para os valores de parâmetro, especifique um ou mais IDs de Host Dedicado.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Modificar janelas de

É possível modificar todos os campos de uma janela de evento, exceto seu ID. Por exemplo, quando o horário de verão começar, convém modificar o agendamento da janela de eventos. Para janelas de eventos existentes, talvez você queira adicionar ou remover destinos.

Para modificar um volume do EBS, use um dos métodos a seguir.

Console

Para modificar uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. SelecioneAções,Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser modificada e escolhaAções,Janela Modificar evento da.
5. Modifique os campos na janela de eventos e escolhaModify event window.

AWS CLI

Para modificar uma janela de eventos usando oAWS CLI, é possível modificar o intervalo de tempo ou a expressão cron e associar ou desassociar um ou mais destinos à janela de evento.

Modificar a hora da janela de

É possível modificar um intervalo de tempo ou uma expressão cron ao modificar a janela de evento, mas não ambos.

Para modificar o intervalo de tempo de uma janela de eventos

Usar amodify-instance-event-windowe especifique a janela de evento a ser modificada. Especifique o`--time-range`Parâmetro para modificar o intervalo de tempo. Você também deve especificar o parâmetro `--cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modificar um conjunto de intervalos de tempo para uma janela de eventos

Usar amodify-instance-event-windowe especifique a janela de evento a ser modificada. Especifique o`--time-range`Parâmetro para modificar o intervalo de tempo. Você também não pode especificar o`--cron-expression`Parâmetro na mesma chamada.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
```

```
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para modificar a expressão cron de uma janela de eventos

Usar amodify-instance-event-windowe especifique a janela de evento a ser modificada. Especifique o`--cron-expression`para modificar a expressão cron. Você também deve especificar o parâmetro `--time-range`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modificar os alvos associados a uma janela de evento

É possível associar alvos adicionais a uma janela de evento. Também é possível desassociar alvos existentes de uma janela de evento. No entanto, apenas um tipo de destino (IDs de instância, IDs de host dedicado ou tags de instância) pode ser associado a uma janela de evento.

Para associar alvos adicionais a uma janela de evento

Para obter instruções sobre como associar alvos a uma janela de evento, consulteAssociate a target with an event window.

Para desassociar tags de instância de uma janela de eventos

Usar adisassociar-instance-event-janelae especifique o`instance-event-window-id`parâmetro para especificar a janela de evento. Para desassociar tags de instância, especifique o`--association-targete` para os valores de parâmetro, especifique uma ou mais tags.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para desassociar uma ou mais instâncias de uma janela de eventos

Usar adisassociar-instance-event-janelae especifique o`instance-event-window-id`parâmetro para especificar a janela de evento. Para desassociar instâncias, especifique o`--association-targete` para os valores de parâmetro, especifique um ou mais IDs de instância.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para desassociar um host dedicado de uma janela de eventos

Usar adisassociar-instance-event-janelae especifique `oinstance-event-window-id`parâmetro para especificar a janela de evento. Para desassociar um Host Dedicado, especifique o`--association-targete`, para os valores de parâmetro, especifique um ou mais IDs de Host Dedicado.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
```

```
    }
}
```

Excluir janelas de eventos

É possível excluir uma janela de eventos de cada vez usando um dos métodos a seguir.

Console

Para excluir uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. SelecioneAções,Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser excluída e escolhaAções,Janela de evento Excluir instância.
5. Quando solicitado, digite **`delete`** e escolha Delete (Excluir).

AWS CLI

Para excluir uma janela de eventos

Usar adelete-instance-event-windowe especifique a janela de evento a ser excluída.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Para forçar a exclusão de uma janela de eventos

Usar a`--force-delete`se a janela de evento estiver atualmente associada a destinos.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Saída esperada

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Marcar janelas de eventos

É possível marcar uma janela de evento ao criá-la ou posteriormente.

Para marcar uma janela de evento ao criá-la, consulteCriar janelas de eventos.

Use um dos métodos a seguir para marcar uma janela de evento.

Console

Para marcar uma janela de eventos atual

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. SelecioneAções,Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser marcada e escolhaAções,Gerenciar tags de janela de evento de.
5. Para adicionar uma tag, escolha Add tag. Repita esse procedimento para cada tag.
6. Escolha Salvar.

AWS CLI

Para marcar uma janela de eventos atual

Use o comando create-tags para marcar os recursos existentes. No exemplo a seguir, a solicitação de existente é marcada com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Monitorar instâncias usando o CloudWatch

É possível monitorar suas instâncias usando o Amazon CloudWatch, que coleta e processa os dados brutos do Amazon EC2 em métricas legíveis, quase em tempo real. Essas estatísticas são registradas para um período de 15 meses, de forma que você possa acessar informações históricas e ganhar uma perspectiva melhor sobre como seu serviço ou aplicação Web está se saindo.

Por padrão, o Amazon EC2 envia dados de métrica ao CloudWatch em períodos de 5 minutos. Para enviar dados de métrica para sua instância ao CloudWatch em períodos de 1 minuto, é possível habilitar o monitoramento detalhado na instância. Para ter mais informações, consulte Habilitar ou desabilitar o monitoramento detalhado para instâncias.

O console do Amazon EC2 exibe uma série de gráficos com base nos dados brutos do Amazon CloudWatch. Dependendo de suas necessidades, é possível preferir obter dados para suas instâncias do Amazon CloudWatch em vez de gráficos no console.

Para saber mais sobre faturamento e custos do Amazon CloudWatch, consulte Faturamento e custos do CloudWatch no Guia do usuário do Amazon CloudWatch.

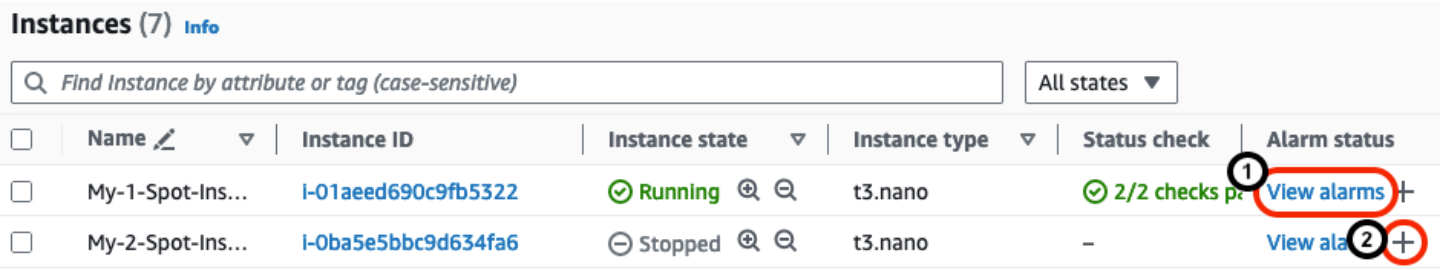
Conteúdo

- Alarmes de instância do Amazon EC2
- Habilitar ou desabilitar o monitoramento detalhado para instâncias
- Listar as métricas disponíveis do CloudWatch para as instâncias
- Instale e configure o agente do CloudWatch usando o console do Amazon EC2 para adicionar métricas adicionais
- Obter estatísticas para as métricas das instâncias
- Representar métricas em gráficos para as instâncias
- Criar um alarme do CloudWatch para uma instância
- Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância

Alarmes de instância do Amazon EC2

É possível visualizar e criar alarmes do Amazon CloudWatch para suas Instâncias na tela Instâncias do console do Amazon EC2.

A captura de tela a seguir indica os controles do console, numerados 1 e 2 para visualização e criação de alarmes na tela Instâncias.



Visualizar alarmes na tela Instâncias

É possível visualizar os alarmes de cada instância na tela Instâncias.

Para visualizar o alarme de uma instância na tela Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na tabela Instâncias, para a instância escolhida, escolha Visualizar alarmes (numerados com 1 na captura de tela anterior).
4. Na janela Detalhes do alarme para ***i-0123456789example***, escolha o nome do alarme para visualizar no console do CloudWatch.

Criar alarmes na tela Instâncias

É possível criar um alarme para cada instância na tela Instâncias.

Para criar um alarme para uma instância na tela Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na tabela Instâncias, para a instância escolhida, escolha o sinal de adição (numerado com 2 na captura de tela anterior).
4. Na tela Gerenciar alarmes do CloudWatch, crie seu alarme. Para ter mais informações, consulte Criar um alarme do CloudWatch para uma instância.

Habilitar ou desabilitar o monitoramento detalhado para instâncias

Por padrão, sua instância está habilitada para monitoramento básico. Também é possível habilitar o monitoramento detalhado.

Veja na tabela abaixo as diferenças entre o monitoramento básico e o monitoramento detalhado de instâncias.

Tipo de monitoramento	Descrição	Cobranças
Monitoramento básico	Somente as métricas de verificação de status estão disponíveis em períodos de um minuto. Todas as outras métricas estão disponíveis em períodos de cinco minutos.	Sem cobrança.
Monitoramento detalhado	Todas as métricas, inclusive as de verificação de status, estão disponíveis em períodos de um minuto. Para obter esse nível de dados, é necessário especificamente habilitá-lo para a instância. Para as instâncias onde você tiver habilitado monitoramento detalhado, também é possível obter dados agregados nos grupos de instâncias semelhantes.	A cobrança é feita por métrica enviada ao CloudWatch. Você não é cobrado pelo armazenamento de dados. Para obter mais informações, consulte Nível pago e Exemplo 1 – Monitoramento detalhado do EC2 na página de definição de preço de Amazon CloudWatch.

Tópicos

- Permissões obrigatórias do IAM
- Habilitar o monitoramento detalhado
- Desativar o monitoramento detalhado

Permissões obrigatórias do IAM

Para habilitar o monitoramento detalhado de uma instância, o usuário deve ter permissão para usar a ação de API MonitorInstances. Para desativar o monitoramento detalhado de uma instância, o usuário deve ter permissão para usar a ação de API UnmonitorInstances.

Habilitar o monitoramento detalhado

É possível habilitar o monitoramento detalhado em uma instância quando a executá-la ou depois de a instância estiver sendo executada ou interrompida. Habilitar o monitoramento detalhado em uma instância não afeta o monitoramento dos volumes do EBS anexados à instância. Para obter mais informações, consulte Métricas de uso do Amazon CloudWatch para o Amazon EBS.

Console

Para habilitar o monitoramento detalhado para uma instância existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Ações, Monitorar e solucionar problemas, Gerenciar monitoramento detalhado.
4. Na página de detalhes Detailed monitoring (Monitoramento detalhado), em Detailed monitoring (Monitoramento detalhado), marque a caixa de seleção Enable (Habilitar).
5. Escolha Save (Salvar).

Para habilitar o monitoramento detalhado ao executar uma instância

Ao executar uma instância usando o console do Amazon EC2, em Detalhes avançados, marque a caixa de seleção Monitoramento detalhado do CloudWatch.

AWS CLI

Para habilitar o monitoramento detalhado para uma instância existente

Use o comando monitor-instances para habilitar o monitoramento detalhado das instâncias especificadas.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Para habilitar o monitoramento detalhado ao executar uma instância

Use o comando run-instances com o marcador `--monitoring` para ativar o monitoramento detalhado.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Desativar o monitoramento detalhado

É possível desativar o monitoramento detalhado em uma instância quando executá-la ou depois de a instância estar sendo executada ou ter sido interrompida.

Console

Para desabilitar o monitoramento detalhado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Ações, Monitorar e solucionar problemas, Gerenciar monitoramento detalhado.
4. Na página de detalhes Detailed monitoring (Monitoramento detalhado), em Detailed monitoring (Monitoramento detalhado), desmarque a caixa de seleção Enable (Habilitar).
5. Escolha Save (Salvar).

AWS CLI

Para desabilitar o monitoramento detalhado

Use o comando unmonitor-instances para desativar o monitoramento detalhado das instâncias especificadas.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Listar as métricas disponíveis do CloudWatch para as instâncias

O Amazon EC2 envia métricas para o Amazon CloudWatch. É possível usar o AWS Management Console, a AWS CLI ou uma API para listar as métricas que o Amazon EC2 envia para o CloudWatch. Por padrão, cada ponto de dados abrange os 5 minutos seguintes ao início da atividade para a instância. Se você tiver habilitado o monitoramento detalhado, cada ponto de dados abrangerá o minuto seguinte ao início da atividade. Observe que, para as estatísticas Mínimo, Máximo e Média, a granularidade mínima para as métricas que o EC2 fornece é de 1 minuto.

Para obter informações sobre a obtenção de estatísticas para essas métricas, consulte Obter estatísticas para as métricas das instâncias.

Tópicos

- Métricas de instância
- Métricas de crédito de CPU
- Métricas de host dedicado
- Métricas do Amazon EBS para instâncias baseadas em Nitro
- Métricas de verificação de status
- Métricas de espelhamento de tráfego
- Métricas do grupo do Auto Scaling
- Dimensões de métrica do Amazon EC2
- Métricas de uso do Amazon EC2
- Listar métricas usando o console
- Listar métricas usando o AWS CLI

Métricas de instância

O namespace `AWS/EC2` inclui as métricas de instância a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUUtilization`	A porcentagem de tempo físico de CPU que o Amazon EC2 usa para executar a instância do EC2, que inclui o tempo gasto para executar o código do usuário e o código do Amazon EC2. Em um nível muito alto, `CPUUtilization` é a soma da `CPUUtilization` do guest e da `CPUUtilization` do hypervisor. As ferramentas em seu sistema operacional podem mostrar uma porcentagem diferente da do CloudWatch devido a fatores como	Percentual	• Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
	simulação de dispositivos legados, configuração de dispositivos não legados, workloads com interrupções pesadas, migração ao vivo e atualização ao vivo.		
`DiskReadOps`	Operações de leitura concluídas de todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado. Para calcular a média de operações de I/O por segundo (IOPS) para o período, divida o total das operações pelo número de segundos no período em questão. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Contagem	• Soma • Média • Mínimo • Máximo
`DiskWriteOps`	Operações de gravação concluídas em todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado. Para calcular a média de operações de I/O por segundo (IOPS) para o período, divida o total das operações pelo número de segundos no período em questão. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Contagem	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`DiskReadBytes`	Bytes lidos de todos os volumes de armazenamento de instâncias disponíveis para a instância. Essa métrica é utilizada para determinar o volume de dados que a aplicação lê do disco rígido da instância. Isso pode ser usado para determinar a velocidade da aplicação. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `DiskReadBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`DiskWriteBytes`	Bytes gravados em todos os volumes de armazenamento de instâncias disponíveis para a instância. Essa métrica é utilizada para determinar o volume de dados que a aplicação grava no disco rígido da instância. Isso pode ser usado para determinar a velocidade do aplicativo. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `DiskWriteBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`MetadataNoToken`	O número de vezes que o serviço de metadados de instância (IMDS) foi acessado com êxito por meio de um método que não usa um token. Essa métrica é usada para determinar se existem processos que acessam metadados de instância que usam o serviço de metadados de instância versão 1 (IMDSv1), que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo, o serviço de metadados de instância versão 2 (IMDSv2), o valor será 0. Para ter mais informações, consulte Transição para usar o Serviço de metadados da instância versão 2.	Contagem	• Soma • Percentis
`MetadataNoTokenRejected`	O número de vezes que uma chamada ao IMDSv1 foi tentada após a desabilitação do IMDSv1. Se essa métrica aparecer, ela indica que uma chamada ao IMDSv1 foi tentada e rejeitada . Você pode reabilitar o IMDSv1 ou garantir que todas as suas chamadas usem o IMDSv2. Para ter mais informações, consulte Transição para usar o Serviço de metadados da instância versão 2.	Contagem	• Soma • Percentis

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkIn`	A quantidade de bytes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de entrada para uma única instância. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `NetworkIn` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkOut`	A quantidade de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de saída de uma única instância. O número relatado é o número de bytes enviados durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `NetworkOut` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkPackets In`	A quantidade de pacotes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de entrada em termos do número de pacotes em uma única instância. Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância recebeu nos 5 minutos, divida o valor da estatística Sum (soma) por 300. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os pacotes por segundo. Por exemplo, se você tiver represent ado graficamente `NetworkPacketsIn` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em pacotes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Contagem	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkPackets0ut`	A quantidade de pacotes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de saída em termos do número de pacotes em uma única instância. Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância enviou nos cinco minutos, divida o valor da estatística Sum (soma) por 300. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os pacotes por segundo. Por exemplo, se você tiver represent ado graficamente `NetworkPackets0ut` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em pacotes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Contagem	• Soma • Média • Mínimo • Máximo

Métricas de crédito de CPU

O namespace `AWS/EC2` inclui as seguintes métricas de crédito de CPU para suas instâncias expansíveis.

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUCreditUsage`	O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos). As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística `Sum` em vez da estatística `Average`.	Créditos (minutos de vCPU)	• Soma • Média • Mínimo • Máximo
`CPUCreditBalance`	O número de créditos ganhos de CPU que uma instância acumulou desde que foi executada ou iniciada. Para a T2 Padrão, o `CPUCreditBalance` também inclui o número de créditos de execução que foram acumulados. Os créditos são acumulados no saldo de créditos após terem sido ganhos e são removidos do saldo de créditos quando são gastos. O saldo de crédito tem um limite máximo, determinado pelo tamanho da instância. Depois que o limite for atingido, todos os novos créditos ganhos serão descartados. Para a T2 Padrão, os créditos de execução não são contabilizados para o limite. Os créditos do `CPUCreditBalance` são disponibilizados para que a instância gaste e	Créditos (minutos de vCPU)	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
	apresente intermitência com uma utilização de CPU acima da linha de base. Quando uma instância está em execução, os créditos do `CPUCreditBalance` não expiram. Quando uma instância T3 ou T3a é interrompida, o valor `CPUCreditBalance` persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor `CPUCreditBalance` não persiste, e todos os créditos acumulados são perdidos. As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.		
`CPUSurplusCreditBalance`	O número de créditos excedentes gastos por uma instância `unlimited` quando seu valor `CPUCreditBalance` é zero. O valor `CPUSurplusCreditBalance` é pago pelos créditos de CPU ganhos. Se o número de créditos excedentes ultrapassar o número máximo de créditos que a instância pode ganhar em um período de 24 horas, os créditos excedentes gastos acima do limite máximo incorrerão em uma taxa adicional. As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.	Créditos (minutos de vCPU)	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUSurplusCreditsCharged`	O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional. Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre: • Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora. • A instância é interrompida ou encerrada. • A instância é alterada de `unlimited` para `standard`. As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.	Créditos (minutos de vCPU)	• Soma • Média • Mínimo • Máximo

Métricas de host dedicado

O namespace `AWS/EC2` inclui as métricas a seguir para hosts dedicados T3.

Métrica	Descrição	Unidade	Estatísticas significativas
`DedicatedHostCPUUtilization`	A porcentagem de capacidade computacional alocada que está atualmente em uso pelas instâncias em execução no host dedicado.	Percentual	• Soma • Média • Mínimo • Máximo

Métricas do Amazon EBS para instâncias baseadas em Nitro

O namespace `AWS/EC2` inclui métricas adicionais do Amazon EBS para os volumes anexados a instâncias baseadas no Nitro que não são instâncias bare metal.

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSReadOps`	Operações de leitura concluídas de todos os volumes do Amazon EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de leitura por segundo (IOPS de leitura) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de leitura. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSReadOps` no CloudWatch como `m1`, a função métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Contagem	• Soma • Média • Mínimo • Máximo
`EBSWriteOps`	Operações de gravação concluídas para todos os volumes do EBS anexados à instância em um período especificado.	Contagem	• Soma • Média • Mínimo

Métrica	Descrição	Unidade	Estatísticas significativas
	Para calcular a média de operações de E/S de gravação por segundo (IOPS de gravação) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de gravação. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteOps` no CloudWatch como `m1`, a função métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.		• Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSReadBytes`	Bytes lidos de todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes lidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes lidos/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSReadBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSWriteBytes`	Bytes gravados em todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes gravados durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSIOBalance%`	Fornece informações sobre a porcentagem de créditos de E/S restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo
`EBSByteBalance%`	Fornece informações sobre a porcentagem de créditos de throughput restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo

Para obter informações sobre as métricas fornecidas para seus volumes do EBS, consulte Métricas para volumes do Amazon EBS no Guia do usuário do Amazon EBS. Para obter informações sobre as métricas fornecidas para suas frotas Spot, consulte Métricas do CloudWatch para frota spot.

Métricas de verificação de status

Por padrão, as métricas de verificação de status estão disponíveis a uma frequência de um minuto gratuitamente. Para uma instância recém-executada, os dados de métrica de verificação de status só estarão disponíveis depois que a instância concluir o estado de inicialização (alguns minutos após a instância entrar no estado de `running`). Para obter mais informações sobre verificações de status do EC2, consulte Verificações de status para as instâncias.

O namespace `AWS/EC2` inclui as métricas de verificação de status a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`StatusCheckFailed`	Relata se a instância foi aprovada tanto na verificação do status da instância quanto na verificação do status do sistema no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Contagem	• Soma • Média
`StatusCheckFailed_Instance`	Informa se a instância foi aprovada na verificação de status de instância no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Contagem	• Soma • Média
`StatusCheckFailed_System`	Informa se a instância foi aprovada na verificação de status de sistema do &; no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada).	Contagem	• Soma • Média

Métrica	Descrição	Unidade	Estatísticas significativas
	Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.		
`StatusCheckFailed_AttachedEBS`	Informa se a instância foi aprovada na verificação de status do EBS anexado no último minuto. Essa métrica pode ser `0` (aprovada) ou `1` (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Contagem	• Soma • Média

O namespace `AWS/EBS` inclui a métrica de verificação de status apresentada a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`VolumeStalledIOCheck`	Observação: somente para instâncias do Nitro. Não publicado para volumes anexados ao Amazon ECS e tarefas do AWS Fargate. Informa se um volume foi aprovado ou reprovado em uma verificação de E/S paralisada no último minuto. Essa métrica pode ser `0` (aprovada) ou `1` (reprovada).	Contagem	• Soma • Média • Mínimo • Máximo

Métricas de espelhamento de tráfego

O namespace `AWS/EC2` inclui métricas para tráfego espelhado. Para obter mais informações, consulte Monitorar o tráfego espelhado usando o Amazon CloudWatch no Guia do Amazon VPC Traffic Mirroring.

Métricas do grupo do Auto Scaling

O namespace `AWS/AutoScaling` inclui métricas para grupos do Auto Scaling. Para obter mais informações, consulte Monitorar métricas do CloudWatch para grupos do Auto Scaling e instâncias no Guia do usuário do Amazon EC2 Auto Scaling.

Dimensões de métrica do Amazon EC2

É possível usar as seguintes dimensões para refinar as métricas listadas nas tabelas anteriores.

Dimensão	Descrição
`AutoScalingGroupName`	Essa dimensão filtra os dados solicitados para todas as instâncias em um grupo de capacidade especificado. Um Grupo de Auto Scaling é uma coleção de instâncias que você define se estiver usando o Auto Scaling. Essa dimensão está disponíve l somente para métricas do Amazon EC2 quando as instâncias estão em um grupo de Auto Scaling. Disponível para instâncias com monitoramento básico ou detalhado habilitado.
`ImageId`	Essa dimensão filtra os dados que você solicita para todas as instâncias executando essa Imagem de máquina da Amazon (AMI) do Amazon EC2. Disponível para instâncias com monitoramento detalhado habilitado.
`InstanceId`	Essa dimensão filtra os dados que você solicita somente para a instância identificada. Isso ajuda você a identificar uma instância exata para monitorar os dados.
`InstanceType`	Essa dimensão filtra os dados que você solicita para todas as instâncias executando esse tipo de instância especificado. Isso ajuda você a categorizar seus dados pelo tipo de instância em execução. Por exemplo, é possível comparar dados de uma instância m1.small e uma instância m1.large para determina r qual delas tem o melhor valor comercial para sua aplicação . Disponível para instâncias com monitoramento detalhado habilitado.

Métricas de uso do Amazon EC2

É possível usar métricas de uso do CloudWatch para fornecer visibilidade sobre o uso de recursos de sua conta. Use essas métricas para visualizar o uso do serviço atual nos gráficos e painéis do CloudWatch.

As métricas de uso do Amazon EC2 correspondem às Service Quotas da AWS. Também é possível configurar alarmes que alertem você quando o uso se aproximar de uma cota de serviço. Para obter mais informações sobre a integração do CloudWatch com o Service Quotas, consulte Métricas de uso da AWS no Guia do usuário do Amazon CloudWatch.

O Amazon EC2 publica as seguintes métricas no namespace `AWS/Usage`.

Métrica	Descrição
`ResourceCount`	O número dos recursos especificados em execução em sua conta. Os recursos são definidos pelas dimensões associadas à métrica. A estatística mais útil para essa métrica é `MAXIMUM`, que representa o número máximo de recursos usados durante o período de um minuto.

As dimensões a seguir são usadas para refinar as métricas de uso publicadas pelo Amazon EC2.

Dimensão	Descrição
`Service`	O nome do serviço da AWS que contém o recurso. Para as métricas de uso do Amazon EC2, o valor dessa dimensão é `EC2`.
`Type`	O tipo de entidade que está sendo relatado. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é `Resource`.
`Resource`	O tipo de recurso que está em execução. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é `vCPU`, que retorna informações sobre as instâncias em execução.

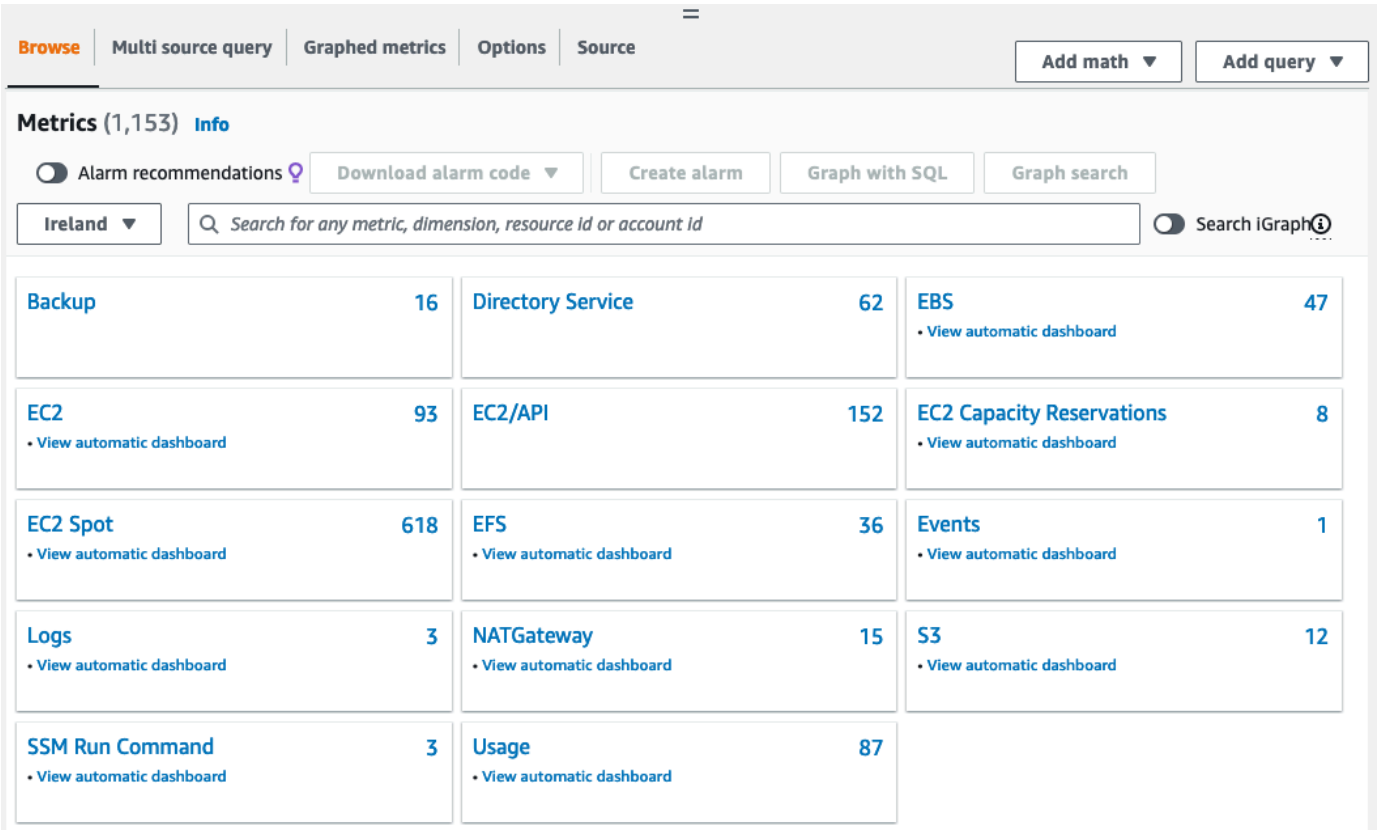
Dimensão	Descrição
`Class`	A classe do recurso que está sendo acompanhado. Para as métricas de uso do Amazon EC2 com `vCPU` como o valor da dimensão `Resource`, os valores válidos são `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` e `X/OnDemand` . Os valores dessa dimensão definem a primeira letra dos tipos de instância relatados pela métrica. Por exemplo, `Standard/OnDemand` retorna informações sobre todas as instâncias em execução com tipos que começam com A, C, D, H, I, M, R, T e Z, e `G/OnDemand` retorna informações sobre todas as instâncias em execução com tipos que começam com G.

Listar métricas usando o console

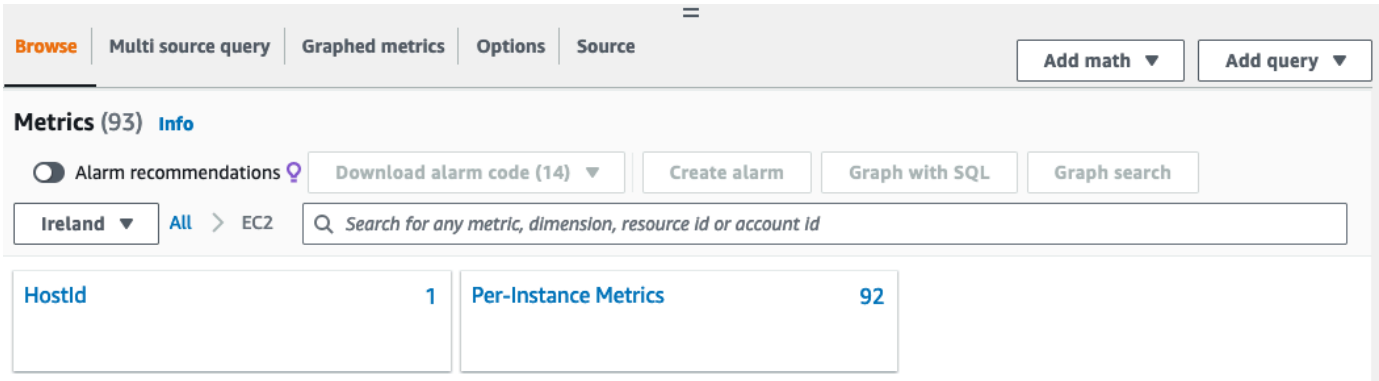
As métricas são agrupadas primeiro pelo namespace e, em seguida, por várias combinações de dimensão dentro de cada namespace. Por exemplo, é possível ver todas as métricas fornecidas pelo Amazon EC2 ou as métricas agrupadas por ID de instância, tipo de instância, ID da imagem (AMI) ou grupo do Auto Scaling.

Para visualizar as métricas disponíveis por categoria (console)

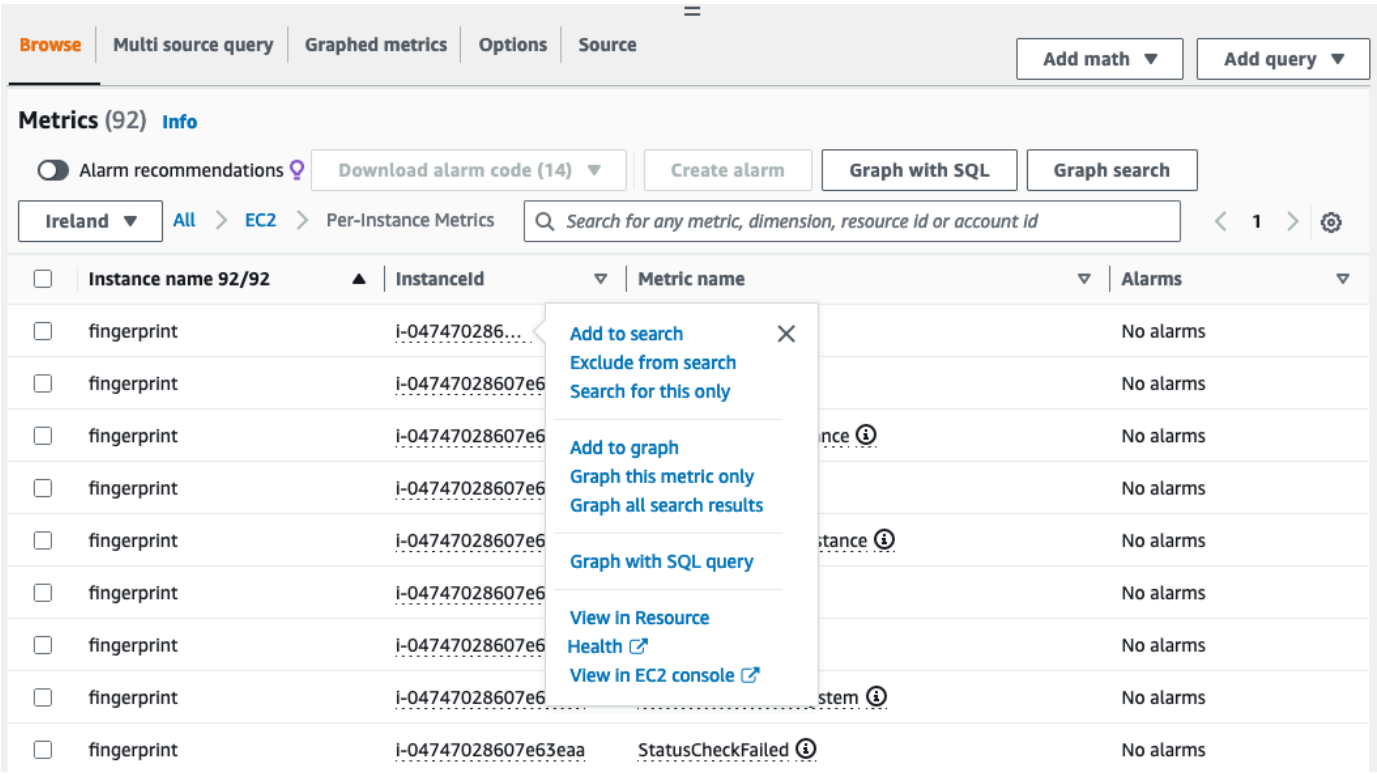
1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, expanda Métricas e escolha Todas as métricas.
3. Escolha o namespace de métricas do EC2.



4. Selecione uma dimensão de métrica (por exemplo, Per-Instance Metrics (Métricas por instância)).



5. Para classificar a métrica, use o cabeçalho da coluna. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica. Para filtrar por recurso, escolha o ID do recurso e, em seguida, escolha Add to search (Adicionar à pesquisa). Para filtrar por métrica, selecione o nome da métrica e, em seguida, escolha Add to search (Adicionar à pesquisa).



Listar métricas usando o AWS CLI

Use o comando list-metrics para listar as métricas do CloudWatch para suas instâncias.

Para listar todas as métricas disponíveis para o Amazon EC2 (AWS CLI)

O exemplo a seguir especifica o namespace `AWS/EC2` para visualizar todas as métricas para o Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

A seguir está um exemplo de saída:

```
{
  "Metrics": [
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
```

```
            }
        ],
        "MetricName": "NetworkOut"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "CPUUtilization"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

Para listar todas as métricas disponíveis para uma instância (AWS CLI)

O exemplo a seguir especifica o namespace `AWS/EC2` e a dimensão `InstanceId` para visualizar os resultados somente para a instância especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
 Name=InstanceId,Value=i-1234567890abcdef0
```

Para listar uma métrica em todas as instâncias (AWS CLI)

O exemplo a seguir especifica o namespace `AWS/EC2` e o nome de uma métrica para visualizar os resultados somente para a métrica especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Instale e configure o agente do CloudWatch usando o console do Amazon EC2 para adicionar métricas adicionais

A instalação e configuração do agente do CloudWatch usando o console do Amazon EC2 está em versão beta para o Amazon EC2 e está sujeita a alterações.

Por padrão, o Amazon CloudWatch fornece métricas básicas, como `CPUUtilization` e `NetworkIn`, para monitorar suas instâncias do Amazon EC2. Para coletar métricas adicionais, você pode instalar o agente do CloudWatch nas suas instâncias do EC2 e, em seguida, configurar o agente para emitir métricas selecionadas. Em vez de instalar e configurar manualmente o agente do CloudWatch em cada instância do EC2, você pode usar o console do Amazon EC2 para fazer isso por você.

Este tópico explica como você pode usar o console do Amazon EC2 para instalar o agente do CloudWatch em suas instâncias e configurar esse agente para emitir métricas selecionadas.

Para ver as etapas manuais desse processo, consulte Instalação do agente do CloudWatch usando o AWS Systems Manager, no Guia do usuário do Amazon CloudWatch. Para obter mais informações sobre o agente do CloudWatch, consulte Coletar métricas, registros e rastreamentos com o agente do CloudWatch.

Tópicos

- Pré-requisitos
- Como funciona
- Custos
- Baixar e configurar o atendente do CloudWatch

Pré-requisitos

Para usar o Amazon EC2 para instalar e configurar o agente do CloudWatch, é necessário atender aos pré-requisitos de usuário e instância descritos nesta seção.

Pré-requisitos da conta

Para usar esse recurso, o usuário ou perfil do console do IAM deve ter as permissões necessárias para usar o Amazon EC2 e as seguintes permissões do IAM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Pré-requisitos da instância

- Estado da instância: `running`
- Sistema operacional com suporte: Linux
- AWS Systems Manager Agent (SSM Agent): Instalado. Duas notas sobre o SSM Agent:
  - O SSM Agent está pré-instalado em algumas imagens de máquina da Amazon (AMIs) fornecidas por terceiros confiáveis AWS. Para obter informações sobre as AMIs com suporte e

as instruções para instalar o SSM Agent, consulte Imagens de máquina da Amazon (AMIs) com o SSM Agent pré-instalado, no Guia do usuário do AWS Systems Manager.

- Se tiver problemas com o SSM Agent, consulte Solução de problemas com o SSM Agent, no Guia do usuário do AWS Systems Manager.

- Permissões do IAM para a instância: as seguintes políticas AWS gerenciadas devem ser adicionadas ao perfil do IAM anexado à instância:
  - AmazonSSMManagedInstanceCore: permite que uma instância use o Systems Manager para instalar e configurar o agente do CloudWatch.
  - CloudWatchAgentServerPolicy: permite que uma instância use o agente do CloudWatch para gravar dados no CloudWatch.

  Para obter informações sobre como adicionar permissões do IAM à sua instância, consulte Usar perfis de instância no Guia do usuário do IAM.

Como funciona

Antes de usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch, você deve se certificar de que seu usuário ou perfil do IAM e as instâncias nas quais você deseja adicionar métricas atendam a determinados pré-requisitos. Em seguida, você pode usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch nas instâncias selecionadas.

Primeiro, atenda aos pré-requisitos

- Você precisa das permissões do IAM necessárias: antes de começar, certifique-se de que seu usuário ou perfil do console tenha as permissões do IAM necessárias para usar esse recurso.
- Instâncias: para usar o recurso, suas instâncias do EC2 devem ser instâncias Linux, ter o SSM Agent instalado, ter as permissões do IAM necessárias e estar em execução.

Em seguida, você poderá usar o recurso

1. Selecione suas instâncias: no console do Amazon EC2, você seleciona as instâncias nas quais instalar e configurar o agente do CloudWatch. Em seguida, inicia o processo escolhendo Configurar agente do CloudWatch.
2. Validar o SSM Agent: o Amazon EC2 verifica se o SSM Agent está instalado e iniciado em cada instância. Todas as instâncias que falharem nessa verificação serão excluídas do processo. O SSM Agent é usado para realizar ações na instância durante esse processo.

3. Valide as permissões do IAM: o Amazon EC2 verifica se cada instância tem as permissões do IAM necessárias para esse processo. Todas as instâncias que falharem nessa verificação serão excluídas do processo. As permissões do IAM permitem que o agente do CloudWatch colete métricas da instância e se integre ao AWS Systems Manager para usar o SSM Agent.
4. Validar o agente do CloudWatch: o Amazon EC2 verifica se o agente do CloudWatch está instalado e em execução em cada instância. Se alguma instância falhar nessa verificação, o Amazon EC2 oferecerá a instalação e a inicialização do agente do CloudWatch para você. O agente do CloudWatch coletará as métricas selecionadas em cada instância quando esse processo for concluído.
5. Selecionar a configuração de métricas: você seleciona as métricas que o agente do CloudWatch emitirá de suas instâncias. Depois de selecionado, o Amazon EC2 armazena um arquivo de configuração no Parameter Store, onde permanece até que o processo seja concluído. O Amazon EC2 excluirá o arquivo de configuração do Parameter Store, a menos que o processo seja interrompido. Observe que, se você não selecionar uma métrica, mas a tiver adicionado anteriormente à sua instância, ela será removida da sua instância quando esse processo for concluído.
6. Atualizar a configuração do agente do CloudWatch: o Amazon EC2 envia a configuração da métrica para o agente do CloudWatch. Essa é a última etapa do processo. Se for bem-sucedida, suas instâncias poderão emitir dados para as métricas selecionadas, e o Amazon EC2 excluirá o arquivo de configuração do Parameter Store.

Custos

As métricas adicionais acrescentadas durante esse processo são cobradas como métricas personalizadas. Para obter mais informações sobre o preço de métricas do CloudWatch, consulte Preço do Amazon CloudWatch.

Baixar e configurar o atendente do CloudWatch

Você pode usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch para adicionar métricas adicionais.

> **Note**
>
> Todas as vezes que você executa esse procedimento, você substitui a configuração existente do agente do CloudWatch. Se você não selecionar uma métrica que tenha sido selecionada anteriormente, ela será removida da instância.

Para instalar e configurar o agente do CloudWatch usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione as instâncias nas quais instalar e configurar o agente do CloudWatch.
4. Escolha Ações, Monitorar e solucionar problemas, Configurar agente do CloudWatch.

   > **Tip**
   >
   > Este recurso ainda não está disponível em todos os Regiões da AWS. Se a opção Configurar agente do CloudWatch não estiver disponível, tente outra região.

5. Para cada etapa do processo, leia o texto do console e escolha Avançar.
6. Para concluir o processo, na etapa final, escolha Concluir.

Obter estatísticas para as métricas das instâncias

É possível obter estatísticas para as métricas do CloudWatch para suas instâncias.

Tópicos

- Visão geral das estatísticas
- Obter estatísticas para uma instância específica
- Agregar estatísticas entre instâncias
- Agregar estatísticas por grupo de Auto Scaling
- Agregar estatísticas por AMI

Visão geral das estatísticas

Estatísticas são agregações de dados de métrica ao longo de períodos especificados. O CloudWatch fornece estatísticas com base nos pontos de dados de métrica fornecidos por seus dados personalizados ou por outros serviços na AWS para o CloudWatch. As agregações são feitas usando o namespace, o nome da métrica, as dimensões e a unidade de medida do ponto de dados no período especificado. A tabela a seguir descreve as estatísticas disponíveis.

Estatística	Descrição
`Minimum`	O valor mais baixo observado durante o período especificado. É possível usar esse valor para determinar baixos volumes de atividade para a sua aplicação
`Maximum`	O valor mais alto observado durante o período especificado. É possível usar esse valor para determinar altos volumes de atividade para a sua aplicação.
`Sum`	Todos os valores enviados para a métrica correspondente, somados. Essa estatística pode ser útil para determinar o volume total de uma métrica.
`Average`	O valor de `Sum` / `SampleCount` durante o período especificado. Ao comparar essa estatística com o `Minimum` e o `Maximum`, é possível determinar o escopo completo de uma métrica e a proximidade da média de uso com o `Minimum` e o `Maximum`. Essa comparação ajuda você a saber quando aumentar ou diminuir seus recursos conforme necessário.
`SampleCount`	A contagem (número) de pontos de dados usados para o cálculo estatístico.
`pNN.NN`	O valor do percentil especificado. É possível especificar qualquer percentil usando até duas casas decimais (por exemplo, p95.45).

Obter estatísticas para uma instância específica

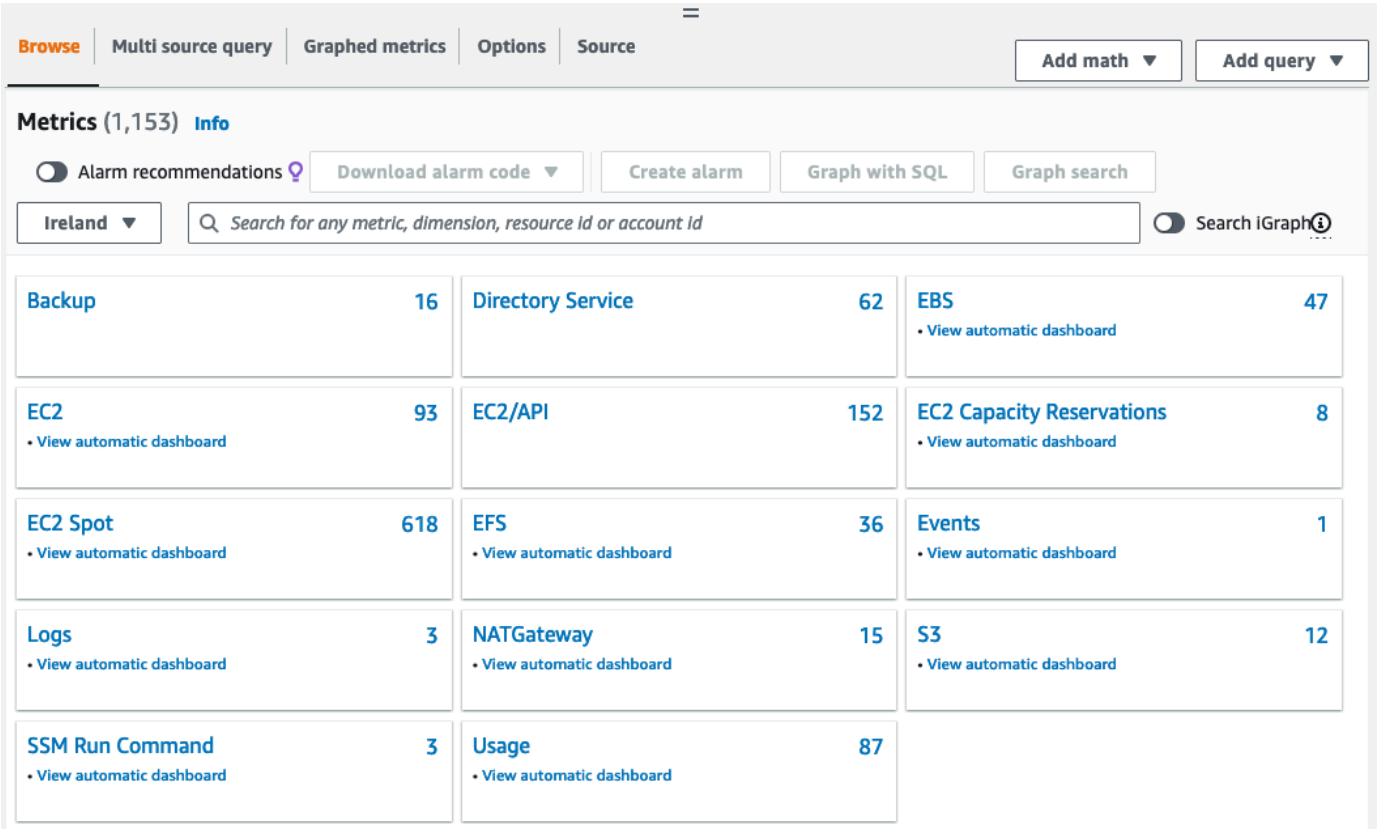
Os exemplos a seguir mostram como usar o AWS Management Console ou a AWS CLI para determinar a utilização horária de CPU de uma instância do EC2 específica.

Requisitos

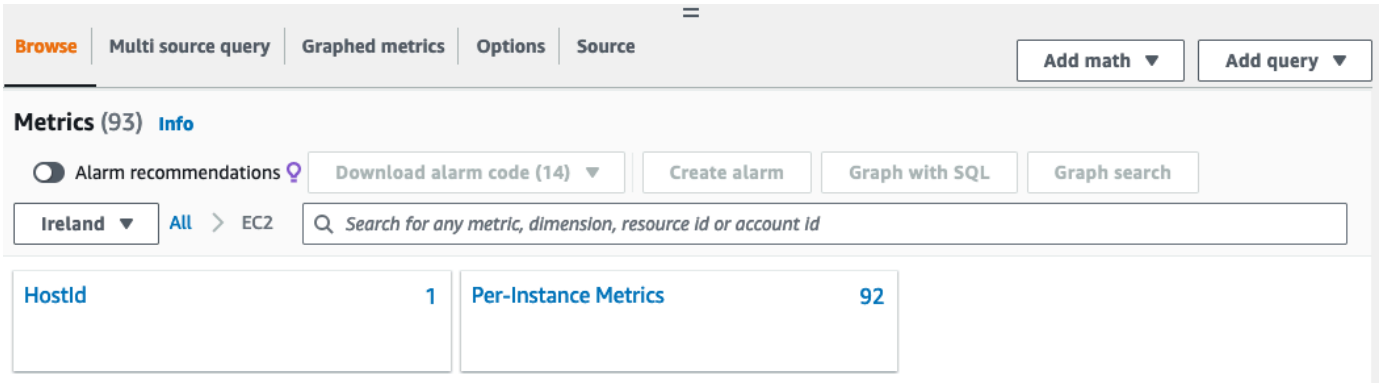
- É necessário ter o ID da instância. É possível obter o ID da instância usando o AWS Management Console ou o comando describe-instances.
- Por padrão, o monitoramento básico é ativado, mas é possível habilitar o monitoramento detalhado. Para ter mais informações, consulte Habilitar ou desabilitar o monitoramento detalhado para instâncias.

Para exibir a utilização de CPU para uma instância específica (console)

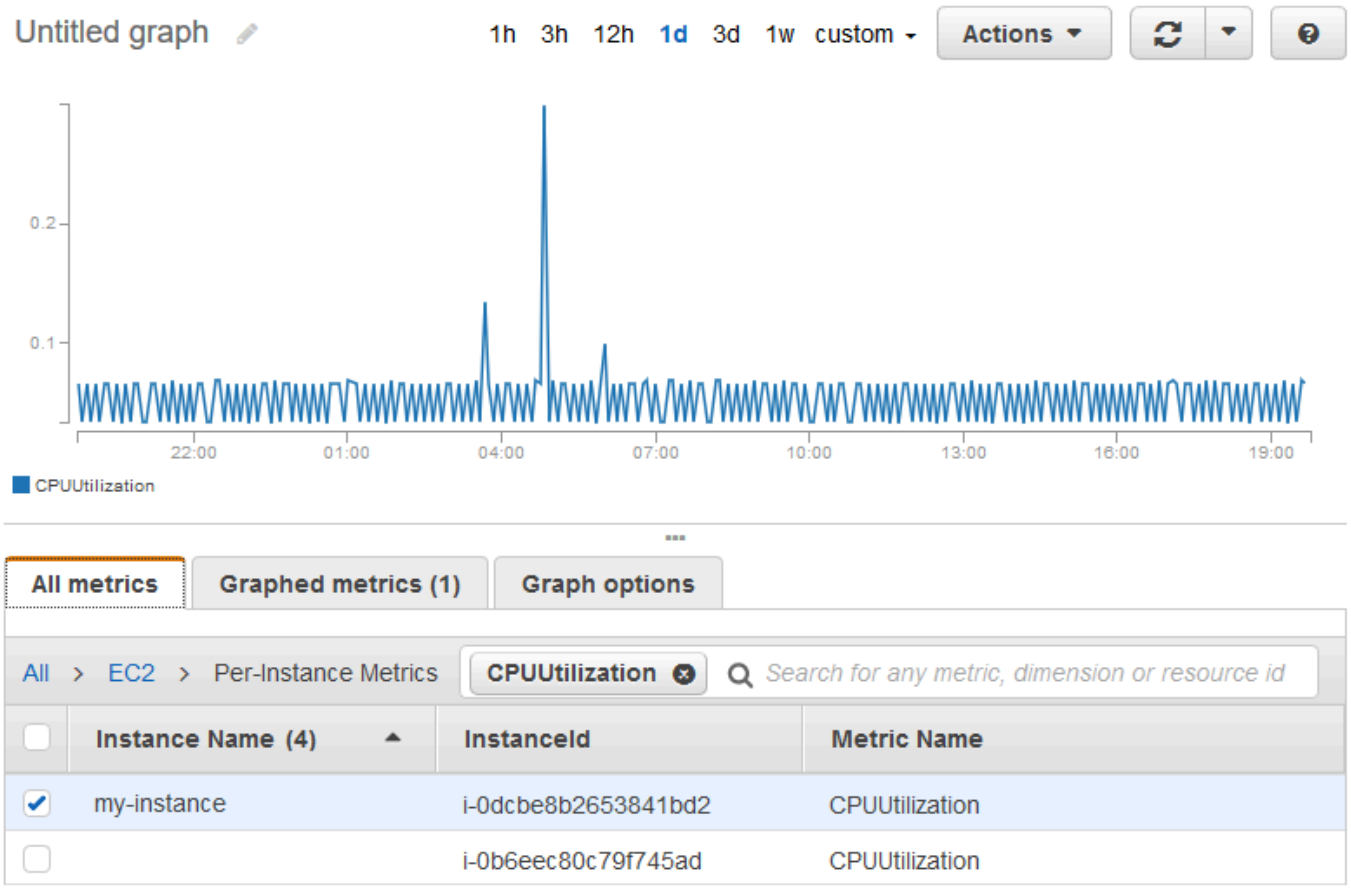
1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace de métricas do EC2.



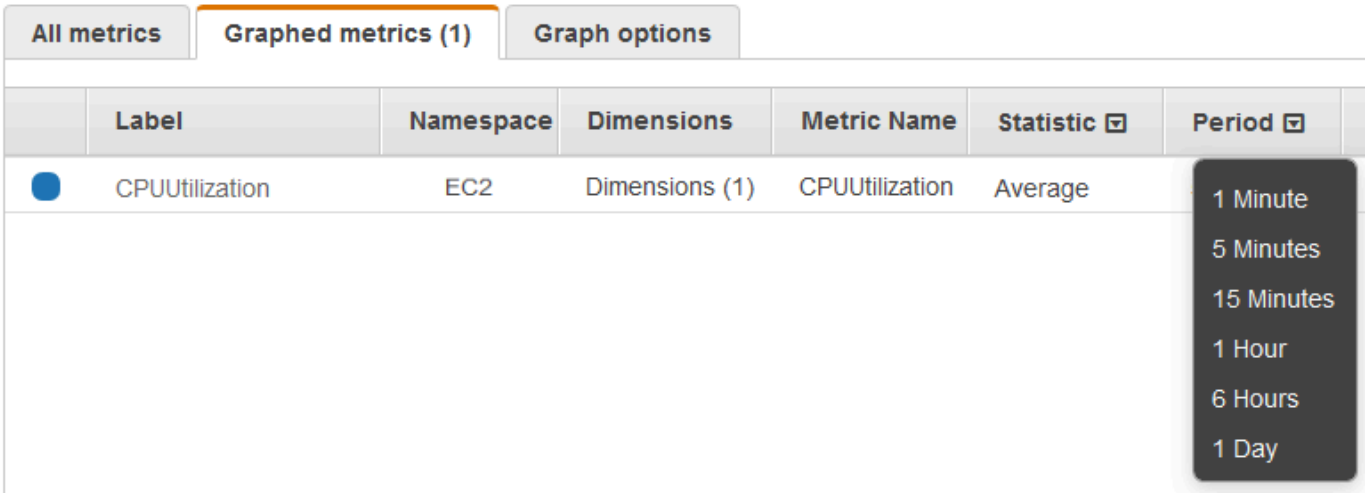
4. Escolha a dimensão Per-Instance Metrics (Métricas por instância).



5. No campo de pesquisa, digite **`CPUUtilization`** e pressione Enter. Escolha a linha da instância específica, que exibe um gráfico da métrica CPUUtilization para a instância. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



6. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.



Para obter a utilização de CPU para uma instância específica (AWS CLI)

Use o comando get-metric-statistics para obter a métrica CPUUtilization da instância específica usando o período e o intervalo de tempo especificados:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

A seguir está um exemplo de saída. Cada valor representa a porcentagem máxima de utilização da CPU para uma única instância do EC2.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Agregar estatísticas entre instâncias

Estatísticas agregadas estão disponíveis para as instâncias que têm o monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados. Antes que seja possível obter estatísticas agregadas em todas as instâncias, é necessário habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos de um minuto.

O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

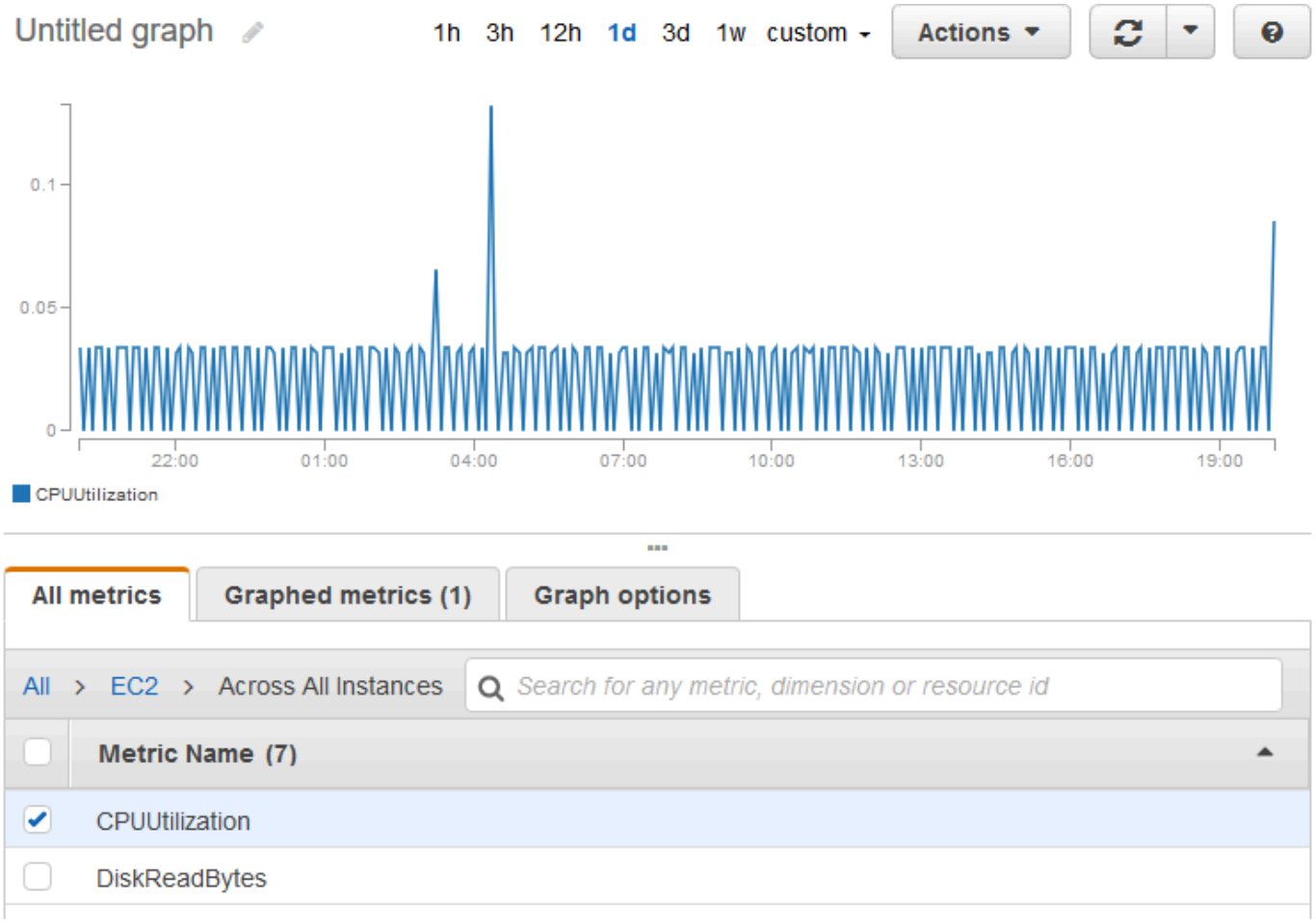
Este exemplo mostra a você como usar o monitoramento detalhado para obter uso médio de CPU para suas instâncias do EC2. Como nenhuma dimensão é especificada, o CloudWatch retorna estatísticas para todas as dimensões no namespace `AWS/EC2`.

> **Important**
>
> Essa técnica para recuperar todas as dimensões em um namespace da AWS não funciona para namespaces personalizados que você publicar no Amazon CloudWatch. Com namespaces personalizados, especifique o conjunto completo de dimensões associadas a um determinado ponto de dados para recuperar estatísticas que incluam o ponto de dados.

Para exibir a utilização média de CPU em suas instâncias (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha Across All Instances (Em todas as instâncias).

4. Escolha a linha que contém CPUUtilization, que exibe um gráfico da métrica para todas as instâncias do EC2. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter a utilização média de CPU em suas instâncias (AWS CLI)

Use o comando get-metric-statistics da seguinte forma para obter a média da métrica CPUUtilization em todas as suas instâncias.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
```

```
    --end-time 2022-10-12T23:18:00
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Agregar estatísticas por grupo de Auto Scaling

É possível agregar estatísticas para as instâncias do EC2 em um grupo do Auto Scaling. O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como recuperar o total de bytes gravados em disco para um grupo do Auto Scaling. O total é calculado para períodos de 1 minuto para um intervalo de 24 horas em todas as instâncias do EC2 no grupo do Auto Scaling especificado.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.

2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Auto Scaling Group (Por grupo de Auto Scaling).
4. Escolha a linha da métrica DiskWriteBytes e o grupo do Auto Scaling específico, que exibe um gráfico da métrica para as instâncias no grupo do Auto Scaling. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).
5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (AWS CLI)

Use o comando get-metric-statistics da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Agregar estatísticas por AMI

É possível agregar estatísticas para suas instâncias com monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados. Antes que seja possível obter estatísticas agregadas em todas as instâncias, é necessário habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos de um minuto.

O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como determinar a utilização média da CPU para todas as instâncias que usam uma imagem de máquina da Amazon (AMI) específica. A média é intervalos de mais de 60 segundos para um período de um dia.

Para exibir a utilização média de CPU por AMI (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Image (AMI) Id (Por ID de imagem (AMI)).
4. Escolha a linha da métrica CPUUtilization e a AMI específica, que exibe um gráfico da métrica para a AMI especificada. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).
5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter utilização média de CPU para um ID de imagem (AWS CLI)

Use o comando get-metric-statistics da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

A seguir está um exemplo de saída. Cada valor representa uma porcentagem de utilização média da CPU para as instâncias do EC2 que executam a AMI especificada.

```
{
```

```
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Representar métricas em gráficos para as instâncias

Depois que executar uma instância, é possível abrir o console do Amazon EC2 e ver os gráficos de monitoramento para a instância na guia Monitoring (Monitoramento). Cada gráfico se baseia em uma das métricas disponíveis do Amazon EC2.

Os gráficos a seguir estão disponíveis:

- Utilização média da CPU (porcentagem)
- Leituras médias do disco (bytes)
- Gravações médias em disco (bytes)
- Rede máxima dentro (bytes)
- Rede máxima fora (bytes)
- Operações de leitura de disco de resumo (contagem)
- Operações de gravação de disco de resumo (contagem)
- Status de resumo (qualquer)
- Instância do status de resumo (contagem)
- Sistema de status de resumo (contagem)

Para mais informações sobre as métricas e os dados que elas fornecem aos gráficos, consulte Listar as métricas disponíveis do CloudWatch para as instâncias.

Represente graficamente métricas usando o console CloudWatch

Também é possível usar o console do CloudWatch para representar graficamente os dados gerados pelo Amazon EC2 e outros serviços da AWS. Para obter mais informações, consulte Representação gráfica de métricas no Guia do usuário do Amazon CloudWatch.

Criar um alarme do CloudWatch para uma instância

É possível criar um alarme do CloudWatch que monitore métricas do CloudWatch de uma de suas instâncias. O CloudWatch enviará automaticamente para você uma notificação quando a métrica atingir um limite especificado. É possível criar um alarme do CloudWatch usando o console do Amazon EC2 ou usar as opções mais avançadas fornecidas pelo console do CloudWatch.

Para criar um alarme usando o console do CloudWatch

Para ver exemplos, consulte Criação de alarmes do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.

Para criar um alarme usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página de detalhes Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar alarme).
5. Em Notificação de alarme, escolha se deseja configurar as notificações do Amazon Simple Notification Service (Amazon SNS). Insira um tópico de Amazon SNS existente ou insira um nome para criar um tópico.
6. Em Ação do alarme, selecione se deseja especificar uma ação a ser feita quando o alarme for acionado. Escolha uma ação na lista.
7. Em Alarm thresholds (Limites de alarme), selecione a métrica e os critérios do alarme. Por exemplo, para criar um alarme que é acionado quando a utilização da CPU atinge 80% por um período de 5 minutos, faça o seguinte:

a. Mantenha as configurações padrão para Agrupar amostras por (Média) e Tipo de dados a amostrar (Utilização da CPU).
b. Escolha **>=** para Alarme quando e insira **0.80** em Por cento.
c. Insira **1** em Período consecutivo e selecione 5 minutos em Período.

8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Criar.

É possível editar suas configurações de alarme do CloudWatch no console do Amazon EC2 ou no console do CloudWatch. Se você quiser excluir seu alarme, poderá fazê-lo a partir no console do CloudWatch. Para obter mais informações, consulte Editar ou excluir um alarme do CloudWatch no Guia do usuário do Amazon CloudWatch.

Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância

Usando as ações de alarme do Amazon CloudWatch, você cria alarmes que automaticamente param, encerram, reinicializam ou recuperam suas instâncias. É possível usar as ações de parada ou encerramento para ajudar a economizar dinheiro quando não precisar mais que uma instância seja executada. É possível usar as ações de reinicialização e recuperação para reinicializar automaticamente essas instâncias ou recuperá-las para um novo hardware caso ocorra um problema no sistema.

> **Note**
>
> Para saber mais sobre alarmes de faturamento e custos do Amazon CloudWatch, consulte Faturamento e custos do CloudWatch no Guia do usuário do Amazon CloudWatch.

A função `AWSServiceRoleForCloudWatchEvents` ligado ao serviço permite que a AWS execute ações de alarme em seu nome. A primeira vez que você criar um alarme no AWS Management Console, na AWS CLI ou na API do IAM, o CloudWatch cria o perfil vinculado ao serviço para você.

Há várias situações nas quais é possível querer interromper ou encerrar sua instância automaticamente. Por exemplo, é possível ter instâncias dedicadas a trabalhos de processamento de folha de pagamento em lote ou tarefas de computação científica que são executadas por um período

e, em seguida, concluem seu trabalho. Em vez de permitir que essas instâncias fiquem ociosas (e acumulem cobranças), é possível interrompê-las ou encerrá-las, o que pode ajudá-lo a fazer uma economia. A principal diferença entre usar as ações de alarme de interrupção e encerramento é que é possível facilmente iniciar uma instância interrompida se precisar executá-la novamente mais tarde e manter o mesmo ID de instância e volume do dispositivo raiz. No entanto, não é possível iniciar uma instância encerrada. Em vez disso, é necessário executar uma nova instância. Quando uma instância é interrompida ou encerrada, os dados nos volumes de armazenamento da instância são perdidos.

É possível adicionar as ações de interrupção, encerramento, reinicialização ou recuperação a qualquer alarme definido em uma métrica por instância do Amazon EC2, incluindo métricas de monitoramento básico e detalhado fornecidas pelo Amazon CloudWatch (no namespace `AWS/EC2`), bem como todas as métricas personalizadas que incluem a dimensão `InstanceId`, desde que seu valor se refira a uma instância do Amazon EC2 em execução.

> **Important**
>
> Os alarmes de verificação de status podem entrar temporariamente no estado `INSUFFICIENT_DATA` se faltarem pontos de dados de métricas. Embora raro, isso pode acontecer quando há uma interrupção nos sistemas de relatórios de métricas, mesmo quando uma instância está íntegra. Recomendamos que você trate o estado `INSUFFICIENT_DATA` como dados ausentes em vez de uma violação de alarme, especialmente ao configurar o alarme para parar, encerrar, reinicializar ou recuperar uma instância.

Suporte a consoles

É possível criar alarmes usando o console do Amazon EC2 ou do CloudWatch. Os procedimentos nesta documentação usam o console do Amazon EC2. Para procedimentos que usam o console do CloudWatch, consulte Criar alarmes que param, encerram, reinicializam ou recuperam uma instância no Guia do usuário do Amazon CloudWatch.

Permissões

Você deve ter a permissão `iam:CreateServiceLinkedRole` para criar ou modificar um alarme que executa as ações de alarme do EC2. A função de serviço é uma função do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir

um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Conteúdo

- Adicionar ações de interrupção a alarmes do Amazon CloudWatch
- Adicionar ações de encerramento a alarmes do Amazon CloudWatch
- Adicionar ações de reinicialização a alarmes do Amazon CloudWatch
- Adicionar ações de recuperação a alarmes do Amazon CloudWatch
- Usar o console do Amazon CloudWatch para visualizar o histórico do alarme e da ação
- Cenários de ação do alarme do Amazon CloudWatch

Adicionar ações de interrupção a alarmes do Amazon CloudWatch

É possível criar um alarme que pare uma instância do Amazon EC2 quando o limite for atingido. Por exemplo, é possível executar instâncias de desenvolvimento ou teste e ocasionalmente se esquecer de desativá-las. É possível criar um alarme que seja acionado quando o percentual médio de utilização da CPU for inferior a 10% em 24 horas, sinalizando que ela está ociosa e não mais em uso. É possível ajustar o limite, a duração e o período para atender às suas necessidades, além de poder adicionar uma notificação do Amazon Simple Notification Service (Amazon SNS) para receber um e-mail quando o alarme for acionado.

As instâncias que usam um volume do Amazon EBS como dispositivo raiz podem ser interrompidas ou encerradas, enquanto as instâncias que usam o armazenamento de instância como dispositivo raiz só podem ser encerradas. Os dados nos volumes de armazenamento de instância são perdidos quando a instância é interrompida ou encerrada.

Para criar um alarme para parar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicativo para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   c. Alterne em Ação alarme e escolha Parar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).

   e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique <= e 10%.

   f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 1 período consecutivo de 5 minutos.

   g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

      > **Note**
      >
      > É possível ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

   h. Escolha Criar.

Adicionar ações de encerramento a alarmes do Amazon CloudWatch

É possível criar um alarme que encerre uma instância do EC2 automaticamente quando um certo limite for atingido (desde que a proteção contra encerramento não esteja ativada para a instância). Por exemplo, é possível encerrar uma instância quando ela tiver concluído seu trabalho e não precisar mais dela. Se você quiser usar a instância posteriormente, pare-a em vez de encerrá-la. Os dados nos volumes de armazenamento de instância são perdidos quando a instância é encerrada.

Para obter informações sobre a habilitação e a desabilitação da proteção contra encerramento de uma instância, consulte Habilitar a proteção contra encerramento.

Para criar um alarme para encerrar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicativo para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   c. Alterne em Ação alarme e escolha Encerrar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).

   e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique **=>** e 10 por cento.

   f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 24 períodos consecutivos de 1 hora.

   g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

> **Note**
>
> É possível ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

h. Escolha Criar.

Adicionar ações de reinicialização a alarmes do Amazon CloudWatch

É possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e reinicialize automaticamente a instância. A ação de alarme de reinicialização é recomendada para falhas de verificação de integridade da instância (ao contrário da ação de alarme de recuperação, que é adequado para falhas de verificação de integridade do sistema). Reinicializar a instância equivale a reinicializar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reinicializar sua instância. Quando você reinicializa uma instância, ela permanece no mesmo host físico, para que sua instância mantenha seu nome DNS público, o endereço IP privado e os dados em seus volumes de armazenamento de instância.

A reinicialização de uma instância não inicia uma nova hora de faturamento de instância (com uma cobrança mínima de um minuto), diferente do que acontece na interrupção e na reinicialização da instância. Os dados nos volumes de armazenamento de instância são retidos quando a instância é reinicializada. Os volumes de armazenamento de instâncias devem ser remontados no sistema de arquivos após uma reinicialização. Para ter mais informações, consulte Reinicializar a instância.

> **Important**
>
> Para evitar um comportamento de disputa entre as ações de reinicialização e recuperação, evite configurar o mesmo número de períodos de avaliação para um alarme de reinicialização e um alarme de recuperação. Recomendamos que você defina alarmes de reinicialização para três períodos de avaliação de um minuto cada. Para obter mais informações, consulte Avaliar um alarme no Guia do usuário do Amazon CloudWatch.

Para criar um alarme para reinicializar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicativo para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   c. Alterne em Ação alarme e escolha Reinicializar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: instance (Falha na verificação de status: instância).

   e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, digite 3 períodos consecutivos de 5 minutos.

   f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

   g. Escolha Criar.

Adicionar ações de recuperação a alarmes do Amazon CloudWatch

É possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2. Se a instância for invalidada devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para corrigi-lo, será possível recuperar a instância automaticamente. Instâncias encerradas não podem ser recuperadas. Uma instância recuperada é idêntica à instância

original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados de instância.

O CloudWatch impede que você adicione uma ação de recuperação a um alarme que esteja em uma instância que não oferece suporte a ações de recuperação.

Quando o alarme `StatusCheckFailed_System` for acionado e a ação de recuperação for iniciada, você será notificado pelo tópico do Amazon SNS que escolheu ao criar o alarme e a ação de recuperação associada. Durante a recuperação da instância, a instância será migrada durante uma reinicialização da instância e todos os dados na memória serão perdidos. Quando o processo é concluído, as informações serão publicadas no tópico do SNS que você tiver configurado para o alarme. Qualquer pessoa que estiver inscrita neste tópico do SNS receberá uma notificação por e-mail com o status da tentativa de recuperação e instruções adicionais. Você perceberá uma reinicialização de instância na instância recuperada.

> **Note**
>
> A ação de recuperação pode ser usada somente com `StatusCheckFailed_System`, não com `StatusCheckFailed_Instance`.

Os problemas a seguir podem causar falha nas verificações de status do sistema:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

A ação de recuperação é compatível somente nas instâncias com as características a seguir. Para ter mais informações, consulte Resiliência de instância.

Se a sua instância tiver um endereço IP público, ela reterá o endereço IP público após a recuperação.

> **Important**
>
> Para evitar um comportamento de disputa entre as ações de reinicialização e recuperação, evite configurar o mesmo número de períodos de avaliação para um alarme de

reinicialização e um alarme de recuperação. É recomendável que você defina os alarmes de recuperação para dois períodos de avaliação de um minuto cada. Para obter mais informações, consulte Avaliar um alarme no Guia do usuário do Amazon CloudWatch.

Para criar um alarme para recuperar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (
   
) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicativo para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   > **Note**
   >
   > Os usuários devem se inscrever no tópico do SNS especificado para receber notificações por email quando o alarme for acionado. O Usuário raiz da conta da AWS sempre recebe notificações por e-mail quando ocorrem ações de recuperação automática de instância, mesmo que um tópico do SNS não esteja especificado ou o usuário raiz não esteja inscrito no tópico de SNS especificado.

   c. Alterne em Ação alarme e escolha Recuperar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: system (Falha na verificação de status: sistema).

e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, digite 2 períodos consecutivos de 5 minutos.

f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

g. Escolha Criar.

Usar o console do Amazon CloudWatch para visualizar o histórico do alarme e da ação

É possível visualizar o histórico de alarmes e ações no console do Amazon CloudWatch. O Amazon CloudWatch mantém as últimas duas semanas de histórico de alarmes e ações.

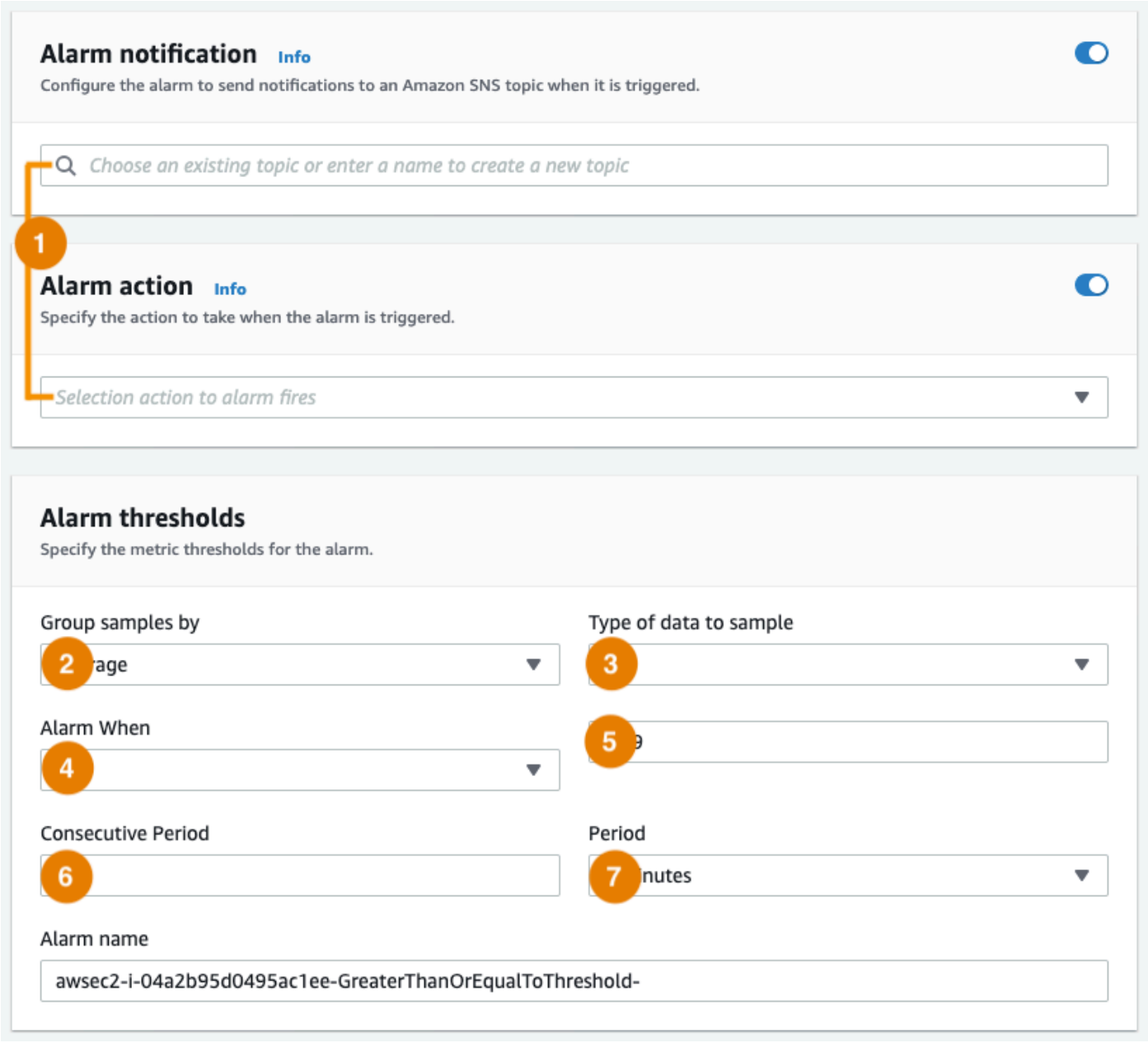
Para visualizar o histórico de alarmes e ações acionados (console do CloudWatch)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Alarmes.
3. Selecione um alarme.
4. A guia Detalhes mostra a transição de estado mais recente juntamente com os valores de tempo e métrica.
5. Escolha a guia Histórico para visualizar as entradas mais recentes do histórico.

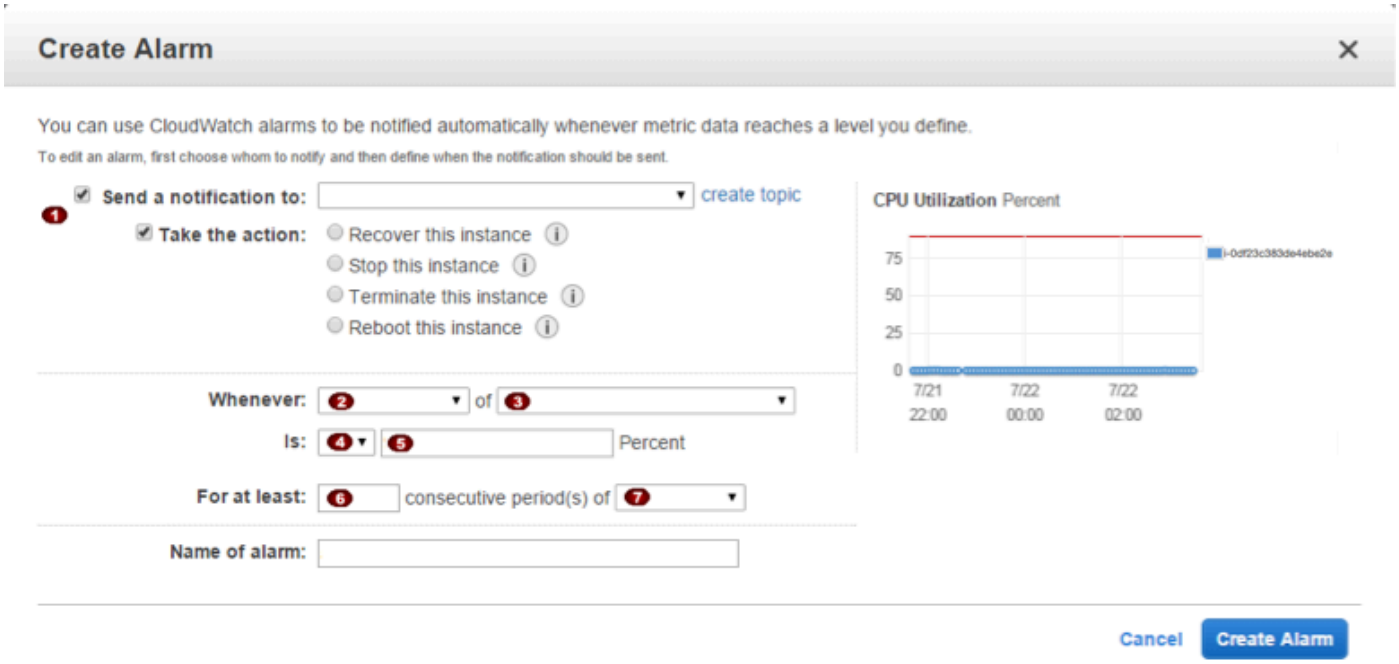
Cenários de ação do alarme do Amazon CloudWatch

É possível usar o console do Amazon EC2 para criar as ações de alarme que interrompem ou encerram uma instância do Amazon EC2 quando determinadas circunstâncias são atendidas. Na captura de tela a seguir da página do console onde você define as ações de alarme, nós numeramos as configurações. Nós também numeramos as configurações nos cenários a seguir, para ajudá-lo a criar as ações apropriadas.

New console


Alarm notification Info
Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.
Choose an existing topic or enter a name to create a new topic
1
Alarm action Info
Specify the action to take when the alarm is triggered.
Selection action to alarm fires
Alarm thresholds
Specify the metric thresholds for the alarm.
Group samples by
2
Type of data to sample
3
Alarm When
4
5
Consecutive Period
6
Period
7
Alarm name
awsec2-i-04a2b95d0495ac1ee-GreaterThanOrEqualToThreshold-

Old console



Cenário 1: interromper instâncias de teste e desenvolvimento ociosas

Crie um alarme que interrompa uma instância usada para desenvolvimento ou teste de software quando estiver inativa pelo menos uma hora.

Configuração	Valor
1	Interromper
2	Máximo
3	Utilização da CPU
4	<=
5	10%
6	1
7	1 hora

Cenário 2: interromper instâncias ociosas

Crie um alarme que interrompa uma instância e envie um e-mail quando a instância estiver inativa por 24 horas.

Configuração	Valor
1	Interromper e enviar e-mail
2	Média
3	Utilização da CPU
4	<=
5	5%
6	24
7	1 hora

Cenário 3: enviar e-mail em servidores Web com tráfego incomumente alto

Crie um alarme que envie o e-mail quando uma instância ultrapassar 10 GB de tráfego de rede de saída por dia.

Configuração	Valor
1	E-mail
2	Soma
3	Saída de rede
4	>
5	10 GB
6	24

Configuração	Valor
7	1 hora

Cenário 4: interromper servidores Web com tráfego incomumente alto

Crie um alarme que pare uma instância e envie uma mensagem de texto (SMS) se o tráfego de saída exceder 1 GB por hora.

Configuração	Valor
1	Parar e enviar SMS
2	Soma
3	Saída de rede
4	>
5	1 GB
6	1
7	1 hora

Cenário 5: Interromper uma instância danificada

Crie um alarme que interrompa uma instância em falhe três verificações de status consecutivas (executadas em intervalos de 5 minutos).

Configuração	Valor
1	Interromper
2	Média
3	Falha na verificação de status: sistema
4	-

Configuração	Valor
5	-
6	1
7	15 minutos

Cenário 6: Encerrar instâncias quando os trabalhos de processamento em lote estiverem concluídos

Crie um alarme que encerre uma instância que execute trabalhos em lote quando não estiver mais enviando os dados dos resultados.

Configuração	Valor
1	Encerrar
2	Máximo
3	Saída de rede
4	<=
5	100,000 bytes
6	1
7	5 minutos

Automatizar o Amazon EC2 usando o EventBridge

Você pode usar o Amazon EventBridge para automatizar seus Serviços da AWS e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicações ou alterações de recursos. Os eventos dos serviços da AWS são entregues ao EventBridge quase em tempo real. É possível criar regras para indicar os eventos de seu interesse e quais ações deverão ser executadas quando um evento corresponder a uma regra. Ações que podem ser automaticamente acionadas incluem:

- Invocar uma função do AWS Lambda
- Invocar o Run Command do Amazon EC2
- Retransmitir o evento para o Amazon Kinesis Data Streams
- Ativar máquina de estado do AWS Step Functions
- Notificar um tópico do Amazon SNS
- Notificar uma fila do Amazon SQS

Veja a seguir exemplos de como utilizar o EventBridge com o Amazon EC2:

- Ative uma função Lambda sempre que uma instância entrar no estado de execução.
- Notifique um tópico do Amazon SNS quando um volume do Amazon EBS for criado ou modificado.
- Envie um comando para uma ou mais instâncias do Amazon EC2 usando o Run Command do Amazon EC2 sempre que um evento ocorrer em outro produto da AWS.

Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Tipos de eventos do Amazon EC2

O Amazon EC2 oferece suporte aos seguintes tipos de evento:

- Alteração do estado da AMI do EC2
- Notificação de alteração de estado do EC2 Fast Launch
- Erro de frota do EC2
- Informações de frota do EC2
- Alteração da instância da frota do EC2
- Alteração da solicitação de instância spot da frota do EC2
- Alteração do estado da frota do EC2
- Recomendação de redistribuição de instâncias do EC2
- Notificação de alteração do estado da instância do EC2
- Erro na frota spot do EC2
- Informações sobre a frota spot do EC2
- Alteração da instância da frota spot do EC2
- Alteração da solicitação de instância spot da frota spot do EC2

- Alteração do estado da frota spot do EC2
- Alerta de interrupção da instância spot do EC2
- Atendimento de solicitação de instância spot do EC2
- Notificação de subutilização de ODCR do EC2

Para obter informações sobre os tipos de evento compatíveis com o Amazon EBS, consulte EventBridge para Amazon EBS.

Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail

A API do Amazon EC2 está integrada ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por um perfil ou por um AWS service (Serviço da AWS). O CloudTrail captura todas as chamadas de API para o Amazon EC2 como eventos, incluindo as chamadas do console e de chamadas de código para as operações de API. Ao usar as informações coletadas pelo CloudTrail, é possível determinar a solicitação que foi feita à API do Amazon EC2, o endereço IP do qual a solicitação foi feita, o momento em que ela foi feita e assim por diante.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre a API do Amazon EC2 no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no Amazon EC2 e no Amazon EBS, ela é registrada em um evento do CloudTrail com outros eventos de AWS service (Serviço da AWS) no Histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na Conta da AWS, incluindo eventos do Amazon EC2 e do Amazon EBS, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Criar uma trilha para a sua Conta da AWS

- Integrações de AWS service (Serviço da AWS) com logs do CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Amazon EC2 e as ações de gerenciamento do Amazon EBS são registradas pelo CloudTrail e documentadas na Amazon EC2 API Reference (Referência da API do Amazon EC2). Por exemplo, as chamadas para as ações RunInstances, DescribeInstances ou CreateImage geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou de usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Compreensão das entradas do arquivo de log da API do Amazon EC2

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O arquivo de log a seguir mostra que um usuário encerrou uma instância.

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
```

```
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Uso do AWS CloudTrail para auditar conexões realizadas ao usar o EC2 Instance Connect

Use o AWS CloudTrail para auditar os usuários que se conectam às suas instâncias por meio do EC2 Instance Connect.

Para auditar a atividade do SSH por meio do EC2 Instance Connect usando o console do AWS CloudTrail

1. Abra o console do CloudTrail em https://console.aws.amazon.com/cloudfront/.
2. Verifique se você está na região correta.
3. No painel de navegação, selecione Event history (Histórico de eventos).
4. Para Filter (Filtro), selecione Event source (Fonte do evento), ec2-instance-connect.amazonaws.com.
5. (Opcional) Para Time range (Intervalo de tempo), selecione um intervalo de tempo.
6. Selecione o ícone Refresh events (Atualizar eventos).
7. A página exibe os eventos que correspondem às chamadas de API de SendSSHPublicKey. Expanda um evento usando a seta para visualizar detalhes adicionais, como nome de usuário e chave de acesso da AWS usada para fazer a conexão SSH e o endereço IP de origem.
8. Para exibir todas as informações do evento no formato JSON, selecione View event (Exibir evento). O campo requestParameters contém o ID da instância de destino, o nome do usuário do sistema operacional e a chave pública usada para fazer a conexão do SSH.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
```

```
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```

Se você tiver configurado a conta da AWS para coletar eventos do CloudTrail em um bucket do S3, poderá fazer download e auditar as informações de forma programática. Para obter mais informações, consulte Obter e visualizar arquivos de log do CloudTrail no Guia do usuário do AWS CloudTrail.

Monitorar s aplicações .NET e SQL Server com o CloudWatch Application Insights

O CloudWatch Application Insights for .NET e SQL Server ajuda você a monitorar as aplicações .NET e SQL Server que usam instâncias do Amazon EC2 juntamente com outros recursos de aplicações da AWS. Ele identifica e configura os principais logs de métricas e alarmes na pilha de tecnologia e nos recursos da aplicação (por exemplo, banco de dados Microsoft SQL Server, servidores Web (IIS) e de aplicações, SO, load balancers e filas). Ele monitora continuamente os logs e as métricas para detectar e correlacionar anomalias e erros. Quando erros e anomalias são detectados, o Application Insights gera o CloudWatch Events que é possível usar para configurar notificações ou executar ações. Para auxiliar na solução de problemas, ele cria painéis automatizados para os problemas detectados, que incluem anomalias de métricas correlacionadas e erros de log com informações adicionais para indicar a potencial causa do problema. Os painéis

automatizados ajudam você a tomar medidas corretivas rápidas para manter suas aplicações íntegras e para evitar o impacto nos usuários finais do sua aplicação.

Para visualizar uma lista completa de logs e métricas compatíveis, consulte Logs and Metrics Supported by Amazon CloudWatch Application Insights (Logs e métricas compatíveis com o Amazon CloudWatch Application Insights).

Informações fornecidas sobre os problemas detectados:

- Um breve resumo do problema
- A data e a hora de início do problema
- A gravidade do problema: High/Medium/Low (Alta/média/baixa)
- O status do problema detectado: In-progress/Resolved (Em andamento/resolvido)
- Insights: insights gerados automaticamente sobre o problema detectado e a possível causa
- Feedback sobre os insights: o feedback que você forneceu sobre a utilidade dos insights gerados pelo CloudWatch Application Insights para .NET e SQL Server
- Observações relacionadas: uma visão detalhada das anomalias da métrica e dos trechos do erro de logs relevantes relacionados ao problema em vários componentes da aplicação

Feedback

É possível fornecer feedback em relação aos insights gerados automaticamente sobre problemas detectados designando-os como úteis ou não úteis. Seu feedback sobre os insights com o diagnóstico da aplicação (anomalias da métrica e exceções de log) são usados para melhorar a futura detecção de problemas semelhantes.

Para obter mais informações, consulte a documentação CloudWatch Application Insights (Insights sobre aplicações do CloudWatch) no Guia do usuário do Amazon CloudWatch.

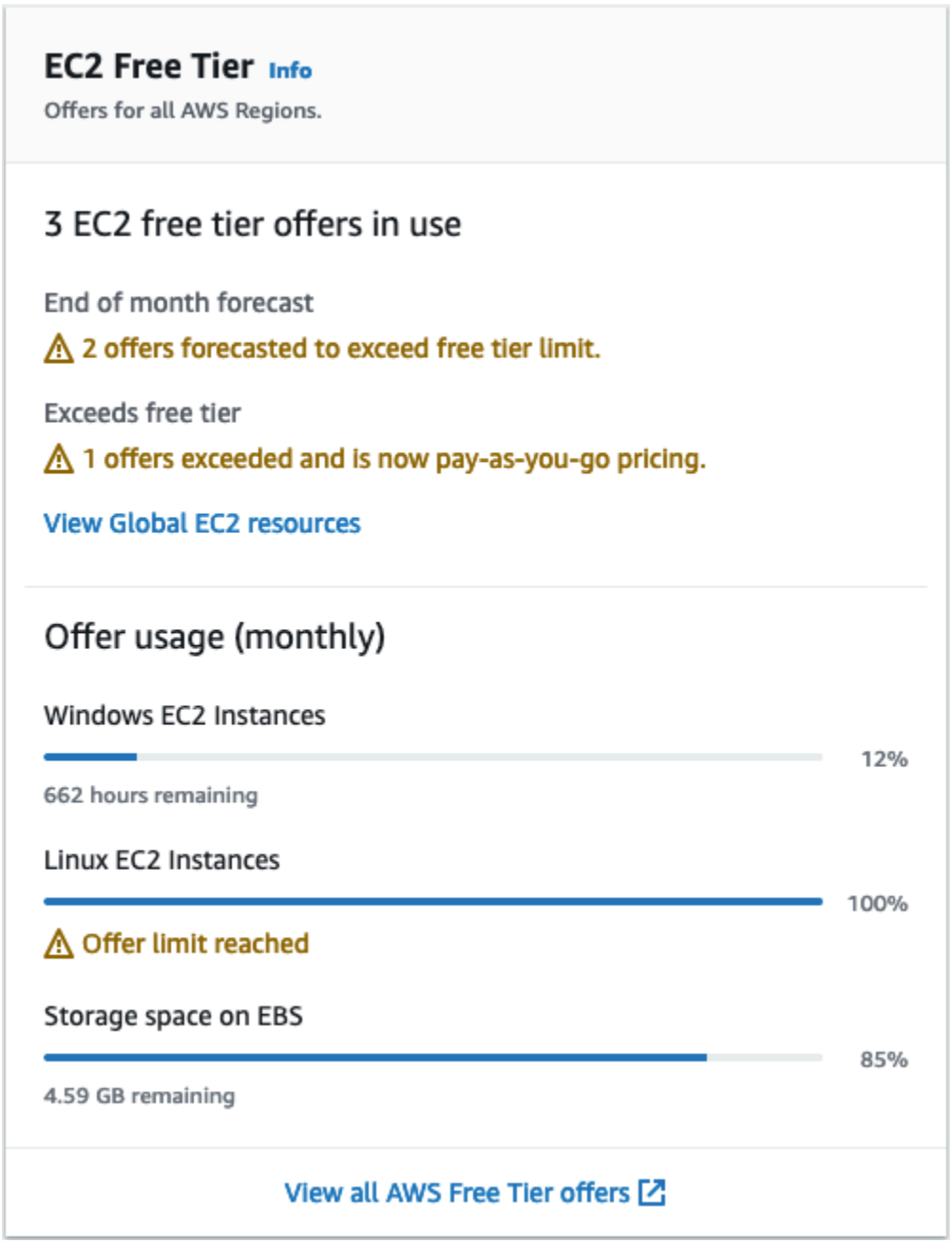
Acompanhamento do uso do nível gratuito para o Amazon EC2

Você poderá usar o Amazon EC2 sem incorrer em nenhum custo se for cliente da AWS há menos de 12 meses e permanecer dentro dos limites de uso do Nível gratuito da AWS. É importante acompanhar seu uso do nível gratuito para evitar surpresas na cobrança. Se você exceder os limites do nível gratuito, incorrerá nas tarifas padrão para pagamento de acordo com o uso.

> **Note**
>
> Se você for cliente da AWS há mais de 12 meses, não estará mais qualificado para usar o nível gratuito e não verá a caixa Nível gratuito do EC2, descrita no procedimento a seguir.

Para acompanhar seu uso do nível gratuito

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Localize a caixa Nível gratuito do EC2 (no canto superior direito).



4. Na caixa Nível gratuito do EC2, verifique seu uso do nível gratuito, da seguinte maneira:

   - Em Ofertas do nível gratuito do EC2 em uso, anote os avisos:
     - Previsão de fim do mês: esse é um aviso de que você incorrerá em custos este mês se continuar com seu padrão de uso atual.
     - Excede o nível gratuito: esse é um aviso de que você excedeu os limites do nível gratuito e já está incorrendo em custos.

- Em Uso da oferta (mensal), anote seu uso de instâncias do Linux, instâncias do Windows e armazenamento do EBS. A porcentagem indica quanto você usou este mês dos seus limites de nível gratuito. Se estiver em 100%, você incorrerá em custos para continuar a usar.

> **Note**
>
> Essas informações só aparecem depois que você criou uma instância. Porém, as informações de uso não são atualizadas em tempo real; elas são atualizadas três vezes ao dia.

5. Para evitar incorrer em custos adicionais, exclua todos os recursos que estão sendo cobrados agora ou que serão cobrados se você exceder o limite de uso do nível gratuito.

   - Para obter instruções sobre a exclusão da instância, avance para a próxima etapa deste tutorial.
   - Para verificar se você tem recursos em outras regiões que possam estar gerando custos, na caixa Nível gratuito do EC2, escolha Exibir recursos globais do EC2 para abrir a Visão global do EC2. Para ter mais informações, consulte Amazon EC2 Global View.

6. Para visualizar seu uso dos recursos de todos os Serviços da AWSNível gratuito da AWS, na parte inferior da caixa Nível gratuito do EC2, escolha Exibir todas as ofertas do Nível gratuito da AWS. Para obter mais informações, consulte Usar o Nível gratuito da AWS no Guia do usuário do Faturamento da AWS.

Redes no Amazon EC2

A Amazon VPC permite que você execute recursos da AWS, como as instâncias do Amazon EC2, em uma rede virtual dedicada à conta da AWS, conhecida como uma nuvem virtual privada (VPC). Ao executar uma instância, é possível selecionar uma sub-rede na VPC. A instância é configurada com uma interface de rede primária, que é uma placa de rede virtual lógica. A instância recebe um endereço IP privado primário do endereço IPv4 da sub-rede e é atribuída à interface da rede primária.

É possível controlar se a instância recebe um endereço IP público do grupo da Amazon de endereços IP públicos. O endereço IP público de uma instância é associado à sua instância somente até que ela seja interrompida ou encerrada. Se você precisar de um endereço IP público persistente, poderá alocar um endereço IP elástico para sua conta da AWS e associá-lo a uma instância ou uma interface de rede. Um endereço IP elástico permanece associado à sua conta AWS até que você o libere e possa movê-lo de uma instância à outra, conforme necessário. É possível trazer o seu próprio intervalo de endereços IP para sua conta AWS, onde ele aparece como um grupo de endereços e, em seguida, alocar endereços IP elásticos do seu grupo de endereços.

Para aumentar a performance da rede e reduzir a latência, é possível executar instâncias em um grupo de posicionamento. É possível obter uma performance significativamente superior de pacotes por segundo (PPS) usando redes aprimoradas. É possível acelerar aplicações de computação e machine learning de alta performance usando um Elastic Fabric Adapter (EFA), que é um dispositivo de rede que pode ser anexado a um tipo de instância compatível.

Recursos

- A VPC abrange as zonas de disponibilidade e a zona Wavelength.
- Endereçamento IP de instâncias do Amazon EC2
- Tipos de nome de host de instância do Amazon EC2
- Traga seus próprios endereços IP (BYOIP) no Amazon EC2
- Endereços IP elásticos
- Interfaces de rede elástica
- Largura de banda de rede de instâncias do Amazon EC2
- Redes aperfeiçoadas no Amazon EC2
- Elastic Fabric Adapter
- Topologia da instância do Amazon EC2

- Grupos de posicionamento
- Unidade de transmissão máxima (MTU) de rede para a instância do EC2
- Nuvens privadas virtuais para as instâncias do EC2

A VPC abrange as zonas de disponibilidade e a zona Wavelength.

O Amazon EC2 está hospedado em vários locais no mundo todo. Esses locais são compostos por Regiões da AWS, zonas de disponibilidade, zonas locais, AWS Outposts e zonas do Wavelength.

- Cada Região é uma área geográfica separada.
- As zonas de disponibilidade são vários locais isolados dentro de cada região.
- As zonas locais fornecem a capacidade de colocar recursos, como computação e armazenamento, em vários locais mais próximos dos usuários finais.
- O AWS Outposts leva serviços, infraestrutura e modelos operacionais nativos da AWS a praticamente qualquer data center, espaço de colocalização ou on-premises.
- As zonas do Wavelength permitem que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos 5G e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação.

A AWS opera data centers de última geração com alta disponibilidade. Embora sejam raras, podem ocorrer falhas que afetam a disponibilidade das instâncias que estão no mesmo local. Se você hospedar todas as suas instâncias em um único local afetado por uma falha, nenhuma delas ficará disponível.

Para ajudar a determinar qual implantação é melhor para você, consulte as Perguntas frequentes do AWS Wavelength.

Conteúdo

- Regiões
- Zonas de disponibilidade
- zonas locais
- Zonas do Wavelength
- AWS Outposts

Regiões

Cada região é projetada para ser isolada das outras regiões. Isso proporciona a maior tolerância a falhas e estabilidade possível.

Ao visualizar os recursos, você vê apenas os recursos que estão vinculados à região especificada. Isso ocorre porque as regiões são isoladas entre si e nós não replicamos os recursos entre regiões automaticamente.

Ao executar uma instância, é necessário selecionar uma AMI que esteja na mesma região. Se a AMI estiver em outra região, será possível copiar a AMI para a região que está usando. Para obter mais informações, consulte Copiar um AMI.

Observe que há uma cobrança para a transferência de dados entre regiões. Para obter mais informações, consulte Definição de preços do Amazon EC2 – Transferência de dados.

Tópicos

- Regiões disponíveis
- Regiões e endpoints
- Descreva suas regiões
- Obter o nome de exibição da região
- Especificar a região para um recurso

Regiões disponíveis

Sua conta determina as regiões que estão disponíveis para você.

- Uma Conta da AWS fornece várias regiões para que você possa iniciar instâncias do Amazon EC2 em locais que atendam às suas necessidades. Por exemplo, talvez você queira executar instâncias na Europa para estar mais próximo de seus clientes europeus ou para cumprir requisitos legais.
- Uma conta AWS GovCloud (Oeste dos EUA) fornece acesso somente à região AWS GovCloud (Oeste dos EUA) e à região AWS GovCloud (Leste dos EUA). Para ter mais informações, consulte AWS GovCloud (US).
- Uma conta da Amazon AWS (China) fornece acesso somente às regiões Pequim e Ningxia. Para obter mais informações, consulte Amazon Web Services na China.

A tabela a seguir lista as regiões fornecidas por Conta da AWS. Não é possível descrever ou acessar regiões adicionais de uma Conta da AWS, como as AWS GovCloud (US) Regions ou as regiões da China. Para usar uma região introduzida depois de 20 de março de 2019, é necessário habilitar a região. Para obter mais informações, consulte Especificar quais regiões da AWS sua conta pode usar no Guia de referência do AWS Account Management.

Código	Nome	Status de opt-in
us-east-2	Leste dos EUA (Ohio)	Não obrigatório
us-east-1	Leste dos EUA (Virgínia)	Não obrigatório
us-west-1	Oeste dos EUA (N. da Califórnia)	Não obrigatório
us-west-2	Oeste dos EUA (Oregon)	Não obrigatório
af-south-1	África (Cidade do Cabo)	Obrigatório
ap-east-1	Ásia-Pacífico (Hong Kong)	Obrigatório
ap-south-2	Ásia-Pacífico (Hyderabad)	Obrigatório
ap-southeast-3	Ásia-Pacífico (Jacarta)	Obrigatório
ap-southeast-4	Ásia-Pacífico (Melbourne)	Obrigatório
ap-south-1	Ásia-Pacífico (Mumbai)	Não obrigatório
ap-northeast-3	Ásia-Pacífico (Osaka)	Não obrigatório
ap-northeast-2	Ásia-Pacífico (Seul)	Não obrigatório
ap-southeast-1	Ásia-Pacífico (Cingapura)	Não obrigatório
ap-southeast-2	Ásia-Pacífico (Sydney)	Não obrigatório
ap-northeast-1	Ásia-Pacífico (Tóquio)	Não obrigatório
ca-central-1	Canadá (Central)	Não obrigatório
ca-west-1	Oeste do Canadá (Calgary)	Obrigatório

Código	Nome	Status de opt-in
eu-central-1	Europa (Frankfurt)	Não obrigatório
eu-west-1	Europa (Irlanda)	Não obrigatório
eu-west-2	Europa (Londres)	Não obrigatório
eu-south-1	Europa (Milão)	Obrigatório
eu-west-3	Europa (Paris)	Não obrigatório
eu-south-2	Europa (Espanha)	Obrigatório
eu-north-1	Europa (Estocolmo)	Não obrigatório
eu-central-2	Europa (Zurique)	Obrigatório
il-central-1	Israel (Tel Aviv)	Obrigatório
me-south-1	Oriente Médio (Barém)	Obrigatório
me-central-1	Oriente Médio (Emirados Árabes Unidos)	Obrigatório
sa-east-1	América do Sul (São Paulo)	Não obrigatório

Para obter mais informações, consulte Infraestrutura global da AWS.

O número e o mapeamento das zonas de disponibilidades por região pode variar entre Contas da AWS. Para obter uma lista de zonas de disponibilidade que estão disponíveis para sua conta, é possível usar o console do Amazon EC2 ou a interface de linha de comando. Para ter mais informações, consulte Descreva suas regiões.

Regiões e endpoints

Ao trabalhar com uma instância usando a interface de linha de comando ou ações de API, é necessário especificar seu endpoint regional. Para obter mais informações sobre as regiões e endpoints para o Amazon EC2, consulte Endpoints e cotas do Amazon EC2 na Referência geral da Amazon Web Services.

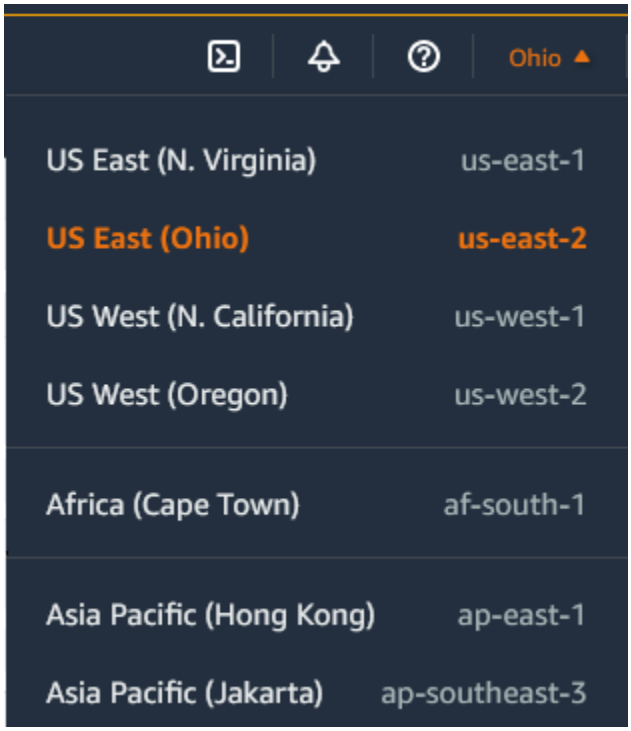
Para obter mais informações sobre os endpoints e os protocolos na AWS GovCloud (Oeste dos EUA), consulte Service Endpoints (Endpoints de serviço) no Guia do usuário da AWS GovCloud (US).

Descreva suas regiões

É possível usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais regiões estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Como localizar suas regiões usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o seletor Regions (Regiões).



3. Seus recursos do EC2 para a região selecionada são exibidos no Painel do EC2 na seção Recursos.

Como localizar suas regiões usando a AWS CLI

Use o comando describe-regions como a seguir para descrever as regiões habilitadas para sua conta.

```
aws ec2 describe-regions
```

Para descrever todas as regiões, incluindo as regiões que estão desabilitadas para sua conta, adicione a opção `--all-regions` da seguinte forma.

```
aws ec2 describe-regions --all-regions
```

Obter o nome de exibição da região

É possível usar o AWS Systems Manager Parameter Store para visualizar o nome de exibição de uma região. Cada região tem parâmetros públicos no caminho a seguir.

```
/aws/service/global-infrastructure/regions/region-code
```

Os parâmetros públicos de uma região incluem os seguinte:

- /aws/service/global-infrastructure/regions/*region-code*/domain
- /aws/service/global-infrastructure/regions/*region-code*/geolocationCountry
- /aws/service/global-infrastructure/regions/*region-code*/geolocationRegion
- /aws/service/global-infrastructure/regions/*region-code*/longName
- /aws/service/global-infrastructure/regions/*region-code*/partition

O parâmetro `longName` contém o nome de exibição da região. O comando get-parameters-by-path a seguir retorna o nome de exibição da região `af-south-1`. Ele usa a opção `--query` para definir o escopo da saída para o nome da região. No Linux, é necessário colocar a string de consulta entre aspas simples. Para executar esse comando usando o prompt de comando do Windows, omita as aspas simples ou altere-as para aspas duplas.

AWS CLI on Linux

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions/af-south-1 \
    --query 'Parameters[?Name.contains(@,`longName`)].Value' \
    --output text
```

AWS CLI on Windows

```
aws ssm get-parameters-by-path ^
```

```
    --path /aws/service/global-infrastructure/regions/af-south-1 ^
    --query "Parameters[?Name.contains(@,`longName`)].Value" ^
    --output text
```

Tools for PowerShell

Se não estiver instalado, instale o módulo AWS.Tools.SimpleSystemsManagement no Tools for PowerShell executando `Install-AWSToolsModule AWS.Tools.SimpleSystemsManagement -CleanUp`.

```
$parameterPath = "/aws/service/global-infrastructure/regions/af-south-1"
$substringToMatch = "longName"
$filteredParameters = Get-SSMParametersByPath -Path $parameterPath `
| Where-Object { $_.Name -like "*$substringToMatch*" } `
| ForEach-Object { Write-Output $_.Value }
$filteredParameters
```

O seguinte é um exemplo de saída.

```
Africa (Cape Town)
```

Para obter mais informações, consulte Trabalhar com parâmetros públicos no Guia do usuário do AWS Systems Manager

Especificar a região para um recurso

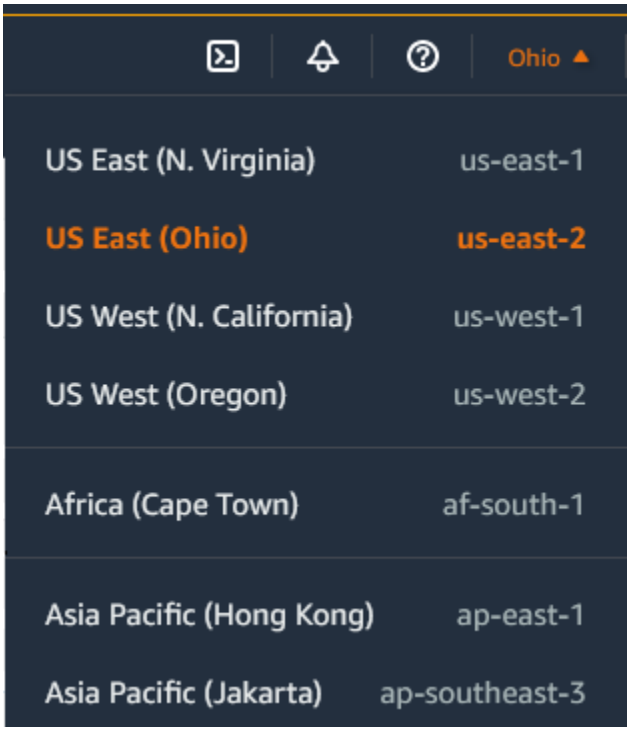
Sempre que você cria um recurso do Amazon EC2, é possível especificar a região para o recurso. É possível especificar a região para um recurso usando o AWS Management Console ou a linha de comando.

Considerações

Alguns recursos da AWS podem não estar disponíveis em todas as regiões. Certifique-se de que é possível criar os recursos necessários nas regiões desejadas antes de executar uma instância.

Para especificar a região para um recurso usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região.



Para especificar a região padrão usando a linha de comando

É possível definir o valor de uma variável de ambiente para o endpoint regional desejado (por exemplo, `https://ec2.us-east-2.amazonaws.com`):

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

Como alternativa, é possível usar o código `--region` (AWS CLI) ou a opção da linha de comando `-Region` (AWS Tools for Windows PowerShell) com cada comando individual. Por exemplo, `--region us-east-2`.

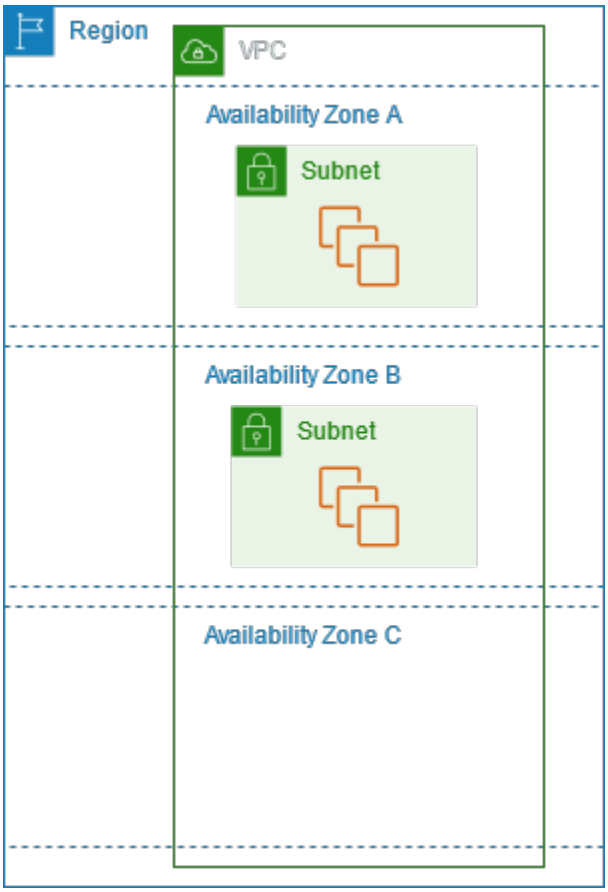
Para obter mais informações sobre os endpoints para o Amazon EC2, consulte Endpoints e cotas do Amazon EC2 na Referência geral da AWS.

Zonas de disponibilidade

Cada região contém vários locais isolados conhecidos como Zonas de Disponibilidade. O código da zona de disponibilidade é o código de região seguido por um identificador de letra. Por exemplo, `us-east-1a`.

Ao iniciar uma instância, você seleciona uma região e uma nuvem privada virtual (VPC). Em seguida, pode selecionar uma sub-rede de uma das zonas de disponibilidade ou permitir que façamos a escolha para você. Se você distribuir suas instâncias em várias zonas de disponibilidade e uma instância falhar, poderá projetar sua aplicação para que uma instância em outra zona de disponibilidade possa processar solicitações. Também é possível usar endereços IP elásticos para mascarar a falha de uma instância em uma zona de disponibilidade rapidamente, remapeando o endereço para uma instância em outra zona de disponibilidade.

O diagrama a seguir ilustra várias zonas de disponibilidade em uma região da AWS. A zona de disponibilidade A e a zona de disponibilidade B têm uma sub-rede, e cada sub-rede tem instâncias. A zona de disponibilidade C não tem sub-redes, portanto, não é possível iniciar instâncias nela.



Como as zonas de disponibilidade crescem com o tempo, nossa capacidade de expandi-las pode se tornar restrita. Se isso acontecer, nós poderemos impedir que você execute uma instância em uma zona de disponibilidade restrita a menos que você já tenha uma instância naquela zona de disponibilidade. Finalmente, também podemos remover a zona de disponibilidade restrita da lista de zonas de disponibilidade para novas contas. Portanto, sua conta pode ter um número diferente de zonas de disponibilidade disponíveis em uma região em comparação a outra conta.

Conteúdo

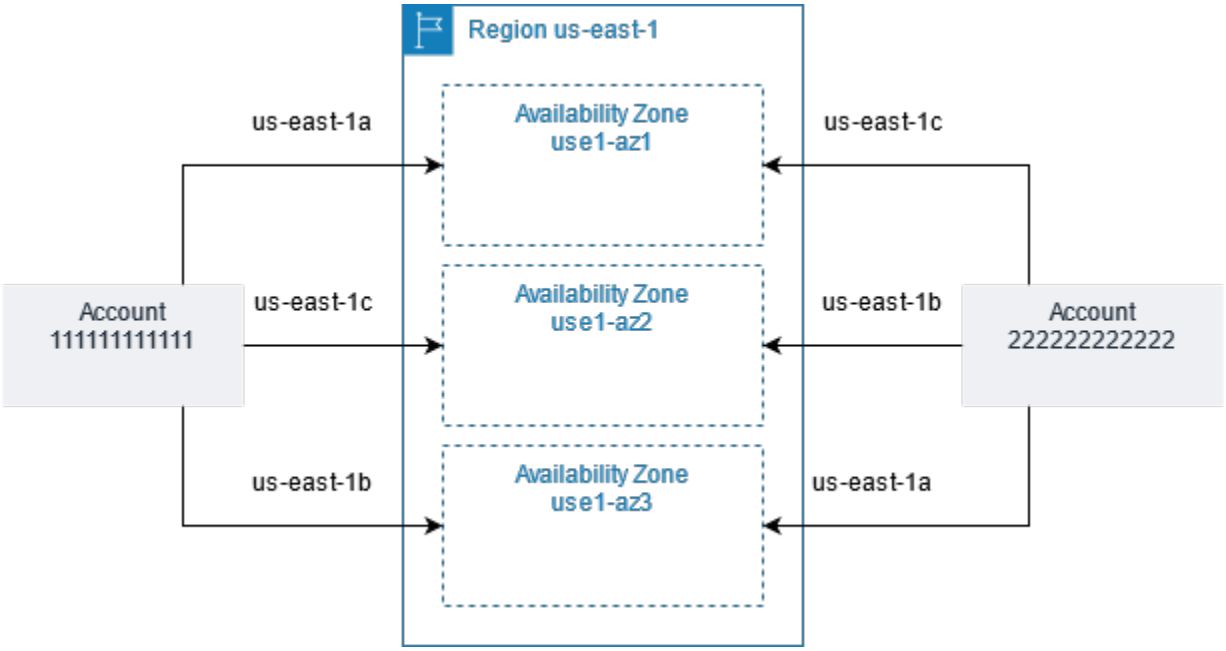
- IDs de AZ
- Descrever suas zonas de disponibilidade
- Executar instâncias em uma zona de disponibilidade
- Migrar uma instância para outra zona de disponibilidade

IDs de AZ

Para garantir que os recursos sejam distribuídos pelas zonas de disponibilidade de uma região, mapeamos de forma independente as zonas de disponibilidade para códigos em cada Conta da AWS nas nossas regiões mais antigas. Por exemplo, o `us-east-1a` para Conta da AWS pode não ser o mesmo local físico que o `us-east-1a` de outro Conta da AWS.

Para coordenar as zonas de disponibilidade entre contas em todas as regiões, mesmo aquelas que mapeiam zonas de disponibilidade, use os AZ IDs, que são identificadores exclusivos e consistentes de uma zona de disponibilidade. Por exemplo, `use1-az1` é um ID de AZ para a região `us-east-1` e tem o mesmo local físico em cada Conta da AWS. É possível visualizar os IDs de AZs da sua conta para determinar o local físico dos recursos em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ `use1-az2` com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é `use1-az2`.

O diagrama a seguir ilustra duas contas com diferentes mapeamentos do código da zona de disponibilidade para ID de AZ.



Descrever suas zonas de disponibilidade

É possível usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais zonas de disponibilidade estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Como localizar suas zonas de disponibilidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região.
3. No painel de navegação, escolha EC2 Dashboard.
4. As zonas de disponibilidade são listadas no painel Integridade de serviço.

Como localizar suas zonas de disponibilidade usando a AWS CLI

- Use o comando describe-availability-zones, como se segue, para descrever as zonas de disponibilidade da região especificada que estão disponíveis para a conta.

```
aws ec2 describe-availability-zones --region region-name
```

- Use o comando describe-availability-zones conforme mostrado a seguir para descrever as zonas de disponibilidade independentemente do status da opção.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Executar instâncias em uma zona de disponibilidade

Ao executar uma instância, selecione uma região que deixe suas instâncias mais próximas de clientes específicos ou cumpra os requisitos legais ou outros. Ao iniciar as instâncias em zonas de disponibilidade separadas, é possível proteger suas aplicações contra falhas em um único local.

Quando você executa uma instância, é possível especificar uma zona de disponibilidade na região que está usando. Se você não especificar uma zona de disponibilidade, selecionaremos uma zona de disponibilidade para você. Ao executar instâncias iniciais, recomendamos aceitar a zona de disponibilidade padrão. Assim, podemos selecionar a melhor zona de disponibilidade para você de acordo com a integridade do sistema e a capacidade disponível. Se você executar instâncias adicionais, somente especifique uma zona de disponibilidade se as novas instâncias tiverem de estar próximas ou separadas de suas instâncias em execução.

Migrar uma instância para outra zona de disponibilidade

Se necessário, será possível migrar uma instância de uma zona de disponibilidade para outra. Por exemplo, se você tentar modificar o tipo de instância e não pudermos iniciar uma instância do novo tipo de instância na zona de disponibilidade atual, será possível migrar a instância para uma zona de disponibilidade com capacidade para o novo tipo de instância.

O processo de migração envolve:

- Criação de uma AMI da instância original
- Execução de uma instância na nova zona de disponibilidade
- Atualização da configuração da nova instância, conforme mostrado no procedimento a seguir

Para migrar uma instância para outra zona de disponibilidade

1. Crie um AMI a partir da instância. O procedimento depende do tipo de volume do dispositivo raiz para a instância. Para obter mais informações, consulte a documentação que corresponde ao volume do seu dispositivo raiz:

   - Criação de uma AMI baseada no Amazon EBS

- Criar uma AMI em Linux com armazenamento de instâncias

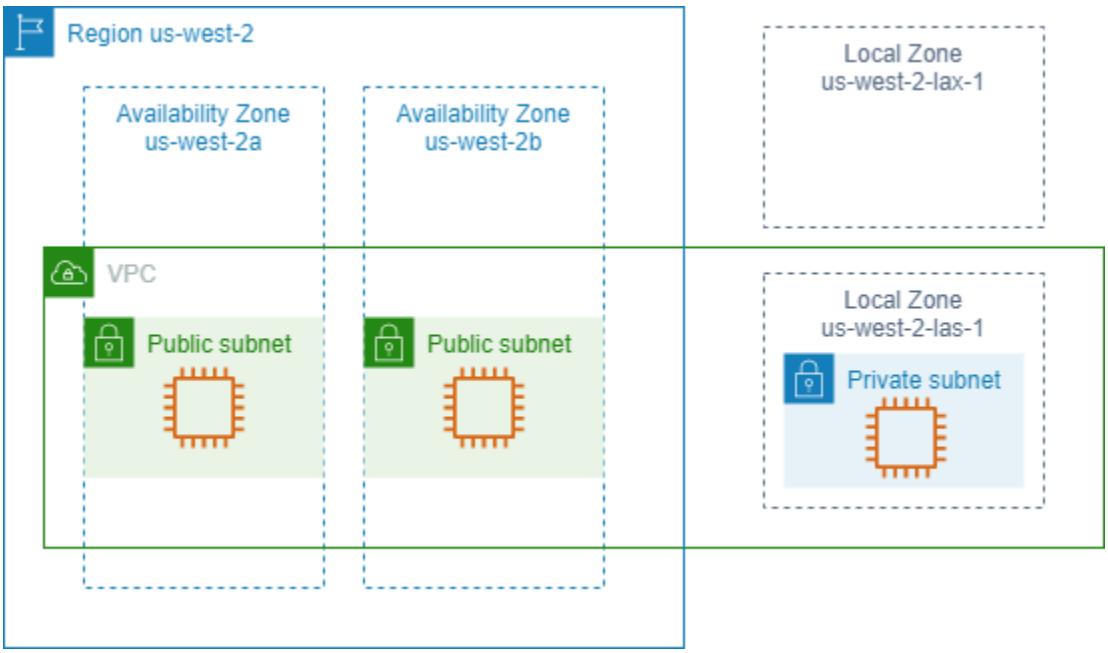
2. Se for necessário preservar o endereço IPv4 privado da instância, você deverá excluir a sub-rede na zona de disponibilidade atual e criar uma sub-rede na nova zona de disponibilidade com o mesmo intervalo de endereço IPv4 que a sub-rede original. Observe que é necessário encerrar todas as instâncias em uma sub-rede antes de excluí-la. Portanto, crie AMIs de todas as instâncias em sua sub-rede de modo que possa mover todas as instâncias na sub-rede atual para a nova sub-rede.
3. Execute uma instância da AMI que você acabou de criar, especificando a nova zona de disponibilidade ou a sub-rede. É possível usar o mesmo tipo de instância que a instância original ou selecionar um novo tipo de instância. Para obter mais informações, consulte Executar instâncias em uma zona de disponibilidade.
4. Se a instância original tiver um endereço IP elástico associado, associe-o à nova instância. Para obter mais informações, consulte Dissociar um endereço IP elástico.
5. Se a instância original for uma Instância reservada, altere a zona de disponibilidade da sua reserva. Se você também tiver mudado o tipo de instância, poderá alterar o tipo de instância para sua reserva. Para obter mais informações, consulte Enviar solicitações de modificação.
6. (Opcional) Encerre a instância original. Para obter mais informações, consulte Como encerrar uma instância.

zonas locais

Uma zona local é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As zonas locais têm suas próprias conexões com a Internet e são compatíveis com o AWS Direct Connect para que os recursos criados em uma zona local possam atender usuários locais com comunicações de baixa latência. Para obter mais informações, consulte O que são zonas locais da AWS? no Guia do usuário de zonas locais da AWS.

O código da zona local é o código da região da seguido por um identificador que indica o local físico. Por exemplo, `us-west-2-lax-1` em Los Angeles.

O diagrama a seguir ilustra a região da AWS `us-west-2`, duas de suas zonas de disponibilidade e duas de suas zonas locais. A VPC abrange as zonas de disponibilidade e uma das zonas locais. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



Para usar uma zona local, é necessário ativá-la primeiro. Para obter mais informações, consulte the section called “Optar por zonas locais”. Depois, crie uma sub-rede na zona local. Finalmente, inicie os recursos na sub-rede da zona local, como instâncias, para que as aplicações fiquem perto dos usuários.

Conteúdo

- Zonas locais disponíveis
- Optar por zonas locais
- Executar instâncias em uma zona local

Zonas locais disponíveis

É possível usar o console do Amazon EC2 ou uma interface da linha de comando para determinar quais zonas locais estão disponíveis para a conta. Para obter uma lista completa, consulte Localizações das zonas locais da AWS.

Como localizar suas zonas locais usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região superior.
3. No painel de navegação, escolha EC2 Dashboard.

4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).

Para localizar suas zonas locais usando a AWS CLI

Use o comando describe-availability-zones, como se segue, para descrever todas as zonas locais na região especificada, mesmo que não estejam disponíveis. Para descrever somente as zonas locais que você habilitou, omita a opção `--all-availability-zones`.

```
aws ec2 describe-availability-zones --region region-name --filters Name=zone-
type,Values=local-zone --all-availability-zones
```

Optar por zonas locais

Antes de especificar uma zona local para um recurso ou serviço, é necessário optar por zonas locais.

Consideração

Alguns recursos da AWS podem não estar disponíveis em todas as regiões. Verifique se é possível criar os recursos necessários nas regiões ou zonas locais desejadas antes de executar uma instância em uma zona local específica. Para obter uma lista de serviços compatíveis com cada zona local, consulteRecursos das zonas locais da AWS.

Para optar por zonas locais usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No canto superior esquerdo da página, selecione New EC2 Experience (Nova experiência do EC2). Não é possível concluir essa tarefa usando a experiência de console antiga.
3. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região superior.
4. No painel de navegação, escolha EC2 Dashboard.
5. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).
6. Escolha uma zona local e escolha Ação > Gerenciar grupo de zonas.
7. Em Status de opt-in, escolha Habilitar.
8. Selecione Atualizar.

Para optar por zonas locais usando o AWS CLI

Use o comando modify-availability-zone-group.

Executar instâncias em uma zona local

Ao executar uma instância, é possível especificar uma sub-rede que está em uma zona local. É possível alocar os endereços IP de um grupo de bordas de rede: Um grupo de bordas de rede é um conjunto exclusivo de zonas de disponibilidade, zonas locais ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, `us-west-2-lax-1a`.

É possível alocar os endereços IP de um grupo de bordas de rede:

- Endereços IPv4 elásticos fornecidos pela Amazon
- Endereços IPv6 da VPC fornecidos pela Amazon (disponíveis somente nas zonas de Los Angeles)

Para obter mais informações sobre como iniciar uma instância em uma zona local, consulte Conceitos básicos do AWS Local Zones no Guia do usuário do AWS Local Zones.

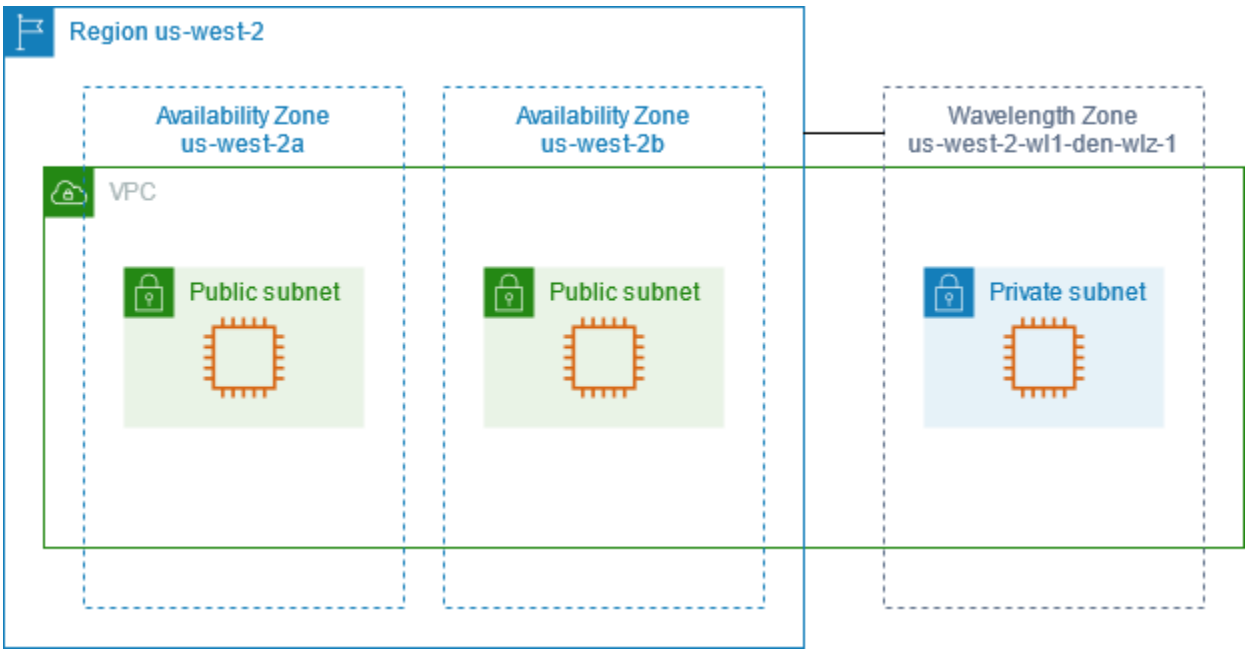
Zonas do Wavelength

O AWS Wavelength permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. Os desenvolvedores podem estender uma nuvem privada virtual (VPC) para uma ou mais zonas do Wavelength e usar os recursos da AWS, como instâncias do Amazon EC2, para executar aplicações que exigem baixíssima latência e uma conexão com serviços da AWS na região.

Uma Wavelength Zone é uma zona isolada no local da transportadora em que a infraestrutura de Wavelength é implantada. As zonas de Wavelength estão vinculadas a uma região. Uma zona de Wavelength é uma extensão lógica de uma região e é gerenciada pelo plano de controle na região.

O código para uma zona Wavelength é seu código de região seguido por um identificador que indica o local físico. Por exemplo, `us-east-1-wl1-bos-wlz-1` em Boston.

O diagrama a seguir ilustra a região da AWS `us-west-2`, duas de suas zonas de disponibilidade e uma zona Wavelength. A VPC abrange as zonas de disponibilidade e a zona Wavelength. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



Para usar uma zona de Wavelength, é necessário primeiro escolher a zona. Para obter mais informações, consulte the section called “Habilitar zonas de Wavelength”. Em seguida, crie uma sub-rede na zona de Wavelength. Por fim, inicie seus recursos na sub-rede das zonas de Wavelength, para que suas aplicações estejam mais próximas dos usuários finais.

As Wavelength Zones não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte Zonas do Wavelength disponíveis no Guia do desenvolvedor da AWS Wavelength.

Tópicos

- Descreva suas zonas de Wavelength
- Habilitar zonas de Wavelength
- Executar instâncias em uma zona de Wavelength

Descreva suas zonas de Wavelength

É possível usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais zonas de Wavelength estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

Como localizar suas zonas de Wavelength usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região.
3. No painel de navegação, escolha EC2 Dashboard.
4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).

Como localizar suas zonas de Wavelength usando a AWS CLI

- Use o comando describe-availability-zones, como se segue, para descrever as zonas de wavelength na região especificada que estão disponíveis para a conta.

```
aws ec2 describe-availability-zones --region region-name
```

- Use o comando describe-availability-zones como a seguir para descrever as zonas de Wavelength independentemente do status da opção.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Habilitar zonas de Wavelength

Antes de especificar uma zona do Wavelength para um recurso ou serviço, é necessário aceitar as zonas do Wavelength.

Considerações

- Alguns recursos da AWS não estão disponíveis em todas as regiões. Certifique-se de que é possível criar os recursos necessários na região ou zona de Wavelength desejada antes de executar uma instância em uma zona de Wavelength específica.

Como ativar zonas de Wavelength usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No canto superior esquerdo da página, selecione New EC2 Experience (Nova experiência do EC2). Não é possível concluir essa tarefa usando a experiência de console antiga.
3. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região.
4. No painel de navegação, escolha EC2 Dashboard.

5. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).
6. Escolha uma zona do Wavelength e escolha Ação > Gerenciar grupo de zonas.
7. Em Status de opt-in, escolha Habilitar.
8. Selecione Atualizar.

Como habilitar zonas de Wavelength usando a AWS CLI

Use o comando modify-availability-zone-group.

Executar instâncias em uma zona de Wavelength

Ao executar uma instância, é possível especificar uma sub-rede que está em uma zona de Wavelength. Você também aloca o endereço IP de uma operadora de um grupo de bordas de rede, que é um conjunto exclusivo de zonas de disponibilidade, zonas locais ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, `us-east-1-wl1-bos-wlz-1`.

Para obter informações sobre como executar uma instância em uma zona do Wavelength, consulte Conceitos básicos do AWS Wavelength Wavelength no Guia do desenvolvedor do AWS Wavelength.

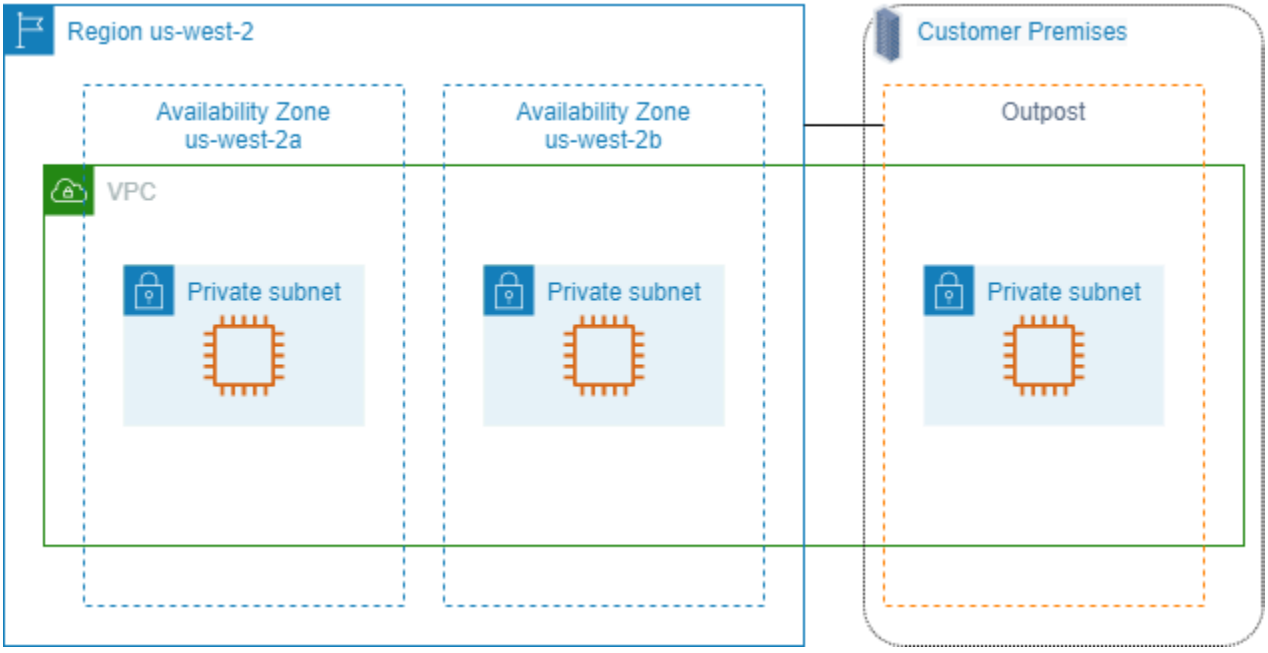
AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS. É possível criar sub-redes no Outpost e especificá-las ao criar recursos da AWS. As instâncias nas sub-redes do Outpost se comunicam com outras instâncias na região da AWS usando endereços IP privados, tudo na mesma VPC.

O diagrama a seguir ilustra a região `us-west-2` da AWS, duas de suas zonas de disponibilidade e um Outpost. A VPC abrange as zonas de disponibilidade e o Outpost. O Outpost está em um data

center on-premises do cliente. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



Para começar a usar o AWS Outposts, crie um Outpost e solicitar capacidade para o Outpost. Para obter mais informações sobre configurações de Outposts, consulte nosso catálogo. Após a instalação do equipamento do Outpost, a capacidade de computação e de armazenamento estará disponível quando você executar instâncias do Amazon EC2 em seu Outpost.

Executar instâncias em um Outpost

É possível executar instâncias do EC2 na sub-rede do Outpost que você criou. Os grupos de segurança controlam o tráfego de entrada e de saída para instâncias com interfaces de rede elástica em uma sub-rede do Outpost, assim como fazem para instâncias em uma sub-rede de zona de disponibilidade. Para se conectar a uma instância do EC2 em uma sub-rede do Outpost, é possível especificar um par de chaves ao executar a instância, como o faz para instâncias em uma sub-rede de zona de disponibilidade.

Recomendamos limitar o volume raiz de uma instância em um rack do Outpost a até 30 GiB. É possível especificar volumes de dados no mapeamento de dispositivo de bloco da AMI ou na instância para fornecer armazenamento adicional. Para eliminar blocos não utilizados do volume de inicialização, consulte Como criar volumes de EBS esparsos no blog da rede de parceiros da AWS.

Recomendamos aumentar o tempo limite de NVMe para o volume raiz. Para obter mais informações, consulte Tempo limite da operação de E/S.

Para obter informações sobre como criar um Outpost, consulte Get started with AWS Outposts (Conceitos básicos do Outpost) no Guia do Usuário AWS Outposts.

Criar um volume em um rack do Outpost

O AWS Outposts oferece modelos de rack e servidor. Se sua capacidade estiver em um rack do Outpost, será possível criar volumes do EBS na sub-rede do Outpost que você criou. Ao criar o volume, especifique o nome de recurso da Amazon (ARN) do Outpost.

O seguinte comando create-volume cria um volume vazio de 50 GB no Outpost especificado.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

É possível modificar dinamicamente o tamanho dos volumes gp2 Amazon EBS sem desanexá-los. Para obter mais informações sobre como modificar um volume sem desassociá-lo, consulte Solicitar modificações para seus volumes do EBS.

Endereçamento IP de instâncias do Amazon EC2

O Amazon EC2 e a Amazon VPC oferecem suporte aos protocolos de endereçamento IPv4 e IPv6. Por padrão, o Amazon VPC usa o protocolo de endereçamento IPv4. Não é possível desabilitar esse comportamento. Ao criar uma VPC, especifique um bloco CIDR IPv4 (um intervalo de endereços IPv4 privados). Opcionalmente, é possível atribuir um bloco CIDR IPv6 à VPC e atribuir os endereços IPv6 desse bloco às instâncias nas sub-redes.

Conteúdo

- Endereços IPv4 privados
- Endereços IPv4 públicos
- Otimização de endereço IPv4 público
- Endereços IP elásticos (IPv4)
- Endereços IPv6
- Trabalhar com os endereços IPv4 para as instâncias
- Trabalhar com os endereços IPv6 para as instâncias
- Diversos endereços IP para as instâncias do EC2
- Configurar um endereço IPv4 privado secundário para uma instância do Windows.

- Hostnames de instância do EC2
- Endereços locais de link

Endereços IPv4 privados

Um endereço IPv4 privado é um endereço IP que não é acessível pela Internet. É possível usar endereços IPv4 privados para comunicação entre instâncias na mesma VPC. Para obter mais informações sobre os padrões e as especificações de endereços IPv4 privados, consulte a RFC 1918. Atribuímos os endereços IPv4 privados a instâncias usando o DHCP.

> **Note**
>
> É possível criar uma VPC com um bloco CIDR publicamente roteável que esteja fora dos intervalos de endereços IPv4 privados especificados na RFC 1918. No entanto, para fins dessa documentação, referimo-nos aos endereços IPv4 privados (ou “endereços IP privados ") como os endereços IP que estão no intervalo CIDR IPv4 da VPC.

As sub-redes da VPC podem ser de um destes tipos:

As sub-redes da VPC podem ser de um destes tipos:

- Sub-redes somente IPv4: você só pode criar recursos nessas sub-redes com endereços IPv4 atribuídos a eles.
- Sub-redes somente IPv6: você só pode criar recursos nessas sub-redes com endereços IPv6 atribuídos a eles.
- Sub-redes IPv4 e IPv6: é possível criar recursos nessas sub-redes com endereços IPv4 ou IPv6 atribuídos a eles.

Quando você inicia uma instância do EC2 em uma sub-rede somente IPv4 ou de pilha dupla (IPv4 e IPv6), a instância recebe um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede. Para obter mais informações, consulte Endereçamento IP no Manual do usuário da Amazon VPC. Se você não especificar um endereço IP privado primário ao executar a instância, selecionaremos um endereço IP disponível no intervalo IPv4 da sub-rede para você. Cada instância tem uma interface de rede padrão (eth0) que recebe o endereço IPv4 privado primário. Também é possível especificar endereços IPv4 privados adicionais, conhecidos como endereços IPv4 privados secundários. Ao contrário de um endereço IP privado primário, os endereços IP privados secundários

podem ser atribuídos novamente de uma instância para outra. Para obter mais informações, consulte Diversos endereços IP para as instâncias do EC2.

Um endereço IPv4 privado, independentemente de ser um endereço primário ou secundário, permanece associado à interface de rede quando a instância é interrompida e reiniciada ou é hibernada e iniciada, e é liberado quando a instância é encerrada.

Endereços IPv4 públicos

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. É possível usar endereços públicos para comunicação entre as instâncias e a Internet.

Quando você inicia uma instância em uma VPC padrão, atribuímos a ela um endereço IP público por padrão. Quando você executa uma instância em uma VPC não padrão, a sub-rede tem um atributo que determina se as instâncias executadas naquela sub-rede recebem um endereço IP público do grupo de endereços IPv4 públicos. Por padrão, não atribuímos um endereço IP público a instâncias iniciadas em uma sub-rede não padrão.

É possível controlar se sua instância recebe um endereço IP público fazendo o seguinte:

- Modificando o atributo de endereçamento IP público da sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede no Guia do usuário da Amazon VPC.
- Habilitando ou desabilitando o recurso de endereçamento IP público durante a execução da instância, o que substitui o atributo de endereçamento IP público da sub-rede. Para ter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância.
- É possível cancelar a atribuição de um endereço IP público da sua instância após a execução gerenciando os endereços IP associados a uma interface de rede.

Um endereço IP público é atribuído à instância no grupo de endereços IPv4 públicos da Amazon e não está associado à sua conta da AWS. Quando um endereço IP público é desassociado da instância, ele é liberado de volta para o grupo de endereços IPv4 públicos, e você não pode reutilizá-lo.

Em alguns casos, liberamos o endereço IP público de sua instância ou atribuímos um novo:

- Liberamos o endereço IP público da instância quando ela é interrompida, hibernada ou encerrada. Sua instância interrompida ou hibernada recebe um novo endereço IP público quando é iniciada.

- Liberamos o endereço IP público de sua instância ao associar um endereço IP elástico a ela. Quando você desassocia o endereço IP elástico da instância, ela recebe um novo endereço IP público.
- Se o endereço IP público da instância em uma VPC foi liberado, ela não receberá um novo se houver mais de uma interface de rede anexada à instância.
- Se o endereço IP público da instância for liberado enquanto houver um endereço IP privado secundário associado a um endereço IP elástico, a instância não receberá um novo endereço IP público.

Se você precisar de um endereço IP público persistente que possa ser associado às instâncias e das instâncias conforme necessário, use um endereço IP elástico.

Se você usar o DNS dinâmico para mapear um nome DNS existente para o endereço IP público de uma nova instância, poderá demorar até 24 horas para o endereço IP ser propagado via Internet. Como resultado, as novas instâncias não poderão receber tráfego quando as instâncias encerradas continuarem a receber solicitações. Para resolver o problema, use um endereço IP elástico. É possível alocar seu próprio endereço IP elástico e associá-lo à instância. Para ter mais informações, consulte Endereços IP elásticos.

> **Note**
>
> - A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.
> - As instâncias que acessam outras instâncias por meio de seu endereço IP NAT público são cobradas pela transferência de dados regional ou via Internet, dependendo de se as instâncias estão na mesma região.

Otimização de endereço IPv4 público

A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

A lista a seguir contém ações que você pode tomar para otimizar o número de endereços IPv4 públicos que você usa:

- Use um balanceador de carga elástico para balancear a carga do tráfego para suas instâncias do EC2 e desabilitar a atribuição automática de IP público na ENI primária atribuída às instâncias. Os balanceadores de carga usam um único endereço IPv4 público, o que reduz o número de endereços IPv4 público. Talvez você também queira consolidar os balanceadores de carga existentes para reduzir ainda mais a contagem de endereços IPv4 públicos.
- Se o único motivo para usar um gateway NAT for usar SSH em uma instância do EC2 em uma sub-rede privada para manutenção ou emergências, considere usar o Endpoint do EC2 Instance Connect no lugar. Com o Endpoint do EC2 Instance Connect, você pode se conectar a uma instância da Internet sem a necessidade de que a instância tenha um endereço IPv4 público.
- Se suas instâncias do EC2 estiverem em uma sub-rede pública com endereços IP públicos alocados a elas, considere mover as instâncias para uma sub-rede privada, remover os endereços IP públicos e usar um gateway NAT público para permitir o acesso de e para suas instâncias do EC2. Há considerações de custo para usar gateways NAT. Use este método de cálculo para decidir se os gateways NAT são econômicos. Você pode obter o `Number of public IPv4 addresses` necessário para esse cálculo criando um relatório de uso e custo de cobrança da AWS.

  ```
  NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
   public IP cost
  ```

  Em que:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Se o total for menor que 1, os gateways NAT são mais baratos que os endereços IPv4 públicos.
- Use AWS PrivateLink para se conectar de forma privada a serviços da AWS ou serviços hospedados por outras contas da AWS, em vez de usar endereços IPv4 públicos e gateways da Internet.

- Traga seu próprio intervalo de endereços IP (BYOIP) para a AWS e use-o para endereços IPv4 públicos em vez de usar endereços IPv4 públicos de propriedade da Amazon.
- Desative o endereço IPv4 público atribuído automaticamente à instância executada em sub-redes. Essa opção geralmente é desabilitada por padrão para VPCs quando você cria uma sub-rede, mas você deve verificar suas sub-redes existentes para garantir que ela esteja desabilitada.
- Se você tiver instâncias do EC2 que não precisam de endereços IPv4 públicos, verifique se as interfaces de rede anexadas às suas instâncias têm a atribuição automática de IP público desabilitada.
- Configure endpoints do acelerador no AWS Global Accelerator para instâncias do EC2 em sub-redes privadas para permitir que o tráfego da Internet flua diretamente para os endpoints em suas VPCs sem exigir endereços IP públicos. Você também pode trazer seus próprios endereços para o AWS Global Accelerator e usar seus próprios endereços IPv4 para os endereços IP estáticos do seu acelerador.

Endereços IP elásticos (IPv4)

Um endereço IP elástico é um endereço IPv4 público que é possível alocar à sua conta. É possível associá-lo e desassociá-lo de instâncias conforme necessário. Ele é alocado para sua conta até que você opte por liberá-lo. Para obter mais informações sobre endereços IP elásticos e como usá-los, consulte Endereços IP elásticos.

Não oferecemos suporte a endereços IP elásticos para IPv6.

Endereços IPv6

Opcionalmente, é possível associar um bloco CIDR IPv6 à VPC e associar blocos CIDR IPv6 às sub-redes. O bloco CIDR IPv6 da VPC é automaticamente atribuído do grupo de endereços IPv6 da Amazon. Você não pode escolher o intervalo você mesmo. Para obter mais informações, consulte um dos tópicos a seguir no Guia do usuário da Amazon VPC.

- Endereçamento IP para suas VPCs e sub-redes
- Adicionar um bloco CIDR IPv6 à sua VPC
- Adicionar um bloco CIDR IPv6 à sua sub-rede

Os endereços IPv6 são globalmente exclusivos e podem ser configurados para permanecer privados ou acessíveis pela Internet. A instância recebe um endereço IPv6 se um bloco CIDR IPv6 estiver associado à VPC e à sub-rede, e se uma das seguintes afirmações for verdadeira:

- A sub-rede está configurada para atribuir automaticamente um endereço IPv6 a uma instância durante a execução. Para obter mais informações, consulte Modify the IPv6 addressing attribute for your subnet (Modificar o atributo de endereçamento IPv6 para a sub-rede).
- Você atribui um endereço IPv6 à instância durante a execução.
- Você atribui um endereço IPv6 à interface de rede primária da instância após a execução.
- Você atribui um endereço IPv6 a uma interface de rede na mesma sub-rede e anexa a interface de rede à instância após a execução.

Quando a instância recebe um endereço IPv6 durante a execução, o endereço é associado à interface de rede primária (eth0) da instância. Você pode gerenciar os endereços IPv6 da interface de rede primária (eth0) das seguintes maneiras:

- Desassociar um endereço IPv6 de uma interface de rede. O número de endereços IPv6 que é possível atribuir a uma interface de rede e o número de interfaces de rede que é possível anexar a uma instância varia de acordo com o tipo de instância. Para ter mais informações, consulte Endereços IP por interface de rede por tipo de instância.
- Habilite um endereço IPv6 primário. Um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Para obter mais informações, consulte Criar uma interface de rede ou Gerenciar endereços IP.

Um endereço IPv6 persiste quando você interrompe e inicia ou hiberna e inicia a instância, e é liberado quando você encerra a instância. Você não pode atribuir novamente um endereço IPv6 enquanto ele estiver atribuído a outra interface de rede — é necessário primeiro cancelar a atribuição.

Você pode controlar se as instâncias são acessíveis através de seus endereços IPv6, controlando o roteamento da sua sub-rede ou usando o grupo de segurança e as regras de ACL de rede. Para obter mais informações, consulte Privacidade do tráfego entre redes no Guia do usuário da Amazon VPC.

Para obter mais informações sobre intervalos de endereço IPv6 reservados, consulte Registro de endereço para finalidades especiais IANA IPv6 e RFC4291.

Trabalhar com os endereços IPv4 para as instâncias

É possível atribuir um endereço IPv4 à instância ao executá-la. É possível ver os endereços IPv4 no console nas páginas Instances (Instâncias) ou Network Interfaces (Interfaces de rede).

Conteúdo

- Visualizar os endereços IPv4
- Atribuir um endereço IPv4 público durante a execução da instância

Visualizar os endereços IPv4

É possível usar o console do Amazon EC2 para visualizar os endereços IPv4 públicos e privados das instâncias. Também é possível determinar os endereços IPv4 públicos e privados da instância usando os metadados da instância. Para obter mais informações, consulte Trabalhar com metadados de instância.

O endereço IPv4 público é exibido como uma propriedade da interface de rede no console, mas é mapeado para o endereço IPv4 privado primário por meio da NAT. Portanto, se você inspecionar as propriedades da interface de rede na instância, por exemplo, por meio do `ifconfig` (Linux) ou do `ipconfig` (Windows), o endereço IPv4 público não será exibido. Para determinar o endereço IPv4 público da instância em uma instância, use os metadados da instância.

Para visualizar os endereços IPv4 de uma instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2InstanceAWS Tools for Windows PowerShell

Para determinar os endereços IPv4 da instância usando os metadados

1. Conecte-se à sua instância. Para ter mais informações, consulte Conexão com a instância do EC2.
2. Use o comando apresentado a seguir para acessar o endereço IP privado.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/local-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Use o comando apresentado a seguir para acessar o endereço IP público. Se um endereço IP elástico estiver associado à instância, o valor retornado será o do endereço IP elástico.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/public-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Atribuir um endereço IPv4 público durante a execução da instância

Toda sub-rede tem um atributo que determina se as instâncias executadas nessa sub-rede recebem um endereço IP público. Por padrão, as sub-redes não padrão têm esse atributo definido como false,

e as sub-redes padrão têm esse atributo definido como true. Quando você executa uma instância, um recurso de endereçamento IPv4 público também está disponível para controlar se a instância está atribuída a um endereço IPv4 público. É possível substituir o comportamento padrão do atributo de endereçamento IP da sub-rede. O endereço IPv4 público é atribuído no grupo de endereços IPv4 públicos da Amazon, e é atribuído à interface de rede com o índice de dispositivo de eth0. Esse recurso depende de determinadas condições no momento em que você executa a instância.

Considerações

- É possível cancelar a atribuição do endereço IP público da sua instância após a execução gerenciando os endereços IP associados a uma interface de rede. Para mais informações sobre endereços IPv4 públicos, consulte Endereços IPv4 públicos.
- Você não atribuir automaticamente um endereço IP público se especificar mais de uma interface de rede. Além disso, você não pode substituir a configuração da sub-rede usando o recurso de atribuição automática de endereço IP público, se especificar uma interface de rede existente para eth0.
- Independentemente de você atribuir ou não um endereço IP público à instância ao iniciá-la, é possível associar um endereço IP elástico à instância depois que ela for executada. Para ter mais informações, consulte Endereços IP elásticos. Também é possível modificar o comportamento do endereçamento IPv4 público da sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede.

Para atribuir um endereço IPv4 público durante a inicialização de uma instância usando o console

Siga o procedimento para iniciar uma instância e, ao definir as Network Settings (Configurações de rede), escolha a opção Auto-assign Public IP (Atribuir IP público automaticamente).

Para habilitar ou desabilitar o recurso de endereçamento IP público usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- Use a opção `--associate-public-ip-address` ou `--no-associate-public-ip-address` com o comando run-instances (AWS CLI)
- Use o parâmetro `-AssociatePublicIp` com o comando New-EC2Instance (AWS Tools for Windows PowerShell)

Trabalhar com os endereços IPv6 para as instâncias

É possível visualizar os endereços IPv6 atribuídos à instância, atribuir um endereço IPv6 público à instância ou cancelar a atribuição de um endereço IPv6 da instância. É possível visualizar esses endereços no console na página Instances (Instâncias) ou Network Interfaces (Interfaces de rede).

Tópicos

- Visualizar os endereços IPv6
- Atribuir um endereço IPv6 a uma instância
- Cancelar a atribuição de um endereço IPv6 de uma instância

Visualizar os endereços IPv6

É possível usar o console do Amazon EC2, a AWS CLI e os metadados de instância para visualizar os endereços IPv6 das instâncias.

Para visualizar os endereços IPv6 para uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Networking (Redes), localize IPv6 addresses (Endereços IPv6).

Para visualizar os endereços IPv6 de uma instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2InstanceAWS Tools for Windows PowerShell

Para visualizar os endereços IPv6 de uma instância usando os metadados de instância

1. Conecte-se à sua instância. Para ter mais informações, consulte Conexão com a instância do EC2.

2. Obtenha o endereço MAC da instância em `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.
3. Use o comando apresentado a seguir para visualizar o endereço IPv6.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
   macs/mac-address/ipv6s
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/
   interfaces/macs/mac-address/ipv6s
   ```

Atribuir um endereço IPv6 a uma instância

Se a VPC e a sub-rede tiverem blocos CIDR IPv6 associados a elas, será possível atribuir um endereço IPv6 à instância durante ou após a execução. O endereço IPv6 é atribuído no intervalo de endereços IPv6 da sub-rede e é atribuído à interface de rede com o índice de dispositivo de eth0.

Para atribuir um endereço IPv6 durante a inicialização da instância

Siga o procedimento para iniciar uma instância e, ao definir Network Settings (Configurações de rede), escolha a opção Auto-assign IPv6 IP (Atribuir IP IPv6).

Para atribuir um endereço IPv6 após a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).

4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), escolha Assign new IP address (Atribuir novo endereço IP). Insira um endereço IPv6 no intervalo da sub-rede ou deixe o campo em branco para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Salvar.

Para atribuir um endereço IPv6 usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- Use a opção `--ipv6-addresses` com o comando run-instances (AWS CLI)
- Use a propriedade `Ipv6Addresses` para `-NetworkInterface` no comando New-EC2Instance (AWS Tools for Windows PowerShell)
- assign-ipv6-addresses (AWS CLI)
- Register-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Cancelar a atribuição de um endereço IPv6 de uma instância

É possível cancelar a atribuição de um endereço IPv6 de uma instância a qualquer momento.

Para cancelar a atribuição de um endereço IPv6 de uma instância usando o console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), selecione Unassign (Cancelar atribuição) ao lado de endereços IPv6.
5. Escolha Salvar.

É possível cancelar a atribuição de um endereço IPv6 de uma instância usando a linha de comando.

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)

- Unregister-EC2Ipv6AddressList (AWS Tools for Windows PowerShell).

Diversos endereços IP para as instâncias do EC2

É possível especificar vários endereços IPv4 privados e endereços IPv6 para as instâncias. O número de interfaces de rede e de endereços de IPv4 e IPv6 privados que é possível especificar para uma instância depende do tipo da instância. Para obter mais informações, consulte Endereços IP por interface de rede por tipo de instância.

Pode ser útil atribuir vários endereços IP a uma instância na VPC para fazer o seguinte:

- Hospedar vários sites em um único servidor usando vários certificados SSL em um único servidor e associando cada certificado a um endereço IP específico.
- Operar aplicações de rede, como firewalls ou load balancers, que têm vários endereços IP para cada interface de rede.
- Redirecionar o tráfego interno para uma instância em espera em caso de falha na instância, atribuindo novamente o endereço IP secundário à instância em espera.

Tópicos

- Como funcionam vários endereços IP
- Trabalhar com vários endereços IPv4
- Trabalhar com vários endereços IPv6

Como funcionam vários endereços IP

A lista a seguir explica como vários endereços IP funcionam com interfaces de rede:

- É possível atribuir um endereço IPv4 privado secundário a qualquer interface de rede.
- É possível atribuir vários endereços IPv6 a uma interface de rede que esteja em uma sub-rede que tem um bloco CIDR IPv6 associado.
- É necessário escolher um endereço IPv4 secundário no intervalo de bloco CIDR IPv4 da sub-rede para a interface de rede.
- É necessário escolher endereços IPv6 no intervalo de bloco CIDR IPv6 da sub-rede para a interface de rede.

- Você associa grupos de segurança a interfaces de rede, não a endereços IP individuais. Portanto, cada endereço IP especificado em uma interface de rede está sujeito ao grupo de segurança de sua interface de rede.
- Vários endereços IP podem ser atribuídos e ter a atribuição cancelada para interfaces de rede anexadas ou instâncias paradas.
- Os endereços IPv4 privados secundários que são atribuídos a uma interface de rede podem ser atribuídos novamente para outra interface de rede se você permitir isso explicitamente.
- Um endereço IPv6 não pode ser atribuído novamente a outra interface de rede. É necessário primeiro cancelar a atribuição do endereço IPv6 da interface de rede existente.
- Ao atribuir vários endereços IP a uma interface de rede usando as ferramentas da linha de comando ou a API, a operação inteira falhará se um dos endereços IP não puder ser atribuído.
- Os endereços IPv4 privados primários, os endereços IPv4 privados secundários, os endereços IP elásticos e os endereços IPv6 permanecem com a interface de rede secundária quando ela é desanexada de uma instância ou anexada a uma instância.
- Embora não seja possível desanexar a interface de rede primária de uma instância, é possível atribuir novamente o endereço IPv4 privado secundário da interface de rede primária para outra interface de rede.

A lista a seguir explica como vários endereços IP funcionam com endereços IP elásticos (IPv4 somente):

- Cada endereço IPv4 privado pode ser associado a um único endereço IP elástico e vice-versa.
- Quando um endereço IPv4 privado secundário é atribuído novamente a outra interface, o endereço IPv4 privado secundário retém a associação a um endereço IP elástico.
- Quando a atribuição de um endereço IPv4 privado secundário é cancelada em uma interface, um endereço IP elástico associado é automaticamente desassociado do endereço IPv4 privado secundário.

Trabalhar com vários endereços IPv4

É possível atribuir um endereço IPv4 privado secundário a uma instância, associar um endereço IPv4 elástico a um endereço IPv4 privado secundário e cancelar a atribuição de um endereço IPv4 privado secundário.

Tarefas

- Atribuir um endereço IPv4 privado secundário
- Configuração do sistema operacional para reconhecer endereços IPv4 privados secundários
- Associar um endereço IP elástico ao endereço IPv4 privado secundário
- Visualizar endereços IPv4 privados secundários
- Cancelar a atribuição de um endereço IPv4 privado secundário

Atribuir um endereço IPv4 privado secundário

É possível atribuir o endereço IPv4 privado secundário à interface de rede para uma instância ao executar a instância ou após a instância estar em execução.

Para atribuir um endereço IPv4 privado secundário ao executar uma instância

1. Siga o procedimento para iniciar uma instância. Em Configurações de rede, escolha Editar.
2. Selecione uma VPC e uma sub-rede.
3. Expanda Configuração de rede avançada.
4. Em IP secundário, escolha Atribuir automaticamente e insira o número de endereços IP (a Amazon atribui automaticamente endereços IPv4 secundários) ou escolha Atribuir e inserir manualmente e insira os endereços IPv4.
5. Conclua as etapas restantes para iniciar a instância.

Para atribuir um endereço IPv4 secundário durante a execução usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- A opção `--secondary-private-ip-addresses` com o comando run-instances (AWS CLI)
- Defina `-NetworkInterface` e especifique o parâmetro `PrivateIpAddresses` com o comando New-EC2Instance (AWS Tools for Windows PowerShell).

Para atribuir um endereço IPv4 privado secundário a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione a interface de rede para a instância.

3. Escolha Ações, Gerenciar endereços IP.
4. Expanda a interface de rede. Em Endereços IPv4, escolha Atribuir novo endereço IP.
5. Insira um endereço IPv4 específico que esteja no intervalo da sub-rede para a instância ou deixe o campo em branco para permitir que a Amazon selecione um endereço IPv4 para você.
6. (Opcional) Escolha Permitir para permitir que o endereço IP privado secundário seja reatribuído se ele já estiver atribuído a outra interface de rede.
7. Escolha Salvar.

Como alternativa, é possível atribuir um endereço IPv4 privado secundário a uma instância. Escolha Instâncias no painel de navegação, selecione a instância, e escolha Ações, Redes, Gerenciar endereços IP. É possível configurar as mesmas informações que configurou nas etapas acima. O endereço IP é atribuído à interface de rede primária (eth0) da instância.

Para atribuir um endereço IPv4 privado secundário a uma instância existente usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- assign-private-ip-addresses (AWS CLI)
- Register-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Configuração do sistema operacional para reconhecer endereços IPv4 privados secundários

Depois de atribuir um endereço IPv4 privado secundário à instância, você precisa configurar o sistema operacional na instância para reconhecer o endereço IP privado secundário.

Instâncias do Linux

- Se estiver usando o Amazon Linux, o pacote ec2-net-utils poderá cuidar desta etapa para você. Ele configura interfaces de rede adicionais que você anexa enquanto a instância está em execução, atualiza os endereços IPv4 secundários durante a renovação da concessão DHCP e atualiza a regras de roteamento relacionadas. É possível atualizar a lista de interfaces imediatamente usando o comando `sudo service network restart` e, em seguida, visualizar a lista atualizada usando `ip addr li`. Se você precisar de controle manual sobre a configuração da rede, poderá remover o pacote ec2-net-utils. Para obter mais informações, consulte Configurar a interface de rede usando ec2-net-utils para Amazon Linux 2.

- Se estiver usando outra distribuição do Linux, consulte a documentação da distribuição do Linux. Procure informações sobre como configurar interfaces de rede adicionais e endereços IPv4 secundários. Se a instância tiver duas ou mais interfaces na mesma sub-rede, pesquise as informações sobre como usar as regras de roteamento para resolver roteamento assimétrico.

Instâncias do Windows

Para ter mais informações, consulte Configurar um endereço IPv4 privado secundário para uma instância do Windows..

Associar um endereço IP elástico ao endereço IPv4 privado secundário

Para associar um endereço IP elástico a um endereço IPv4 privado secundário

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Marcar a caixa de seleção para o endereço IP elástico
4. Escolha Ações, Associar endereço IP elástico.
5. Em Tipo de recurso, selecione Interface de rede. Selecione a interface de rede e o endereço IP secundário na lista Endereço IP privado.
6. Em Interface de rede, selecione a interface de rede. Selecione o endereço IP secundário na lista Endereço IP privado.
7. Em Endereço IP privado, selecione o endereço IP secundário.
8. Selecione Associar.

Para associar um endereço IP elástico a um endereço IPv4 privado secundário usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Visualizar endereços IPv4 privados secundários

Para visualizar os endereços IPv4 privados atribuídos a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Na guia Detalhes, em Endereços IP, localize Endereço IPv4 privado e Endereços IPv4 privados secundários.

Para visualizar os endereços IPv4 privados atribuídos a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção para a instância.
4. Na guia Redes, em Detalhes de rede, localize Endereços IPv4 privados e Endereços IPv4 privados secundários.

Cancelar a atribuição de um endereço IPv4 privado secundário

Se você não precisar mais de um endereço IPv4 privado secundário, poderá cancelar sua atribuição na instância ou na interface de rede. Quando a atribuição de um endereço IPv4 privado secundário é cancelada de uma interface de rede, o endereço IP elástico (se houver) também é desassociado.

Para cancelar a atribuição de um endereço IPv4 privado secundário de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância, escolha Ações, Redes, Gerencia endereços IP.
4. Expanda a interface de rede. Em Endereços IPv4, escolha Cancelar atribuição para cancelar a atribuição do endereço IPv4.
5. Escolha Salvar.

Para cancelar a atribuição de um endereço IPv4 privado secundário de uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede, escolha Ações, Gerenciar endereços IP.
4. Expanda a interface de rede. Em Endereços IPv4, escolha Cancelar atribuição para cancelar a atribuição do endereço IPv4.
5. Escolha Salvar.

Para cancelar a atribuição de um endereço IPv4 privado secundário usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- unassign-private-ip-addresses (AWS CLI)
- Unregister-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Trabalhar com vários endereços IPv6

É possível atribuir vários endereços IPv6 à instância, visualizar os endereços IPv6 atribuídos à instância e cancelar a atribuição de endereços IPv6 da instância.

Tópicos

- Atribuir vários endereços IPv6
- Visualizar os endereços IPv6
- Cancelar a atribuição de um endereço IPv6

Atribuir vários endereços IPv6

É possível atribuir um ou mais endereços IPv6 à instância durante ou após a execução. Para atribuir um endereço IPv6 a uma instância, a VPC e a sub-rede em que você executa a instância devem ter um bloco CIDR IPv6 associado.

Para atribuir vários endereços IPv6 durante a execução

1. Siga o procedimento para iniciar uma instância. Em Configurações de rede, escolha Editar.
2. Selecione uma VPC e uma sub-rede.
3. Expanda Configuração de rede avançada.

4. Em IPs IPv6, escolha Atribuir automaticamente e o número de endereços IP (a Amazon atribui automaticamente os endereços IPv6) ou escolha Atribuir e inserir manualmente e insira os endereços IPv6.
5. Conclua as etapas restantes para iniciar a instância.

É possível usar a tela Instances do console do Amazon EC2 para atribuir vários endereços IPv6 a uma instância existente. Isso atribui os endereços IPv6 à interface de rede primária (eth0) da instância. Para atribuir um endereço IPv6 específico à instância, verifique se o endereço IPv6 já não está atribuído a outra instância ou interface de rede.

Para atribuir vários endereços IPv6 a uma instância existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Ações, Redes, Gerenciar endereços IP.
4. Expanda a interface de rede. Em Endereços IPv6, escolha Atribuir novo endereço IP para cada endereço IPv6 que deseja adicionar. É possível especificar um endereço IPv6 no intervalo da sub-rede ou deixar o campo em branco para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Salvar.

Como alternativa, é possível atribuir vários endereços IPv6 a uma interface de rede existente. A interface de rede deve ter sido criada em uma sub-rede com um bloco CIDR IPv6 associado. Para atribuir um endereço IPv6 específico à interface de rede, assegure-se de que o endereço IPv6 já não tenha sido designado para outra interface de rede.

Para atribuir vários endereços IPv6 a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede, escolha Ações, Gerenciar endereços IP.
4. Expanda a interface de rede. Em Endereços IPv6, escolha Atribuir novo endereço IP para cada endereço IPv6 que deseja adicionar. É possível especificar um endereço IPv6 no intervalo da sub-rede ou deixar o campo em branco para permitir que a Amazon escolha um endereço IPv6 para você.

5. Escolha Salvar.

Visão geral da CLI

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- Atribuir um endereço IPv6 durante a execução:
  - Use a opção `--ipv6-addresses` ou `--ipv6-address-count` com o comando run-instances (AWS CLI)
  - Defina `-NetworkInterface` e especifique os parâmetros `Ipv6Addresses` ou `Ipv6AddressCount` com o comando New-EC2Instance (AWS Tools for Windows PowerShell).
- Atribuir um endereço IPv6 a uma interface de rede:
  - assign-ipv6-addresses (AWS CLI)
  - Register-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Visualizar os endereços IPv6

É possível visualizar os endereços IPv6 de uma instância ou de uma interface de rede.

Para visualizar os endereços IPv6 privados atribuídos a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção para sua instância.
4. Na guia Redes, localize o campo Endereços IPv6.

Para visualizar os endereços IPv6 atribuídos a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para sua interface de rede.
4. Na guia Detalhes, em Endereços IP, localize o campo Endereços IPv6.

Visão geral da CLI

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- Visualizar endereços IPv6 de uma instância:
  - describe-instances (AWS CLI)
  - Get-EC2InstanceAWS Tools for Windows PowerShell
- Para visualizar os endereços IPv6 de uma interface de rede:
  - describe-network-interfaces (AWS CLI)
  - Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Cancelar a atribuição de um endereço IPv6

É possível cancelar a atribuição de um endereço IPv6 da interface de rede primária de uma instância ou cancelar a atribuição de um endereço IPv6 de uma interface de rede.

Para cancelar a atribuição de um endereço IPv6 de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da sua instância e escolha Ações, Redes, Gerenciar endereços IP.
4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), selecione Unassign (Cancelar atribuição) ao lado de endereços IPv6.
5. Escolha Salvar.

Para cancelar a atribuição de um endereço IPv6 de uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção da sua interface de rede e, em seguida, escolha Ações, Gerenciar endereços IP.
4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), selecione Unassign (Cancelar atribuição) ao lado de endereços IPv6.
5. Escolha Salvar.

Visão geral da CLI

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2Ipv6AddressList (AWS Tools for Windows PowerShell)

Configurar um endereço IPv4 privado secundário para uma instância do Windows.

É possível especificar vários endereços IPv4 privados para as instâncias. Depois de atribuir um endereço IPv4 privado secundário a uma instância, você precisa configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado secundário.

> **Note**
>
> Essas instruções são baseadas no Windows Server 2022. A implantação dessas etapas pode variar dependendo do sistema operacional da instância do Windows.

Tarefas

- Pré-requisitos
- Etapa 1: configurar o endereçamento IP estático na sua instância
- Etapa 2: Configurar um endereço IP privado secundário para a instância
- Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário

Pré-requisitos

1. Atribua o endereço IPv4 privado secundário à interface de rede para a instância. É possível atribuir o endereço IPv4 privado secundário ao iniciar a instância ou após a instância estar em execução. Para obter mais informações, consulte Atribuir um endereço IPv4 privado secundário.
2. Aloque um endereço de IP elástico ao endereço IPv4 privado secundário. Para ter mais informações, consulte Alocar um endereço IP elástico e Associar um endereço IP elástico ao endereço IPv4 privado secundário.

Etapa 1: configurar o endereçamento IP estático na sua instância

Para permitir que sua instância do Windows use vários endereços IP, configure sua instância para usar o endereçamento IP estático em vez de um servidor DHCP.

> **Important**
>
> Quando você configura o endereçamento IP estático na sua instância, o endereço IP deve corresponder exatamente o que é exibido no console, na CLI ou na API. Se você inserir esses endereços IP incorretamente, a instância poderia tornar-se inacessível.

Para configurar o endereçamento IP estático em uma instância do Windows

1. Conecte-se à sua instância.
2. Encontre o endereço IP, a máscara da sub-rede e os endereços gateway padrão para a instância ao executar as seguintes etapas:
   - Execute o seguinte comando no PowerShell:

     ```
     ipconfig /all
     ```

     Examine a saída e anote os valores de Endereço IPv4, Máscara de sub-rede, Gateway padrão e Servidores DNS da interface de rede. A saída deve ser semelhante ao exemplo apresentado a seguir:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
        Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
     ```

```
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCP Server . . . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

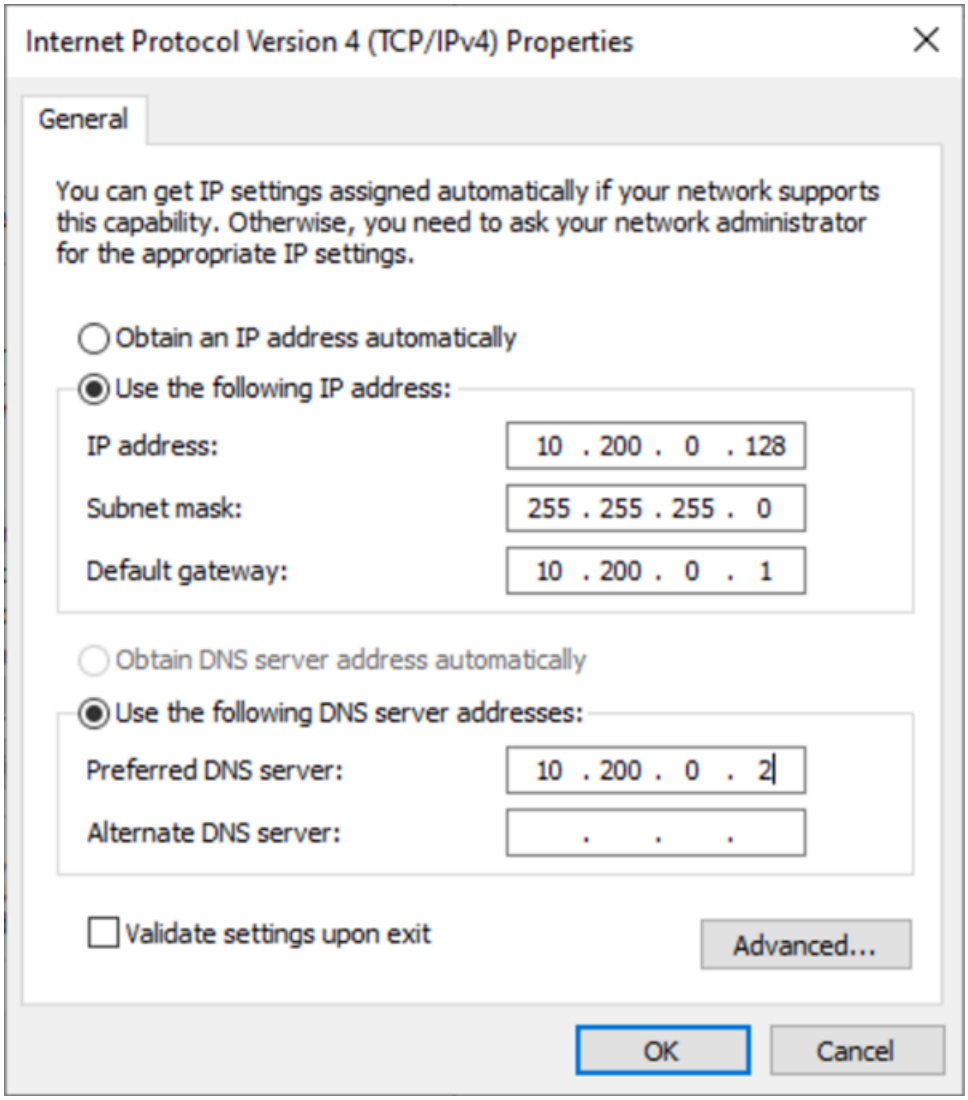
3. Abra o Centro de Rede e Compartilhamento executando o seguinte comando no PowerShell:

```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Abra o menu contextual (botão direito do mouse) para interface de rede (Conexão Local ou Ethernet) e selecione Propriedades.
5. Escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades.
6. Na caixa de diálogo Propriedades do Protocolo TCP/IP Versão 4 (TCP/IPv4), selecione Usar o seguinte endereço IP, insira os valores a seguir e escolha OK.

Campo	Valor
IP address	O endereço IPv4 obtido na etapa 2 acima.
Máscara de sub-rede	A máscara de sub-rede obtida na etapa 2 acima.
Gateway padrão	O endereço do gateway padrão obtido na etapa 2 acima.
Servidor DNS preferido	O servidor DNS obtido na etapa 2 acima.
Servidor DNS alternativo	O servidor DNS alternativo obtido na etapa 2 acima. Se um servidor DNS alternativo não estiver listado, deixe esse campo em branco.

> **Important**
>
> Se você definir o endereço IP para qualquer valor além do endereço IP atual, perderá conectividade com a instância.



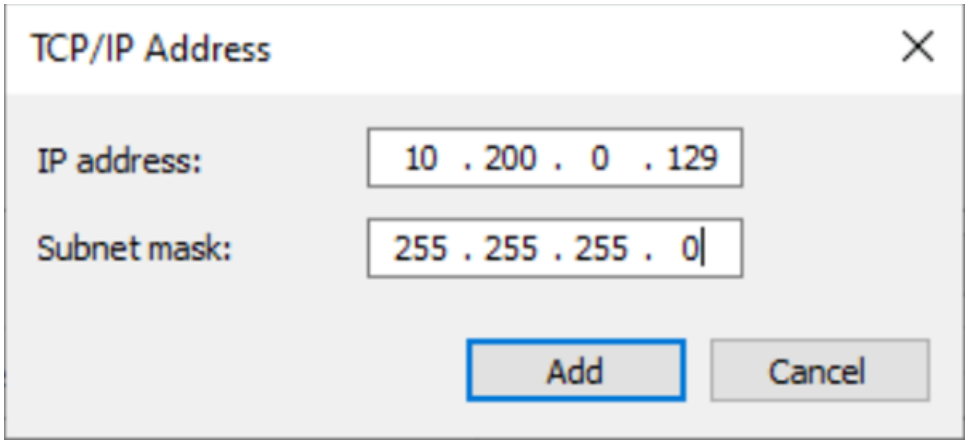
Você perderá conectividade do RDP com a instância do Windows por alguns segundos enquanto a instância converte entre uso de DHCP para endereçamento estático. A instância retém a mesma informação de endereços IP que antes, mas agora essa informação é estática e não é gerenciada por DHCP.

Etapa 2: Configurar um endereço IP privado secundário para a instância

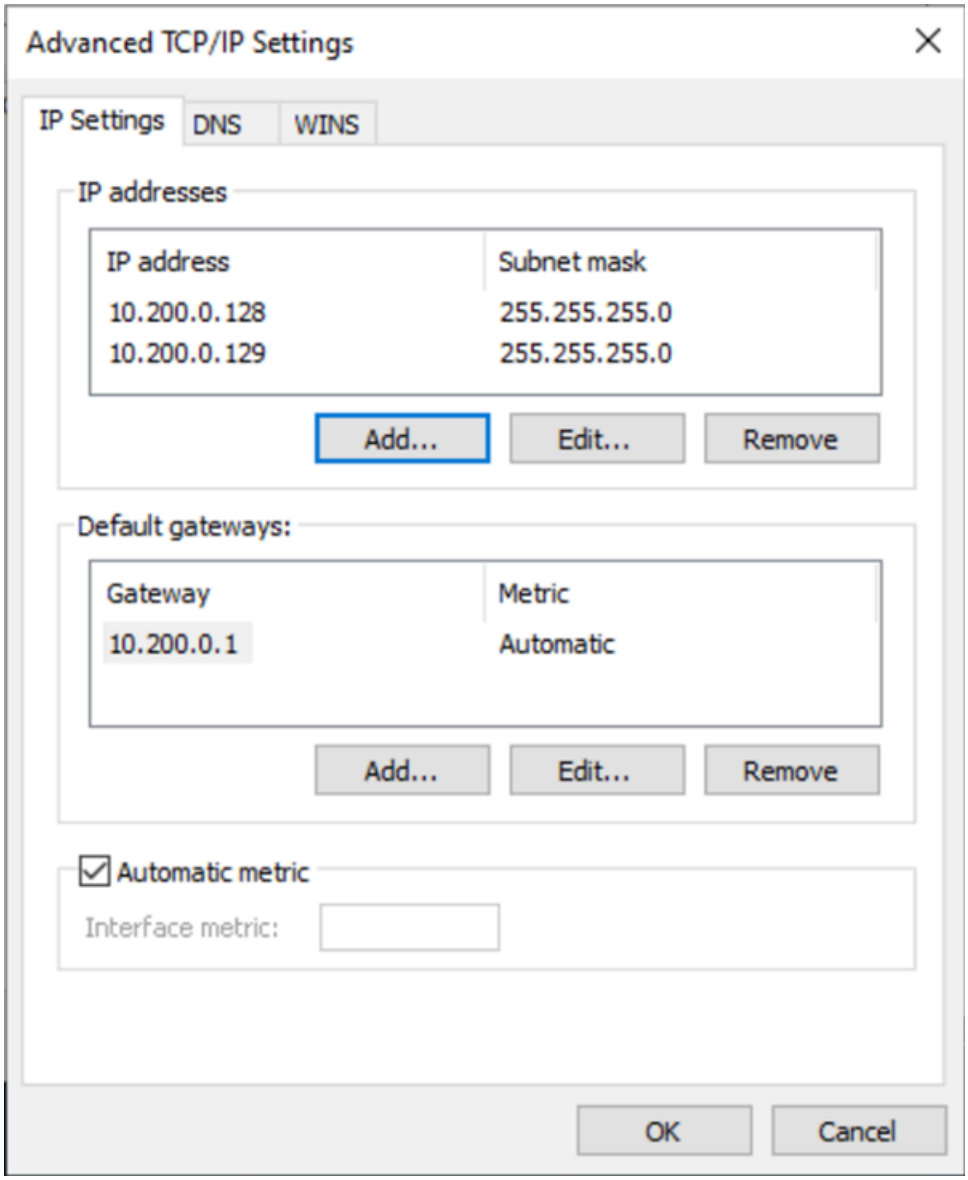
Depois de configurar o endereçamento IP estático na sua instância do Windows, você estará pronto para preparar um segundo endereço IP privado.

Como configurar um endereço IP secundário

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Na (Networking (Rede), observe o endereço IP secundário.
4. Conecte-se à sua instância.
5. Na sua instância do Windows, selecione Iniciar, Painel de Controle.
6. Escolha Rede e Internet, Central de Rede e Compartilhamento.
7. Selecione a interface de rede (Conexão Local ou Ethernet) e escolha Propriedades.
8. Na página Propriedades da Conexão Local, escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades, Avançado.
9. Escolha Adicionar.
10. Na caixa de diálogo Endereço TCP/IP, digite o endereço IP privado secundário para o endereço IP. Em Subnet mask (Máscara de sub-rede), digite a mesma máscara de sub-rede inserida para o endereço IP privado primário em Etapa 1: configurar o endereçamento IP estático na sua instância e selecione Add (Adicionar).



11. Verifique as configurações de endereço IP e selecione OK.



12. Escolha OK, Fechar.
13. Para confirmar se o endereço IP secundário foi adicionado ao sistema operacional, execute o comando `ipconfig /all` no PowerShell. A saída deve ser semelhante à seguinte:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
```

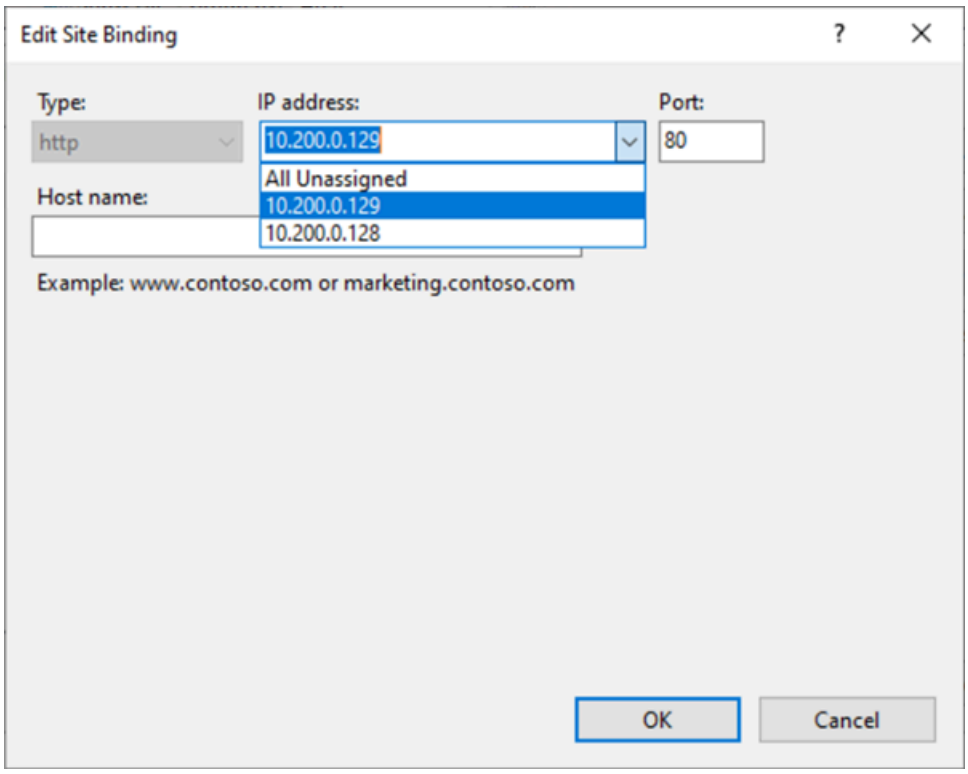
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário

É possível configurar quaisquer aplicações para usar o endereço IP privado secundário. Por exemplo, se sua instância estiver executando um site no IIS, é possível configurar o IIS para usar o endereço IP privado secundário.

Para configurar o IIS para usar o endereço IP privado secundário

1. Conecte-se à sua instância.
2. Abra o Gerenciador do Serviços de Informações da Internet (IIS).
3. No painel Conexões, expanda Sites.
4. Abra o menu contextual (botão direito do mouse) para seu site ou selecione Editar Ligações.
5. Na caixa de diálogo Ligações do Site, para Tipo, escolha http, Editar.
6. Na caixa de diálogo Editar Ligação do Site, para Endereço IP, selecione o endereço IP privado secundário. (Por padrão, cada site aceita solicitações HTTP de todos os endereços IP.)



7. Escolha OK, Fechar.

Hostnames de instância do EC2

Quando você cria uma instância do EC2, o AWS cria um hostname para essa instância. Para obter mais informações sobre os tipos de nome de host e como são provisionados pela AWS, consulte Tipos de nome de host de instância do Amazon EC2. A Amazon fornece um servidor DNS que resolve hostnames fornecidos pela Amazon em endereços IPv4 e IPv6. O servidor DNS da Amazon está localizado na base de seu intervalo de rede VPC mais dois. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC.

Endereços locais de link

Os endereços de link local são endereços IP bem conhecidos e não roteáveis. O Amazon EC2 usa endereços do espaço de endereços locais de link para fornecer serviços que são acessíveis somente por uma instância do EC2. Esses serviços não são executados na instância, mas sim no host subjacente. Ao acessar os endereços locais de link desses serviços, você está se comunicando com o hipervisor Xen ou o controlador do Nitro.

Intervalos de endereços locais de link

- IPv4: 169.254.0.0/16 (169.254.0.0 a 169.254.255.255)
- IPv6: fe80::/10

Serviços acessados usando endereços locais de link

- Serviço de metadados da instância
- Amazon Route 53 Resolver (também conhecido como servidor DNS da Amazon)
- Serviço de Sincronização Temporal da Amazon

Tipos de nome de host de instância do Amazon EC2

Esta seção descreve os tipos de nome de host do sistema operacional da instância do Amazon EC2 disponíveis quando você inicia instâncias em sub-redes da VPC.

O nome do host distingue as instâncias do EC2 em sua rede. Você pode usar o nome de host de uma instância se, por exemplo, quiser executar scripts para se comunicar com algumas ou todas as instâncias de sua rede.

Conteúdo

- Tipos de nomes de host do EC2
- Onde encontrar o nome do recurso e o nome de IP
- Como decidir se deseja escolher o nome do recurso ou o nome de IP
- Modificar configurações de tipo de nome de host e nome de host DNS

Tipos de nomes de host do EC2

Existem dois tipos de hostnames para o hostname do sistema operacional guest quando as instâncias do EC2 são executadas em uma VPC:

- IP name (Nome de IP): o esquema de nomenclatura herdado em que, quando você inicia uma instância, o endereço IPv4 privado da instância está incluído no nome de host da instância. O nome de IP existe durante todo o ciclo de vida da instância do EC2. Quando usado como hostname de DNS privado, ele só retorna o endereço IPv4 privado (registro A).

- Resource name (Nome do recurso): quando você inicia uma instância, o ID da instância do EC2 está incluído no nome de host da instância. O nome do recurso existe durante todo o ciclo de vida da instância do EC2. Quando usado como hostname de DNS privado, ele pode retornar o endereço IPv4 privado (registro A) e/ou o endereço IPv6 Global Unicast (registro AAAA).

O tipo de nome de host do sistema operacional convidado da instância do EC2 depende das configurações de sub-rede:

- Se a instância for iniciada em uma sub-rede somente IPv4, será possível selecionar nome de IP ou nome do recurso.
- Se a instância for iniciada em uma sub-rede de pilha dual (IPv4+IPv6), será possível selecionar nome de IP ou nome do recurso.
- Se a instância for iniciada em uma sub-rede somente IPv6, o nome do recurso será usado automaticamente.

Conteúdo

- Nome de IP
- Nome do recurso
- Diferença entre o nome de IP e o nome do recurso

Nome de IP

Quando você inicia uma instância do EC2 com o Hostname type (Tipo de nome de host) de IP name (Nome de IP), o nome de host do sistema operacional convidado será configurado para usar o endereço IPv4 privado.

- Formato para uma instância em us-east-1: *`private-ipv4-address`*`.ec2.internal`
- Exemplo: *`ip-10-24-34-0`*`.ec2.internal`
- Formato para uma instância em qualquer outra região da AWS: *`private-ipv4-address.region`*`.compute.internal`
- Exemplo: *`ip-10-24-34-0.us-west-2`*`.compute.internal`

Nome do recurso

Quando você inicia instâncias do EC2 em sub-redes somente IPv6, o Hostname type (Tipo de nome de host) do Resource name (Nome do recurso) é selecionado por padrão. Quando você inicia uma instância em sub-redes somente IPv4 ou pilha dupla (IPv4+IPv6), é possível selecionar a opção Resource name (Nome do recurso). Após iniciar uma instância, é possível gerenciar a configuração de nome de host. Para ter mais informações, consulte Modificar configurações de tipo de nome de host e nome de host DNS.

Quando você inicia uma instância do EC2 com um Hostname type (Tipo de nome de host) de Resource name (Nome de recurso), o hostname do sistema operacional convidado é configurado para usar o ID da instância do EC2.

- Formato para uma instância em us-east-1: *ec2-instance-id*.ec2.internal
- Exemplo: *i-0123456789abcdef*.ec2.internal
- Formato para uma instância em qualquer outra região da AWS: *ec2-instance-id.region*.compute.internal
- Exemplo: *i-0123456789abcdef.us-west-2*.compute.internal

Diferença entre o nome de IP e o nome do recurso

Consultas ao DNS para nomes de IP e nomes de recurso coexistem para garantir compatibilidade com versões anteriores e permitir a migração de nomenclatura baseada em IP para nomes de host para nomenclatura baseada em recursos. Para hostnames de DNS privados baseados em nomes de IP, você não pode configurar se uma consulta de registro de DNS A para a instância é respondida ou não. As consultas de registro de DNS A são sempre respondidas independentemente das configurações de nome de host do sistema operacional convidado. Entretanto, para nomes de host de DNS privados baseados em nome do recurso, é possível configurar se as consultas de DNS A ou DNS AAAA para a instância são respondidas ou não. Você configura o comportamento de resposta quando inicia uma instância ou modifica uma sub-rede. Para ter mais informações, consulte Modificar configurações de tipo de nome de host e nome de host DNS.

Onde encontrar o nome do recurso e o nome de IP

Esta seção descreve onde encontrar os tipos de nome de host do nome do recurso e o nome de IP no console do EC2.

Conteúdo

- Ao criar uma instância do EC2
- Ao visualizar os detalhes de uma instância do EC2 existente

Ao criar uma instância do EC2

Quando você cria uma instância do EC2, dependendo do tipo de sub-rede selecionada, Hostname type (Tipo de nome de host) de Resource name (Nome de recurso) pode estar disponível ou pode estar selecionada e não poder ser modificada. Esta seção explica em que cenários você encontra os tipos de nome de host do nome do recurso e o nome de IP.

Cenário 1

Crie uma instância do EC2 no assistente (consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta) e, ao configurar os detalhes, escolha uma sub-rede que você configurou para ser somente IPv6.

Neste caso, Hostname type (Tipo de nome de host) de Resource name (Nome do recurso) é selecionado automaticamente e não pode ser modificado. As opções de DNS Hostname (Nome de host DNS) em Enable IP name IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 [registro A] de nome de IP) e Enable resource-based IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 [registro A] baseadas em recursos) são desmarcadas automaticamente, não sendo possível modificá-las. A opção Enable resource-based IPv6 (AAAA record) DNS requests (Habilitar solicitações DNS IPv6 [registro AAAA] baseadas em recursos) é selecionada por padrão, mas é possível modificá-la. Se estiver selecionada, as solicitações DNS para o nome do recurso serão resolvidas como o endereço IPv6 (registro AAAA) dessa instância do EC2.

Cenário 2

Crie uma instância do EC2 no assistente (consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta) e, ao configurar os detalhes, escolha uma sub-rede configurada com um bloco CIDR IPv4 ou um bloco CIDR IPv4 e IPv6 (“pilha dupla”).

Nesse caso, a opção Enable IP name IPV4 (A record) DNS requests (Habilitar solicitações DNS de IPV4 de nome de IP [registro A]) é selecionada automaticamente e não pode ser alterada. Isso significa que as solicitações para o nome IP serão resolvidas como o endereço IPv4 (registro A) dessa instância do EC2.

As opções são padrão para as configurações da sub-rede, mas é possível modificar as opções para essa instância, dependendo das configurações de sub-rede:

- Hostname type (Tipo de nome de host): determina se você deseja que o nome de host do sistema operacional convidado da instância do EC2 seja o nome do recurso ou o nome de IP. O valor padrão é IP name (Nome de IP).
- Enable resource-based IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 baseado em recursos [registro A]): determina se as solicitações ao nome do recurso são resolvidas como o endereço IPv4 privado (registro A) dessa instância do EC2. Essa opção não é selecionada por padrão.
- Enable resource-based IPv6 (AAAA record) DNS requests (Habilitar solicitações DNS IPv6 baseado em recursos [registro AAAA]): determina se as solicitações ao nome do recurso são resolvidas como o endereço GUA IPv6 (registro AAAA) dessa instância do EC2. Essa opção não é selecionada por padrão.

Ao visualizar os detalhes de uma instância do EC2 existente

É possível ver os valores do nome de host de uma instância do EC2 existente na guia Details (Detalhes) para a instância do EC2:

- Hostname type (Tipo de nome de host): o nome de host em nome de IP ou formato de nome do recurso.
- Private IP DNS name (IPv4 only) (Nome de DNS do IP privado [somente IPv4]): o nome de IP que sempre é resolvido como o endereço IPv4 privado da instância.
- Private resource DNS name (Nome de DNS de recurso privado): o nome do recurso que pode ser resolvido como registros de DNS para essa instância.
- Answer private resource DNS name (Responder ao nome de DNS de recurso privado): o nome de recurso é resolvido como registros de DNS IPv4 (A), IPv6 (AAAA) ou IPv4 e IPv6 (A e AAAA).

Além disso, se você se conectar à instância do EC2 diretamente por SSH e inserir o comando `hostname`, verá o nome de host no formato nome de IP ou nome do recurso.

Como decidir se deseja escolher o nome do recurso ou o nome de IP

Ao iniciar uma instância do EC2 (consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta), se você escolher um Hostname type (Tipo de nome de host) do Resource name (Nome do recurso), a instância do EC2 será executada com um nome de host no formato de nome do recurso. Nesses casos, o registro DNS dessa instância do EC2 também poderá apontar para o nome do recurso. Isso permite a flexibilidade de escolher se esse nome de

host será resolvido para o endereço IPv4, o endereço IPv6 ou para ambos os endereços IPv4 e IPv6 da instância. Se você planeja usar o IPv6 no futuro ou se estiver usando sub-redes de pilha dupla atualmente, é melhor usar um Hostname type (Tipo de nome de host) do Resource name (Nome do recurso) para alterar a resolução de DNS para os nomes de host de suas instâncias sem fazer alterações nos registros DNS por conta própria. O nome do recurso permite adicionar e remover a resolução de DNS IPv4 e IPv6 em uma instância do EC2.

Se, em vez disso, você escolher um Hostname type (Tipo de nome de host) de IP name (Nome de IP) e usá-lo como nome de host DNS, ele só poderá resolver para o endereço IPv4 da instância. Ele não será resolvido para o endereço IPv6 da instância, mesmo que a instância tenha um endereço IPv4 e um endereço IPv6 associado a ela.

Modificar configurações de tipo de nome de host e nome de host DNS

Siga as etapas desta seção para modificar as configurações de tipo de nome de host e nome de host DNS para sub-redes ou instâncias do EC2 depois que forem iniciadas.

Conteúdo

- Subredes
- Instâncias do EC2

Subredes

Modifique as configurações de uma sub-rede selecionando uma sub-rede no console da VPC e escolhendo Actions (Ações), Edit subnet settings (Editar configurações da sub-rede).

> **Note**
>
> Alterar as configurações de sub-rede não altera a configuração das instâncias do EC2 que já foram executadas na sub-rede.

- Hostname type (Tipo de nome de host): determina se você deseja que a configuração padrão de nome de host do sistema operacional convidado da instância do EC2 iniciada na sub-rede seja o nome do recurso ou o nome de IP.
- Enable DNS hostname IPv4 (A record) requests (Habilitar solicitações de nome de host DNS IPv4 (registro A)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv4 (registro A) privado dessa instância do EC2.

- Enable DNS hostname IPv6 (A record) requests (Habilitar solicitações de nome de host DNS IPv6 (registro AAAA)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv4 (registro A) desta instância do EC2.

Instâncias do EC2

Siga as etapas desta seção para modificar as configurações de tipo de nome de host e nome de host DNS para uma instância do EC2.

> **Important**
>
> - Para alterar a configuração Use resource based namingas guest OS hostname (Usar nomenclatura baseada em recursos como nome de host do sistema operacional convidado), primeiro é necessário interromper a instância. Para alterar as configurações Answer DNS hostname IPv4 (A record) request (Responder solicitação de hostname DNS IPv4 (registro A)) Answer DNS hostname IPv6 (AAAA record) requests ((Responder solicitação de hostname DNS IPv6 (registro A)), você não precisa interromper a instância.
> - Para modificar qualquer uma das configurações para tipos de instância EC2 sem suporte do EBS, não será possível interromper a instância. É necessário terminar a instância e iniciar uma nova instância com as configurações de tipo de nome de host e nome de host DNS desejadas.

Como modificar o tipo de nome de host e as configurações de nome de host DNS para uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Se você for alterar a configuração Use resource based naming as guest OS hostname (Usar nomenclatura baseada em recursos como nome de host do sistema operacional convidado), primeiro interrompa a instância do EC2. Caso contrário, ignore essa etapa.

   Para interromper a instância, selecione-a e escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
3. Selecione a instância e escolha Actions (Ações), Instance settings (Configurações da instância), Change resource based naming options (Alterar opções de nomenclatura baseada em recurso).

- Use resource based naming as guest OS hostname (Usar nomenclatura baseada em recursos como nome de host do sistema operacional convidado): determina se você deseja que o nome de host do sistema operacional convidado da instância do EC2 seja o nome do recurso ou o nome de IP.
- Answer DNS hostname IPv4 (A record) requests (Responder solicitações de nome de host DNS IPv4 (registro A)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv4 privado desta instância do EC2.
- Answer DNS hostname IPv6 (AAAA record) requests (Responder solicitações de nome de host DNS IPv6 (registro AAAA)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv6 (registro AAAA) desta instância do EC2.

4. Escolha Salvar.
5. Se você interrompeu a instância, inicie-a novamente.

Traga seus próprios endereços IP (BYOIP) no Amazon EC2

É possível trazer parte ou todo o seu intervalo de endereços IPv4 ou IPv6 publicamente roteáveis da rede on-premises para sua conta da AWS. Você continua controlando o intervalo de endereços e pode anunciar o intervalo de endereços na Internet via AWS. Depois de levar o intervalo de endereços para a AWS, ele aparecerá em sua conta da AWS como um grupo de endereços.

Para obter uma lista das regiões em que o BYOIP está disponível, consulte Disponibilidade regional.

> **Note**
>
> - As etapas nesta página descrevem como trazer seu próprio intervalo de endereços IP para uso somente no Amazon EC2.
> - Para trazer seu próprio intervalo de endereços IP para uso no AWS Global Accelerator, consulte Trazer seus próprios endereços IP (BYOIP) no Guia do desenvolvedor do AWS Global Accelerator.
> - Para usar seu próprio intervalo de endereços IP para uso no Amazon VPC IP Address Manager, consulte o Tutorial: traga seus endereços IP para o IPAM no Guia do usuário do IPAM da Amazon VPC.

Conteúdo

- Definições BYOIP
- Requisitos e cotas
- Pré-requisitos de integração para seu intervalo de endereços BYOIP
- Integração do BYOIP
- Trabalhar com o intervalo de endereços
- Validar o BYOIP
- Disponibilidade regional
- Disponibilidade da zona local
- Saiba mais

Definições BYOIP

- Certificado autoassinado X.509: um padrão de certificado mais comumente usado para criptografar e autenticar dados dentro de uma rede. É um certificado usado pela AWS para validar o controle do espaço IP a partir de um registro RDAP. Para obter mais informações sobre certificados X.509, consulte RFC 3280.
- Número de sistema autônomo (ASN): um identificador global exclusivo que define um grupo de prefixos de IP executados por uma ou mais operadoras de rede que mantêm uma política de roteamento única e claramente definida.
- Registro regional da Internet (RIR): uma organização que gerencia a alocação e o registro de endereços IP e ASNs em uma região do mundo.
- Registry Data Access Protocol (RDAP): um protocolo somente de leitura para consultar dados de registro atuais em um RIR. As entradas no banco de dados do RIR consultado são chamadas de “registros RDAP”. Certos tipos de registros precisam ser atualizados pelos clientes por meio de um mecanismo fornecido pelo RIR. Esses registros são consultados pela AWS para verificar o controle de um espaço de endereço no RIR.
- Autorização de origem de rota (ROA): um objeto criado por RIRs para que os clientes autentiquem anúncios IP em sistemas autônomos específicos. Para obter uma visão geral, consulte Autorizações de origem de rota (ROAs) no site do ARIN.
- Registro local da Internet (LIR):: organizações, como provedores de serviços de Internet, que alocam um bloco de endereços IP de um RIR para seus clientes.

Requisitos e cotas

- O intervalo de endereços deve ser registrado no seu Registro Regional da Internet (RIR). Consulte seu RIR para ver quaisquer políticas relacionadas a regiões geográficas. O BYOIP atualmente oferece suporte ao registro no American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) ou no Asia-Pacific Network Information Centre (APNIC). Ele deve ser registrado para uma entidade empresarial ou institucional e não pode ser registrado para uma única pessoa.
- O intervalo de endereços IPv4 mais específico que é possível trazer é /24.
- O intervalo mais específico de endereços IPv6 que é possível trazer é /48 para CIDRs anunciáveis publicamente e /56 para CIDRs que não são anunciáveis publicamente.
- As ROAs não são necessárias para intervalos CIDR que não são anunciáveis publicamente, mas os registros RDAP ainda precisam ser atualizados.
- É possível trazer cada intervalo de endereços para uma região da AWS de cada vez.
- É possível trazer um total de cinco intervalos de endereços IPv4 e IPv6 BYOIP por região da AWS para sua conta da AWS. Não é possível ajustar as cotas para CIDRs BYOIP usando o console do Service Quotas, mas você pode solicitar um aumento da cota entrando em contato com o AWS Support Center, conforme descrito em Cotas de serviços da AWS, na Referência geral da AWS.
- Você não pode compartilhar seu intervalo de endereços IP com outras contas usando AWS RAM a menos que você use o IP Address Manager (IPAM) da Amazon VPC e integre o IPAM com o AWS Organizations. Para obter mais informações, consulte Integrar IPAM com o AWS Organizations no Guia do usuário do Amazon VPC IPAM.
- Os endereços no intervalo de endereços IP devem ter um histórico limpo. Podemos investigar a reputação do intervalo de endereços IP e reservar o direito de rejeitar um intervalo de endereços IP, se ele contiver um endereço IP que tenha má reputação ou esteja associado a comportamento mal-intencionado.
- O espaço de endereço herdado, o espaço de endereço IPv4 que foi distribuído pelo registro central da Internet Assigned Numbers Authority (IANA) antes da formação de Regional Internet Registries (RIR), ainda requer um objeto ROA correspondente.
- Para LIRs, é comum o uso de um processo manual para atualizar os registros. Dependendo do LIR, a implantação pode levar dias.
- Um único objeto ROA e registro RDAP são necessários para um bloco CIDR grande. É possível trazer vários blocos CIDR menores desse intervalo para a AWS, mesmo em várias regiões da AWS, usando o único objeto e registro.

- Não há suporte para BYOIP em zonas de comprimento de onda ou em AWS Outposts.
- Não faça alterações manuais no BYOIP no RADb ou em qualquer outro IRR. O BYOIP atualizará automaticamente o RADb. Qualquer alteração manual que inclua o ASN do BYOIP fará com que a operação de provisão do BYOIP falhe.
- Se você trouxer um intervalo de endereços IPv4 para a AWS, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Pré-requisitos de integração para seu intervalo de endereços BYOIP

O processo de integração do BYOIP tem duas fases, para as quais é necessário executar três etapas. Essas etapas estão descritas no diagrama a seguir. Incluímos etapas manuais nesta documentação, mas seu RIR pode oferecer serviços gerenciados para ajudar você nessas etapas.

Fase de preparação

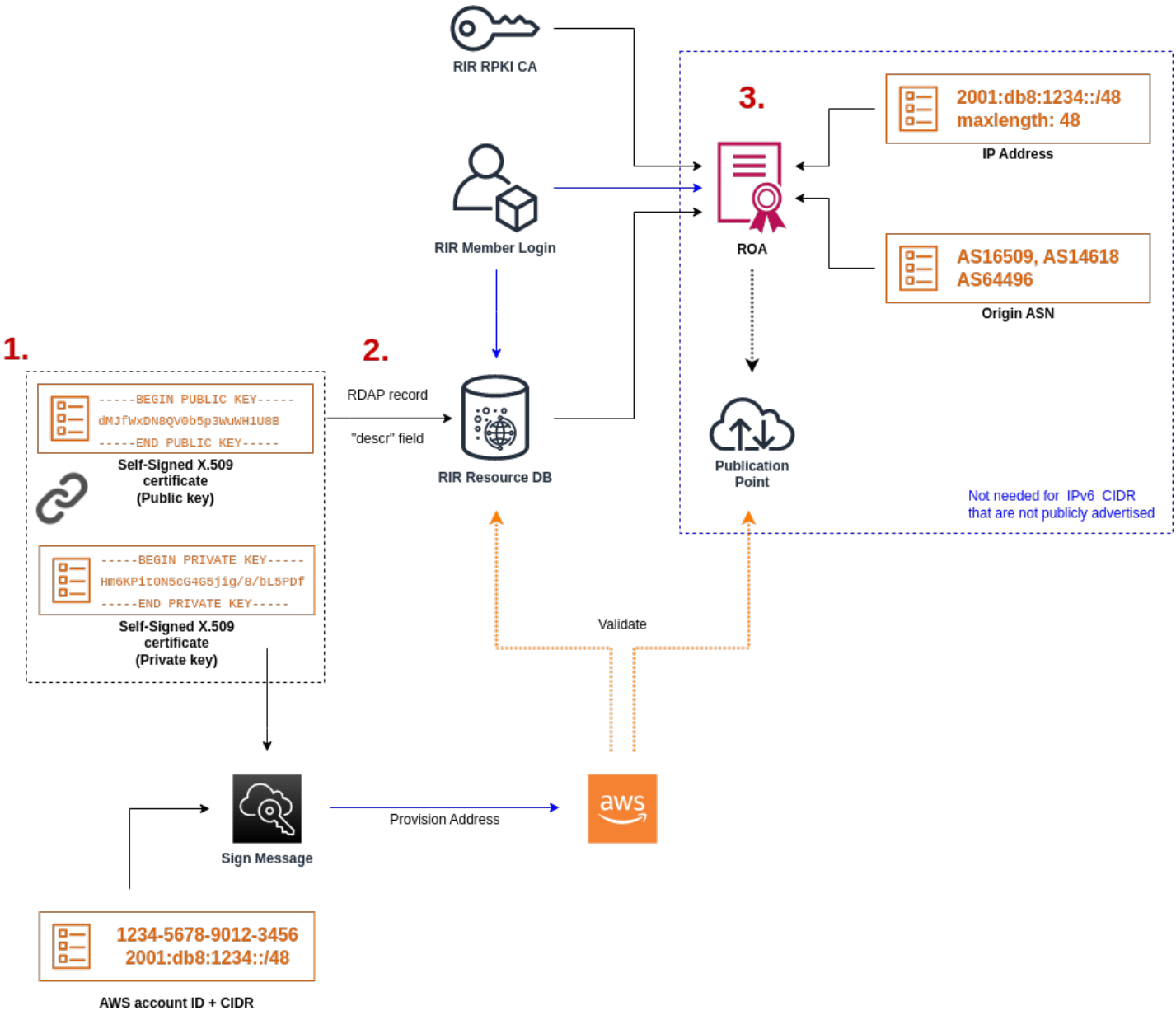
1. Crie uma chave privada e utilize-a para gerar um certificado X.509 autoassinado para fins de autenticação. Esse certificado é usado somente durante a fase de provisionamento.

Fase de configuração do RIR

2. Carregue o certificado autoassinado nos comentários do registro RDAP.

3. Criar um objeto ROA no seu RIR. Uma ROA define o intervalo de endereços desejado, os Autonomous System Numbers (ASNs – Números de Sistema Autônomo) autorizados a anunciar o intervalo de endereços e uma data de validade para registro do RIR na Resource Public Key Infrastructure (RPKI – Infraestrutura de Chave Pública de Recursos).

> **Note**
>
> Não é necessário ter uma ROA para o espaço de endereços IPv6 não anunciáveis publicamente.



Para trazer vários intervalos de endereços, é necessário repetir esse processo com cada um deles. No entanto, as etapas de preparação e configuração do RIR não precisam ser repetidas, basta dividir um bloco contíguo em várias regiões da AWS diferentes.

Colocar em um intervalo de endereços não tem efeito em quaisquer intervalos de endereços que você trouxe anteriormente.

> **Important**
>
> Antes de integrar seu intervalo de endereços, preencha os seguintes pré-requisitos. As tarefas nesta seção exigem um terminal Linux e podem ser executadas usando o Linux, o AWS CloudShell ou o Subsistema Windows para Linux..

1. Crie uma chave privada e gere um certificado X.509

Siga o procedimento a seguir para criar um certificado autoassinado X.509 e adicione-o ao registro RDAP para seu RIR. Esse par de chaves é usado para autenticar o intervalo de endereços com o RIR. Os comandos openssl requerem o OpenSSL versão 1.0.2 ou posterior.

Copie os comandos a seguir e substitua apenas os valores de espaço reservado (em texto itálico colorido).

Esse procedimento segue a prática recomendada de criptografar sua chave RSA privada e exigir uma frase para acessá-la.

1. Gere uma chave privada RSA de 2048 bits, como mostrado a seguir.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

   O parâmetro `-aes256` especifica o algoritmo usado para criptografar a chave privada. O comando retorna a seguinte saída, incluindo prompts para definir uma frase de acesso:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

   É possível fazer inspecionar a chave pública com o seguinte comando:

```
$ openssl pkey -in private-key.pem -text
```

   Isso retorna um prompt de frase de acesso e o conteúdo da chave, que deve ser semelhante ao seguinte:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
```

```
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
```

```
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Mantenha sua chave privada em um local seguro quando ela não estiver em uso.

2. Gere um certificado X.509 usando a chave privada criada na etapa anterior. Neste exemplo, o certificado expira em 365 dias, após o qual ele não é mais confiável. Defina a expiração adequadamente. O certificado apenas deve ser válido durante o processo de provisionamento. Você poderá remover o certificado do seu registro do RIR após a conclusão do provisionamento. O comando `tr -d "\n"` remove caracteres de nova linha (quebras de linha) da saída. Você precisa fornecer um nome comum quando solicitado, mas os outros campos podem ser deixados em branco.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Isso resulta em uma saída semelhante à seguinte:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> O nome comum não é necessário para provisionamento da AWS. Pode ser qualquer nome de domínio interno ou público.

É possível inspecionar o certificado usando o seguinte comando:

```
$ cat certificate.pem
```

A saída deve ser uma string longa, codificada em PEM, sem quebras de linha, prefaciada por `-----BEGIN CERTIFICATE-----` e seguida por `-----END CERTIFICATE-----`.

2. Carregue o certificado X.509 no registro RDAP no RIR

Adicione o certificado criado anteriormente ao registro RDAP do RIR. Certifique-se de incluir as strings `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` antes e depois da

parte codificada. Todo esse conteúdo deve estar em uma única e longa linha. O procedimento para atualizar o RDAP depende do RIR:

- Para o ARIN, use o portal do Account Manager para adicionar o certificado na seção “Comentários públicos” para o objeto “Informações de rede” que representa seu intervalo de endereços. Não o adicione à seção de comentários da sua organização.
- Para o RIPE, adicione o certificado como um novo campo “descr” ao objeto “inetnum” ou “inet6num” que representa seu intervalo de endereços. Geralmente, eles podem ser encontrados na seção “Meus recursos” do portal do banco de dados RIPE. Não o adicione à seção de comentários da sua organização ou ao campo “comentários” dos objetos acima.
- Para o APNIC, envie o certificado por e-mail para helpdesk@apnic.net para adicioná-lo manualmente ao campo “remarks” (observações) do intervalo de endereços. Envie o e-mail usando o contato autorizado do APNIC para os endereços IP.

É possível remover o certificado do seu registro do RIR após a conclusão da etapa de provisionamento abaixo.

3. Criar um objeto ROA no seu RIR

Crie um objeto ROA para autorizar os Amazon ASNs 16509 e 14618 a anunciar o intervalo de endereços, bem como os ASNs atualmente autorizados a anunciar o intervalo de endereços. Para as AWS GovCloud (US) Regions, autorize o ASN 8987 em vez do 16509 e 14618. É necessário definir o tamanho máximo para o CIDR que você está incluindo. O prefixo IPv4 mais específico que você pode incluir é /24. O intervalo mais específico de endereços IPv6 que é possível trazer é /48 para CIDRs anunciáveis publicamente e /56 para CIDRs que não são anunciáveis publicamente.

> **Important**
>
> Se você estiver criando um objeto ROA para o IP Address Manager (IPAM) da Amazon VPC, ao criar as ROAs, para CIDRs IPv4, é necessário definir o comprimento máximo de um prefixo de endereço IP como `/24`. Para CIDRs IPv6, se você estiver adicionando-os a um grupo anunciável, o tamanho máximo de um prefixo de endereço IP deve ser `/48`. Isso garante que você tenha total flexibilidade para dividir seu endereço IP público nas regiões da AWS. O IPAM impõe o comprimento máximo que você definiu. Para obter mais informações sobre endereços BYOIP para IPAM, consulte Tutorial: CIDRs de endereço BYOIP para IPAM no Guia do usuário do IPAM da Amazon VPC.

Pode demorar até 24 horas para que a ROA se torne disponível para a Amazon. Para obter mais informações, consulte o seu RIR:

- ARIN — Solicitações de ROA
- RIPE — Gerenciamento de ROAs
- APNIC — Gerenciamento de rotas

Ao migrar anúncios de uma workload on-premises para a AWS, crie uma ROA para seu ASN existente antes de criar as ROAs para ASNs da Amazon. Caso contrário, talvez você perceba um impacto no roteamento e nos anúncios existentes.

> **Important**
>
> Para que a Amazon anuncie e continue anunciando seu intervalo de endereços IP, as ROAs com os ASNs da Amazon devem estar em conformidade com as diretrizes acima. Se seus ROAs forem inválidos ou não estiverem em conformidade com as diretrizes acima, a Amazon se reserva o direito de parar de anunciar seu intervalo de endereços IP.

> **Note**
>
> Essa etapa não é necessária para o espaço de endereços IPv6 não anunciável publicamente.

Integração do BYOIP

O processo de integração para BYOIP inclui as tarefas apresentadas a seguir, conforme suas necessidades.

Tarefas

- Provisionamento de um intervalo de endereços anunciado publicamente na AWS
- Como provisionar um intervalo de endereços IPv6 que não seja anunciável publicamente
- Anunciar o intervalo de endereços por meio da AWS
- Desprovisionar o intervalo de endereços

Provisionamento de um intervalo de endereços anunciado publicamente na AWS

Ao provisionar um intervalo de endereços para uso com a AWS, você está confirmando que controla o intervalo de endereços e autoriza a Amazon a anunciá-lo. Também verificamos se você controla o intervalo por meio de uma mensagem de autorização assinada. Essa mensagem é assinada com o par de chaves X.509 autoassinadas que você usou ao atualizar o registro RDAP com o certificado X.509. A AWS requer uma mensagem de autorização assinada criptograficamente que é apresentada ao RIR. O RIR autentica a assinatura em relação ao certificado que você adicionou ao RDAP e verifica os detalhes da autorização em relação ao ROA.

Para provisionar o intervalo de endereços

1. Compose message

   Componha a mensagem de autorização de texto simples. O formato da mensagem é o seguinte, em que a data é a data de expiração da mensagem:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Substitua o número da conta, o intervalo de endereços e a data de expiração por seus próprios valores para criar uma mensagem semelhante à seguinte:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Não confundir com uma mensagem ROA, que tem uma aparência semelhante.

2. Assinar mensagens

   Assine a mensagem de texto sem formatação usando a chave privada criada anteriormente. A assinatura retornada pelo comando é uma string longa que você precisará copiar para uso na próxima etapa.

   > **Important**
   >
   > Recomendamos que você copie e cole esse comando. Com exceção do conteúdo da mensagem, não modifique nem substitua nenhum dos valores.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
 | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Endereço de provisão

   Use o comando provisiona-byoip-cidr da AWS CLI para provisionar o intervalo de endereços. A opção `--cidr-authorization-context` usa as strings de mensagem e assinatura que você criou anteriormente.

   > **Important**
   >
   > Você deverá especificar a região da AWS em que o intervalo do BYOIP deve ser provisionado se ele for diferente da configuração da AWS CLI de `Default region name`.

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   O provisionamento de um intervalo de endereços é uma operação assíncrona, de modo que a chamada retorna imediatamente, mas o intervalo de endereços não está pronto para uso até que seu status mude de `pending-provision` para `provisioned`.

4. Monitorar o andamento

   Embora a maior parte do provisionamento seja concluída em duas horas, a conclusão do processo de provisionamento pode levar até uma semana para intervalos que permitam anúncios públicos. Use o comando describe-byoip-cidrs para monitorar seu progresso, como neste exemplo:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   Se houver problemas durante o provisionamento e o status for para `failed-provision`, o comando `provision-byoip-cidr` deverá ser executado novamente após os problemas terem sido resolvidos.

Como provisionar um intervalo de endereços IPv6 que não seja anunciável publicamente

Por padrão, um intervalo de endereços é provisionado para ser publicamente anunciável na Internet. É possível provisionar um intervalo de endereços IPv6 que não será anunciável publicamente. Para rotas que não permitem anúncios públicos, o processo de provisionamento geralmente é concluído em minutos. Quando você associa um bloco CIDR IPv6 de um intervalo de endereços não públicos a uma VPC, o CIDR IPv6 só pode ser acessado por opções de conectividade híbrida compatíveis com IPv6, como AWS Direct Connect, AWS Site-to-Site VPN, ouGateways de trânsito da Amazon VPC.

Não é necessário ter um ROA para provisionar um intervalo de endereços não públicos.

> **Important**
>
> - Você só pode especificar se um intervalo de endereços é anunciável publicamente durante o provisionamento. Não é possível alterar o status de anúncio de um intervalo de endereços posteriormente.
> - A Amazon VPC não oferece suporte a CIDRs de endereço local exclusivo (ULA). Todas as VPCs devem ter CIDRs IPv6 exclusivos. Duas VPCs não podem ter o mesmo intervalo CIDR IPv6.

Para provisionar um intervalo de endereços IPv6 que não será anunciável publicamente, use o comando provision-byoip-cidr a seguir.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Anunciar o intervalo de endereços por meio da AWS

Após ser provisionado, o intervalo de endereços estará pronto para ser anunciado. É necessário anunciar o intervalo de endereço exato que você provisionou. Não é possível anunciar apenas uma parte do intervalo de endereço provisionado.

Se você provisionou um intervalo de endereços IPv6 que não será anunciado publicamente, não será necessário concluir esta etapa.

Recomendamos que você interrompa o anúncio do intervalo de endereços, ou qualquer parte dele, em outros locais antes de anunciá-lo por meio da AWS. Se você continuar a anunciar o seu intervalo de endereços IP, ou qualquer parte dele, em outros locais, não poderemos oferecer suporte nem solucionar os problemas do intervalo de forma confiável. Especificamente, não podemos garantir que o tráfego para o intervalo de endereços, ou qualquer parte dele, entre em nossa rede.

Para minimizar o tempo de inatividade, é possível configurar os recursos da AWS para usar um endereço do grupo de endereços antes de ele ser anunciado e, em seguida, interromper simultaneamente o anúncio no local atual e iniciar o anúncio por meio da AWS. Para obter mais informações sobre a alocação de um endereço IP elástico em seu grupo de endereços, consulte Alocar um endereço IP elástico.

Limitações

- É possível executar o comando advertise-byoip-cidr no máximo uma vez a cada 10 segundos, mesmo que você especifique diferentes intervalos de endereços de cada vez.
- É possível executar o comando withdraw-byoip-cidr no máximo uma vez a cada 10 segundos, mesmo que você especifique diferentes intervalos de endereços de cada vez.

Para anunciar o intervalo de endereços, use o seguinte comando advertise-byoip-cidr.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Desprovisionar o intervalo de endereços

Para interromper o uso do intervalo de endereços com a AWS, primeiro libere todos os endereços IP elásticos e desassocie todos os blocos CIDR IPv6 que ainda estiverem alocados do grupo de endereços. Depois, pare de anunciar o intervalo de endereços e, por fim, desprovisione o intervalo de endereços.

Não é possível desprovisionar uma parte do intervalo de endereços. Se você quiser usar um intervalo de endereços mais específico com a AWS, cancele o provisionamento de todo o intervalo de endereços e provisione um intervalo de endereços mais específico.

(IPv4) Para liberar cada endereço IP elástico, use o seguinte comando release-address.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Para desassociar um bloco CIDR IPv6, use o seguinte comando disassociate-vpc-cidr-block.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Para desprovisionar o intervalo de endereços, use o seguinte comando deprovision-byoip-cidr.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Pode levar até um dia para desprovisionar um intervalo de endereços.

Trabalhar com o intervalo de endereços

É possível visualizar e trabalhar com os intervalos de endereços IPv4 e IPv6 que você provisionou na conta.

Intervalos de endereços IPv4

É possível criar um endereço IP elástico no grupo de endereços IPv4 e usá-lo com os recursos da AWS como instâncias do EC2, gateways NAT e balanceadores de carga da rede.

Para visualizar informações sobre os grupos de endereços IPv4 que você provisionou na conta, use o seguinte comando describe-public-ipv4-pools.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Para criar um endereço IP elástico pelo grupo de endereços IPv4, use o comando allocate-address. É possível usar a opção `--public-ipv4-pool` para especificar o ID do grupo de endereços retornado por `describe-byoip-cidrs`. Ou usar a opção `--address` para especificar um endereço do intervalo de endereços que você provisionou.

Intervalos de endereços IPv6

Para visualizar informações sobre os grupos de endereços IPv6 que você provisionou na conta, use o seguinte comando describe-ipv6-pools.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Para criar uma VPC e especificar um CIDR IPv6 pelo grupo de endereços IPv6, use o seguinte comando create-vpc. Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Para associar um bloco CIDR IPv6 do grupo de endereços IPv6 a uma VPC, use o seguinte comando associate-vpc-cidr-block. Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Para visualizar as VPCs e as informações do grupo de endereços IPv6 associado, use o comando describe-vpcs. Para visualizar informações sobre blocos CIDR IPv6 associados de um grupo de endereços IPv6 específico, use o seguinte comando get-associated-ipv6-pool-cidrs.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Se você desassociar o bloco CIDR IPv6 da VPC, ele será liberado de volta para o grupo de endereços IPv6.

Validar o BYOIP

1. Valide o par de chaves x.509 autoassinado

   Valide se o certificado foi carregado e é válido por meio do comando whois.

   Para ARIN, use `whois -h whois.arin.net r + 2001:0DB8:6172::/48` para procurar o registro RDAP do intervalo de endereços. Verifique a seção `Public Comments` para o

`NetRange` (Intervalo de rede) na saída do comando. O certificado deve ser adicionado na seção `Public Comments` do intervalo de endereços.

É possível inspecionar o `Public Comments` que contém o certificado usando o seguinte comando:

```
whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
```

Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

```
Public Comments:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Para RIPE, use `whois -r -h whois.ripe.net 2001:0DB8:7269::/48` para procurar o registro RDAP do intervalo de endereços. Verifique a seção `descr` para o objeto `inetnum` (intervalo de rede) na saída do comando. O certificado deve ser adicionado como um novo campo `descr` para o intervalo de endereços.

É possível inspecionar o `descr` que contém o certificado usando o seguinte comando:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Para AONIC, use `whois -h whois.apnic.net 2001:0DB8:6170::/48` para procurar o registro RDAP do intervalo de endereços BYOIP. Verifique a seção `remarks` para o objeto `inetnum` (intervalo de rede) na saída do comando. O certificado deve ser adicionado como um novo campo `remarks` para o intervalo de endereços.

É possível inspecionar o `remarks` que contém o certificado usando o seguinte comando:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Validar a criação de um objeto ROA

   Valide a criação bem-sucedida de objetos ROA usando a API RIPEstat Data. Certifique-se de testar o intervalo de endereços em relação aos Amazon ASNs 16509 e 14618, além dos ASNs atualmente autorizados a anunciar o intervalo de endereços.

   É possível inspecionar os objetos ROA de diferentes Amazon ASNs com seu intervalo de endereços usando o seguinte comando:

   ```
   curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
   resource=ASN&prefix=CIDR
   ```

   Neste exemplo de saída, a resposta tem resultado de `"status": "valid"` para o Amazon ASN 16509. Isso indica que o objeto ROA para o intervalo de endereços foi criado com êxito:

   ```
   {
   ```

```
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```

Um status de “unknown” indica que o objeto ROA para o intervalo de endereços não foi criado. Um status de “invalid_asn” indica que o objeto ROA para o intervalo de endereços não foi criado com êxito.

Disponibilidade regional

No momento, o recurso BYOIP está disponível em todas as regiões da AWS comerciais, exceto nas regiões localizadas na China.

Disponibilidade da zona local

Uma Local Zone é uma extensão de uma região da AWS na proximidade geográfica dos usuários. As zonas locais são agrupadas em “grupos de borda de rede”. Na AWS, um grupo de borda de rede é uma coleção de zonas de disponibilidade (AZs), zonas locais ou zonas de comprimento de onda das quais a AWS anuncia um endereço IP público. As zonas locais podem ter grupos de borda de rede diferentes das AZs em uma região da AWS para garantir a latência ou a distância física mínimas entre a rede da AWS e os clientes que acessam os recursos nessas zonas.

Você pode provisionar intervalos de endereços BYOIPv4 e anunciá-los nos seguintes grupos de borda de rede da zona local usando a opção `--network-border-group`:

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Se você tiver zonas locais habilitadas (consulte Enable a Local Zone), é possível escolher um grupo de borda de rede para zonas locais ao provisionar e anunciar um CIDR BYOIPv4. Escolha o grupo de bordas de rede com cuidado, pois o EIP e o AWS recurso ao qual ele está associado devem residir no mesmo grupo de bordas de rede.

> **Note**
>
> No momento, não é possível provisionar ou anunciar intervalos de endereços BYOIPv6 em zonas locais.

Saiba mais

Para obter mais informações, consulte o Conversa técnica online da AWS Mergulho profundo em Traga seu próprio IP.

Endereços IP elásticos

Um Endereço IP elástico é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Um endereço IP elástico é alocado para a conta da AWS e será seu até que você o libere. Com um endereço IP elástico, é possível mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na conta. Como alternativa, é possível especificar o endereço IP elástico em um registro DNS para o seu domínio, para que ele acione a sua instância. Para obter mais informações, consulte a documentação para o registro de domínio.

Um endereço IP elástico é um endereço IPv4 público, que é acessível pela Internet. Se a instância não tiver um endereço IPv4 público, será possível associar um endereço IP elástico a ela para permitir a comunicação com a Internet. Por exemplo, isso permite que você se conecte à instância do computador local.

Conteúdo

- Definição de preço de endereços IP elásticos
- Noções básicas sobre endereços IP elásticos
- Trabalhar com endereços IP elásticos
- Cota de endereços IP elásticos

Definição de preço de endereços IP elásticos

A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

Noções básicas sobre endereços IP elásticos

As seguintes são as características básicas de um endereço IP elástico:

- Um endereço IP elástico é estático; ele não muda ao longo do tempo.

- Um endereço IP elástico é destinado ao uso somente em uma região específica e não pode ser movido para uma região diferente.
- Um endereço IP elástico é proveniente do grupo de endereços IPv4 públicos da Amazon ou de um grupo de endereços IPv4 personalizados transferido para sua conta da AWS.
- Para usar um endereço IP elástico, você primeiro aloca um para sua conta e o associa à instância ou a uma interface de rede.
- Quando você associa um endereço IP elástico a uma instância, ele também é associado à interface de rede principal da instância. Quando você associa um endereço IP elástico a uma interface de rede anexada a uma instância, ele também é associado à instância.
- Quando você associa um endereço IP elástico a uma instância ou à sua interface de rede primária, se a instância já tiver um endereço IPv4 público associado, esse endereço IPv4 público será liberado de volta ao grupo de endereços IPv4 públicos da Amazon, e o endereço IP elástico será associado à instância em vez disso. Não é possível reutilizar o endereço IPv4 público anteriormente associado à instância ou converter esse endereço IPv4 público em um endereço IP elástico. Para ter mais informações, consulte Endereços IPv4 públicos.
- É possível desassociar um endereço IP elástico de um recurso e reassociá-lo a outro recurso. Para evitar um comportamento inesperado, certifique-se de que todas as conexões ativas com o recurso nomeado na associação existente sejam fechadas antes de fazer a alteração. Depois de associar seu endereço IP elástico a um recurso diferente, será possível reabrir suas conexões com o recurso recém-associado.
- Um endereço IP elástico desassociado permanece alocado à sua conta até você liberá-lo explicitamente. Você recebe cobranças por todos os endereços IP elásticos em sua conta, independentemente de estarem associados ou desassociados a uma instância. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.
- Quando você associa um endereço IP elástico a uma instância que tinha um endereço IPv4 público anteriormente, o nome do host DNS público da instância é alterado para corresponder ao endereço IP elástico.
- Resolvemos o nome DNS do host público para o endereço IPv4 público ou ao endereço IP elástico da instância fora da rede da instância e para o endereço IPv4 privado da instância na rede da instância.
- Quando você aloca um endereço IP elástico em um grupo de endereços IP que você levou para sua conta da AWS, ele não é contado nos limites de endereços IP elásticos. Para obter mais informações, consulte Cota de endereços IP elásticos.

- Ao alocar os endereços IP elásticos, é possível associar os endereços IP elásticos a um grupo de borda de rede. Esse é o local a partir do qual anunciamos o bloco CIDR. Definir o grupo de borda de rede limita o bloco CIDR a esse grupo. Se você não especificar o grupo de borda de rede, definiremos o grupo de borda que contém todas as zonas de disponibilidade na região (por exemplo, `us-west-2`).
- Um endereço IP elástico deve ser usado somente um grupo de borda de rede específico.

Trabalhar com endereços IP elásticos

As seções a seguir descrevem como é possível trabalhar com endereços IP elásticos.

Tarefas

- Alocar um endereço IP elástico
- Descrever seus endereços IP elásticos
- Aplicar uma tag em um endereço IP elástico
- Associar um endereço IP elástico a uma instância ou interface de rede
- Dissociar um endereço IP elástico
- Transferir endereços IP elásticos
- Liberar um endereço IP elástico
- Recuperar um endereço IP elástico
- Usar DNS reverso para aplicações de e-mail

Alocar um endereço IP elástico

É possível alocar um endereço IP elástico no grupo de endereços IPv4 públicos da Amazon ou em um grupo de endereços IP personalizados que você levou para a conta da AWS. Para obter mais informações sobre como levar seu próprio intervalo de endereços IP para sua conta da AWS, consulte Traga seus próprios endereços IP (BYOIP) no Amazon EC2.

É possível alocar um endereço IP elástico usando um dos seguintes métodos.

Console

Para alocar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, escolha Network & Security (Rede e segurança) e Elastic IPs (IPs elásticos).
3. Escolha Allocate Elastic IP address (Alocar endereço IP elástico).
4. (Opcional) Ao alocar um endereço IP elástico (EIP), você escolhe o Grupo de borda de rede no qual alocar o EIP. Um grupo de bordas de rede é uma coleção de zonas de disponibilidade (AZs), das AWS quais a anuncia um endereço IP público. As Zonas Locais (Local Zones) e Zonas Wavelength (Wavelength Zones) podem ter grupos de fronteira de rede diferentes das Zonas de Disponibilidade (AZs) em uma Região para garantir a latência mínima ou distância física entre a rede AWS e os clientes que acessam os recursos nessas Zonas.

   > **Important**
   >
   > Você deve alocar um EIP no mesmo grupo de fronteiras de rede do AWS recurso que será associado ao EIP. Um EIP (Endereço IP Elástico) em um grupo de fronteira de rede só pode ser anunciado em zonas dentro desse grupo de fronteira de rede e não em nenhuma outra zona representada por outros grupos de fronteira de rede.

   Se você tiver Zonas Locais ou Zonas de Comprimento de Wavelength ativadas (para obter mais informações, consulte Habilitar uma Zona Local ou Ativar zonas de comprimento de onda), você pode escolher um grupo de borda de rede para AZs, Zonas Locais ou Zonas de Comprimento de Onda. Escolha o grupo de bordas de rede com cuidado, pois o EIP e o AWS recurso ao qual ele está associado devem residir no mesmo grupo de bordas de rede. É possível usar o console do EC2 para visualizar o grupo de borda de rede em que estão as zonas de disponibilidade, as zonas locais ou as zonas de Wavelength. Normalmente, todas as zonas de disponibilidade em uma região pertencem ao mesmo grupo de fronteiras de rede, enquanto as zonas locais ou zonas de comprimento de onda pertencem a seus próprios grupos de fronteiras de rede separados.

   Se você não tiver zonas locais ou zonas de comprimento de onda habilitadas, ao alocar um EIP, o grupo de bordas de rede que representa todas as AZs da região (como `us-west-2`) será predefinido para você e não será possível alterá-lo. Isso significa que o EIP alocado para esse grupo de borda de rede será anunciado em todas as AZs da região em que você está.
5. Em Public IPv4 address pool (Grupo de endereços IPv4 público), escolha uma das seguintes opções:

- Amazon's pool of IPv4 addresses (Grupo de endereços IPv4 da Amazon) — Se você deseja que um endereço IPv4 seja alocado a partir do grupo de endereços IPv4 da Amazon.
- Endereço IPv4 público que você traz para sua conta da AWS: se deseja alocar um endereço IPv4 de um grupo de endereços IP que você trouxe para sua conta da AWS. Essa opção será desabilitada se você não tiver nenhum pool de endereços IP.
- Customer owned pool of IPv4 addresses (Grupo de endereços IPv4 de propriedade do cliente): se você quiser alocar um endereço IPv4 de um grupo criado a partir de sua rede on-premises para uso com um AWS Outpost. Essa opção será desativada se você não tiver um Outpost da AWS.

6. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Escolha Remover à direita da chave e do valor da tag.

7. Escolha Allocate.

AWS CLI

Para alocar um endereço IP elástico

Use o comando da AWS CLI allocate-address.

PowerShell

Para alocar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell New-EC2Address.

Descrever seus endereços IP elásticos

É possível descrever um endereço IP elástico usando um dos seguintes métodos.

Console

Como descrever seus endereços IP elásticos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser exibido e escolha Actions (Ações), View details (Exibir detalhes).

AWS CLI

Como descrever seus endereços IP elásticos

Use o comando da AWS CLI describe-addresses.

PowerShell

Como descrever seus endereços IP elásticos

Use o comando do AWS Tools for Windows PowerShell Get-EC2Address.

Aplicar uma tag em um endereço IP elástico

É possível atribuir tags personalizadas aos endereços IP elásticos para categorizá-los de diferentes formas, como por objetivo, por proprietário ou por ambiente. Isso ajuda a localizar rapidamente um endereço IP elástico específico baseado em tags personalizadas que você atribuiu a ele.

O rastreamento de alocação de custos usando tags de endereço IP elástico não é compatível.

É possível marcar um endereço IP elástico usando um dos seguintes métodos.

Console

Para aplicar uma tag em um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser marcado e escolha Actions (Ações), View details (Exibir detalhes).

4. Na seção Tags, escolha Manage tags (Gerenciar tags).
5. Especifique um par de chave e valor de tag.
6. (Opcional) Escolha Add tag (Adicionar tag) para adicionar outras tags.
7. Escolha Save (Salvar).

AWS CLI

Para aplicar uma tag em um endereço IP elástico

Use o comando da AWS CLI create-tags.

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Para aplicar uma tag em um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell New-EC2Tag.

O comando `New-EC2Tag` precisa de um parâmetro de `Tag`, especificando os pares de chave e valor a serem usados na tag de endereço IP elástico. Os comandos a seguir criam o parâmetro de `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
 PS C:\> $tag.Key = "Owner"
 PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Associar um endereço IP elástico a uma instância ou interface de rede

Se você está associando um endereço IP elástico à sua instância para habilitar a comunicação com a Internet, deve garantir também que sua instância está em uma sub-rede pública. Para obter mais informações, consulte Gateways da Internet no Guia do usuário da Amazon VPC.

É possível associar um endereço IP elástico a uma instância ou interface de rede usando um dos seguintes métodos.

Console

Para associar um endereço Elastic IP a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).
4. Em Resource type (Tipo de recurso), escolha Instance (Instância).
5. Por exemplo, escolha a instância à qual associar o endereço IP elástico. Também é possível inserir texto para pesquisar uma instância específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

Como associar um endereço IP elástico a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).
4. Em Resource type (Tipo de recurso), selecione Network interface (Interface de rede).
5. Em Network interface (Interface de rede), escolha a interface de rede à qual associar o endereço IP elástico. Também é possível inserir texto para pesquisar uma interface de rede específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

AWS CLI

Como associar um endereço IP elástico

Use o comando da AWS CLI associate-address.

PowerShell

Como associar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell Register-EC2Address.

Dissociar um endereço IP elástico

É possível desassociar um endereço IP elástico de uma instância ou interface de rede a qualquer momento. Depois de desassociar o endereço IP elástico, é possível reassociá-lo a outro recurso.

É possível desassociar um endereço IP elástico usando um dos seguintes métodos.

Console

Como desassociar e reassociar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser desassociado e escolha Actions (Ações), Disassociate Elastic IP address (Desassociar endereço IP elástico).
4. Escolha Disassociate (Desassociar).

AWS CLI

Para dissociar um endereço IP elástico

Use o comando da AWS CLI disassociate-address.

PowerShell

Para dissociar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell Unregister-EC2Address.

Transferir endereços IP elásticos

Esta seção descreve como transferir endereços IP elásticos de uma Conta da AWS para outra. A transferência de endereços IP elásticos pode ser útil nas seguintes situações:

- Reestruturação organizacional: use transferências de endereços IP elásticos para passar rapidamente workloads de uma Conta da AWS para outra. Nao é necessário esperar que novos endereços IP elásticos sejam listados como permitidos em seus grupos de segurança e NACLs.
- Administração de segurança centralizada: use uma conta de segurança da AWS centralizada para rastrear e transferir endereços IP elásticos que tiver a conformidade de segurança verificada.
- Recuperação de desastres: use transferências de endereços IP elásticos para remapear rapidamente IPs para workloads da Internet voltadas para o público durante eventos de emergência.

Não há cobrança pela transferência de endereços IP elásticos.

Tarefas

- Habilitar a transferência de endereços IP elásticos
- Desabilitar a transferência de endereços IP elásticos
- Aceitar um endereço IP elástico transferido

Habilitar a transferência de endereços IP elásticos

Esta seção descreve como aceitar um endereço IP elástico transferido. Observe as seguintes limitações relacionadas à habilitação de endereços IP elásticos para transferência:

- Os endereços IP elásticos podem ser transferidos de qualquer Conta da AWS (conta de origem) para qualquer outra conta da AWS na mesma região da AWS (conta de transferência).
- Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando da AWS CLI describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.
- As transferências aceitas ficam visíveis para a conta de origem (por exemplo, no console da AWS ou ao usar o comando da AWS CLI describe-address-transfers) por três dias após a aceitação das transferências.
- A AWS não notifica as contas de transferência sobre solicitações pendentes de transferência de endereços IP elásticos. O proprietário da conta de origem deve notificar o proprietário da conta de transferência sobre uma solicitação de transferência de endereços IP que este deve aceitar.

- Todas as tags associadas a um endereço IP elástico que está sendo transferido são redefinidas quando a transferência é concluída.
- Não é possível transferir endereços IP elásticos alocados de grupos de endereços IPv4 públicos que você traz para sua conta da Conta da AWS (comumente chamados de grupos de endereços traga seu próprio IP (BYOIP)).
- Caso tente transferir um endereço IP elástico que tenha um registro DNS reverso associado a ele, você poderá iniciar o processo de transferência, mas a conta de transferência não poderá aceitar a transferência até que o registro DNS associado seja removido.
- Se tiver habilitado e configurado o AWS Outposts, talvez você tenha alocado endereços IP elásticos de um grupo de endereços IP pertencentes ao cliente (CoIPs). Não é possível transferir endereços IP elásticos alocados de um CoIP. No entanto, você pode usar o AWS RAM para compartilhar um CoIP com outra conta. Para obter mais informações, consulte Customer-owned IP addresses (Endereços IP pertencentes ao cliente) no Guia do usuário do AWS Outposts Outposts.
- É possível usar o Amazon VPC IPAM para rastrear a transferência de endereços IP elásticos para contas em uma organização da AWS Organizations. Para obter mais informações, consulte Visualizar histórico de endereços IP. Se um endereço IP elástico for transferido para uma Conta da AWS fora da organização, o histórico de auditoria IPAM do endereço IP elástico será perdido.

Essas etapas devem ser concluídas pela conta de origem.

Console

Para habilitar a transferência de endereços IP elásticos

1. Verifique se você está usando a conta da AWS de origem.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha Elastic IPs.
4. Selecione um ou mais endereços IP elásticos para habilitar para transferência e escolha Actions (Ações), Enable transfer (Habilitar transferência).
5. Se você estiver transferindo vários endereços IP elásticos, verá a opção Transfer type (Tipo de transferência). Escolha uma das seguintes opções:
   - Escolha Single account (Conta única) se estiver transferindo os endereços IP elásticos para uma única conta da AWS.
   - Escolha Multiple accounts (Várias contas) se estiver transferindo os endereços IP elásticos para várias contas da AWS.

6. Em Transfer account ID (ID da conta de transferência), insira os IDs das contas da AWS para as quais deseja transferir os endereços IP elásticos.
7. Confirme a transferência inserindo **`enable`** na caixa de texto.
8. Selecione Enviar.
9. Para aceitar a transferência, consulte Aceitar um endereço IP elástico transferido. Para desabilitar a transferência, consulte Desabilitar a transferência de endereços IP elásticos.

AWS CLI

Para habilitar a transferência de endereços IP elásticos

Use o comando enable-address-transfer.

PowerShell

Para habilitar a transferência de endereços IP elásticos

Use o comando Enable-EC2AddressTransfer.

Desabilitar a transferência de endereços IP elásticos

Esta seção descreve como desabilitar uma transferência de IP elásticos após a habilitação da transferência.

Estas etapas devem ser concluídas pela conta de origem que habilitou a transferência.

Console

Para desabilitar uma transferência de endereço IP elástico

1. Verifique se você está usando a conta da AWS de origem.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha Elastic IPs.
4. Na lista de recursos de IPs elásticos, verifique se a propriedade que mostra o status de transferência da coluna está habilitada.
5. Selecione um ou mais endereços IP elásticos que tenham Transfer status (Status de transferência) Pending (Pendente) e escolha Actions (Ações), Disable transfer (Desabilitar transferência).

6. Confirme digitando **`disable`** na caixa de texto.
7. Selecione Enviar.

AWS CLI

Para desabilitar a transferência de endereços IP elásticos

Use o comando disable-address-transfer.

PowerShell

Para desabilitar a transferência de endereços IP elásticos

Use o comando Disable-EC2AddressTransfer.

Aceitar um endereço IP elástico transferido

Esta seção descreve como aceitar um endereço IP elástico transferido.

Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando da AWS CLI describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.

Ao aceitar transferências, observe as seguintes exceções que podem ocorrer e como resolvê-las:

- AddressLimitExceeded: se sua conta de transferência tiver excedido a cota de endereços IP elásticos, a conta de origem poderá habilitar a transferência de endereços IP elásticos, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Por padrão, todas as contas da AWS estão limitadas a 5 endereços IP elásticos por região. Consulte Cota de endereços IP elásticos para obter instruções sobre como aumentar o limite.
- InvalidTransfer.AddressCustomPtrSet: se você ou alguém da sua organização tiver configurado o endereço IP elástico que você está tentando transferir para usar pesquisa reversa de DNS, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deverá remover o registro de DNS do endereço IP elástico. Para ter mais informações, consulte Usar DNS reverso para aplicações de e-mail.

- InvalidTransfer.AddressAssociated: se houver um endereço IP elástico associado a uma instância do ENI ou EC2, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deve desassociar o endereço IP elástico. Para ter mais informações, consulte Dissociar um endereço IP elástico.

Para quaisquer outras exceções, entre em contato com o AWS Support.

Essas etapas devem ser concluídas pela conta de transferência.

Console

Para aceitar uma transferência de endereço IP elástico

1. Verifique se você está usando a conta de transferência.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha Elastic IPs.
4. Escolha Actions (Ações), Accept transfer (Aceitar transferência).
5. Quando a transferência for aceita, nenhuma tag associada ao endereço IP elástico que está sendo transferido será transferida com o endereço IP elástico. Se desejar definir uma etiqueta Name (Nome) para o endereço IP elástico que está aceitando, selecione Create a tag with a key of 'Name' and a value that you specify (Criar uma tag com uma chave “Nome” e um valor especificado por você).
6. Insira o endereço IP elástico que deseja transferir.
7. Se você estiver aceitando vários endereços IP elásticos transferidos, escolha Add address (Adicionar endereço) para inserir um endereço IP elástico adicional.
8. Selecione Enviar.

AWS CLI

Para aceitar uma transferência de endereço IP elástico

Use o comando accept-address-transfer.

PowerShell

Para aceitar uma transferência de endereço IP elástico

Use o comando Approve-EC2AddressTransfer.

Liberar um endereço IP elástico

Se você não precisar mais de um endereço IP elástico, recomendamos que o libere usando um dos seguintes métodos. O endereço para lançamento não deve estar associado atualmente a um recurso da AWS, como uma instância do EC2, um gateway NAT ou um Network Load Balancer.

> **Note**
>
> Se você contatou o suporte da AWS para configurar o DNS reverso para um endereço IP elástico (EIP), é possível remover o DNS reverso, mas você não pode liberar o endereço IP elástico porque ele foi bloqueado pelo Suporte da AWS. Para desbloquear o endereço IP elástico, entre em contato com AWS Support. Depois que o endereço IP elástico for desbloqueado, será possível liberar o endereço IP elástico.

Console

Para liberar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser liberado e escolha Actions (Ações), Release Elastic IP addresses (Liberar endereços IP elásticos).
4. Escolha Release (Liberar).

AWS CLI

Para liberar um endereço IP elástico

Use o comando da AWS CLI release-address.

PowerShell

Para liberar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell Remove-EC2Address.

Recuperar um endereço IP elástico

Se você divulgou seu Endereço IP elástico, será possível recuperá-lo. As seguintes regras se aplicam:

- Não é possível recuperar um endereço IP elástico se ele tiver sido alocado a outra conta da AWS, ou se isso resultar em endereços IP elásticos acima do limite.
- Você não pode recuperar tags associadas a um endereço IP elástico.
- É possível recuperar um endereço IP elástico apenas usando a API do Amazon EC2 ou uma ferramenta da linha de comando.

AWS CLI

Como recuperar um endereço IP elástico

Use o comando da AWS CLI allocate-address e especifique o endereço IP usando o parâmetro `--address` da seguinte maneira.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Como recuperar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell New-EC2Address e especifique o endereço IP usando o parâmetro `-Address` da seguinte maneira.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Usar DNS reverso para aplicações de e-mail

Se você pretende enviar e-mails a terceiros a partir de uma instância, recomendamos que provisione um ou mais endereços IP elásticos e atribua registros DNS reversos estáticos aos endereços IP elásticos que você usa para enviar e-mails. Isso pode ajudar a evitar que o seu e-mail seja sinalizado como spam por algumas organizações antispam. O AWS trabalha com ISPs e organizações antispam da Internet para reduzir a chance de que e-mails enviados desses endereços sejam sinalizados como spam.

Considerações

- Antes de criar um registro DNS reverso, é necessário definir um registro DNS de encaminhamento correspondente (registro do tipo A) que acione o seu endereço IP elástico.
- Se um registro DNS reverso estiver associado a um endereço IP elástico, o endereço IP elástico será bloqueado para sua conta e não poderá ser liberado de sua conta até que o registro seja removido.
- AWS GovCloud (US) Region

  Não é possível criar um registro DNS reverso usando o console ou a AWS CLI. A AWS deve atribuir os registros DNS reversos estáticos para você. Abra Solicitar a remoção do DNS reverso e limitações de envio de e-mail e forneça os endereços de IP elásticos e registros DNS reversos.

Crie um registro de DNS reverso

Para criar um registro DNS reverso, escolha a guia que corresponda ao método de sua preferência.

Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Update reverse DNS (Atualizar DNS reverso).
4. Em Nome do domínio de DNS reverso, digite o nome do domínio.
5. Digite **`update`** para confirmar.
6. Escolha Update.

AWS CLI

Use o comando modify-address-attribute na AWS CLI, conforme mostrado no seguinte exemplo:

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --
domain-name example.com
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
```

```
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

Remover um registro de DNS reverso

Para remover um registro DNS reverso, escolha a guia que corresponda ao método de sua preferência.

Console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Update reverse DNS (Atualizar DNS reverso).
4. Em Nome do domínio de DNS reverso, limpe o nome do domínio.
5. Digite **`update`** para confirmar.
6. Escolha Update.

AWS CLI

Use o comando reset-address-attribute na AWS CLI, conforme mostrado no seguinte exemplo:

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
```

```
    ]
}
```

> **Note**
>
> Se você receber o erro a seguir ao executar o comando, poderá enviar uma Solicitação para remover limitações no envio de e-mail ao AWS Support para obter assistência. Não foi possível liberar o endereço com ID de alocação porque está bloqueado em sua conta.

Cota de endereços IP elásticos

Por padrão, todas as contas da AWS têm uma cota de cinco (5) endereços IP elásticos por região, pois os endereços públicos da Internet (IPv4) são um recurso público escasso. Recomendamos enfaticamente usar um endereço IP elástico principalmente para a capacidade de remapear o endereço para outra instância no caso de falha da instância, e usar os nomes de host DNS para qualquer outra comunicação entre nós.

Como verificar quantos endereços IP elásticos estão em uso

Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/ e escolha IPs elásticos no painel de navegação.

Verificar a cota atual de endereços IP elásticos da conta

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. Na barra de navegação (na parte superior da tela), selecione uma região.
3. No painel, escolha Amazon Elastic Compute Cloud (Amazon EC2).

   Se o Amazon Elastic Compute Cloud (Amazon EC2) não estiver listado no painel, escolha Serviços da AWS, insira **`EC2`** no campo de pesquisa e escolha Amazon Elastic Compute Cloud (Amazon EC2).
4. Na página de Service Quotas do Amazon EC2, insira **`IP`** no campo de pesquisa. O limite é EC2-VPC Elastic IPs (IPs elásticos de EC2-VPC). Para obter mais informações, escolha o limite.

Se achar que a arquitetura justifica endereços IP elásticos adicionais, será possível solicitar um aumento de cota diretamente no console do Service Quotas. Para solicitar um aumento de cota,

escolha Solicitar aumento no nível da conta. Para ter mais informações, consulte Service Quotas do Amazon EC2.

Interfaces de rede elástica

Uma interface de rede elástica é um componente lógico de redes em uma VPC que representa uma cartão de rede virtual. Ele pode incluir os seguintes atributos:

- Um endereço IPv4 privado primário do intervalo de endereços IPv4 de sua VPC
- Um endereço IPv6 primário do intervalo de endereços IPv6 da sua VPC
- Um ou mais endereços IPv4 privados secundários do intervalo de endereços IPv4 de sua VPC
- Um endereço IP elástico (IPv4) por endereço IPv4 privado
- Um endereço IPv4 público
- Um ou mais endereços IPv6
- Um ou mais grupos de segurança
- Um endereço MAC
- Um indicador de verificação de origem/destino
- Uma descrição

É possível criar e configurar interfaces de rede e anexá-las a instâncias na mesma zona de disponibilidade. Sua conta também pode ter interfaces de rede gerenciadas pelo solicitante que são criadas e administradas pelos serviços da AWS, para que você possa usar outros recursos e serviços. Você não pode gerenciar essas interfaces de rede si mesmo. Para obter mais informações, consulte Interfaces de rede gerenciadas pelo solicitante.

Esse recurso da AWS é chamado de interface de rede no AWS Management Console e na API do Amazon EC2. Portanto, usamos "interface de rede" nesta documentação em vez de "interface de rede elástica". O termo "interface de rede" nesta documentação significa sempre "interface de rede elástica".

Tópicos

- Conceitos básicos da interface de rede
- Placas de rede
- Endereços IP por interface de rede por tipo de instância
- Trabalhar com interfaces de rede

- Melhores práticas para configurar interfaces de rede
- Cenários para interfaces de rede
- Interfaces de rede gerenciadas pelo solicitante
- Atribuir prefixos a interfaces de rede do Amazon EC2

Conceitos básicos da interface de rede

É possível criar uma interface de rede, associá-la a uma instância, desassociá-la de uma instância e associá-la a outra instância. Os atributos de uma interface de rede a seguem, pois está associada ou desassociada de uma instância e reassociada a outra instância. Quando você move uma interface de rede de uma instância para outra, o tráfego de rede é redirecionado para a nova instância.

Interface de rede primária

Cada instância tem uma interface de rede padrão, chamada interface de rede primária. Você não pode desanexar uma interface de rede primária de uma instância. É possível criar e associar interfaces de rede adicionais. O número máximo de interfaces de rede que é possível usar varia por tipo de instância. Para obter mais informações, consulte Endereços IP por interface de rede por tipo de instância.

Endereços IPv4 públicos para interfaces de rede

Na VPC, todas as sub-redes têm um atributo modificável que determina se às interfaces de rede criadas naquela sub-rede (e, portanto, em instâncias executadas nessa sub-rede) é atribuído um endereço de público IPv4. Para obter mais informações, consulte Configurações de sub-redes no Guia do usuário da Amazon VPC. O endereço IPv4 público é atribuído pelo pool de endereços IPv4 públicos da Amazon. Quando você executa uma instância, o endereço IP é atribuído à interface de rede primária criada.

Ao criar uma interface de rede, ela herda o atributo de endereçamento de IPv4 público da sub-rede. Se você modificar posteriormente o atributo de endereçamento IPv4 público da sub-rede, a interface de rede manterá a configuração vigente de quando ela foi criada. Se você executar uma instância e especificar uma interface de rede existente como a interface de rede primária, o atributo de endereço IPv4 público será determinado por essa interface de rede.

Para obter mais informações, consulte Endereços IPv4 públicos.

Endereços IP elásticos para interface de rede

Se você tiver um endereço IP elástico, poderá associá-lo a um dos endereços IPv4 privados da interface de rede. É possível associar um endereço IP elástico a cada endereço IPv4 privado.

Se você desassociar um endereço IP elástico de uma interface de rede, poderá liberá-lo de volta para o grupo de endereços. Essa é a única maneira de associar um endereço IP elástico a uma instância em uma sub-rede ou VPC diferente, já que as interfaces de rede são específicas de sub-redes.

Endereços IPv6 públicos para interfaces de rede

É possível associar blocos CIDR de IPv6 à sua VPC e sub-rede e atribuir um ou mais endereços IPv6 do intervalo de sub-rede a uma interface de rede. Cada endereço IPv6 pode ser atribuído a uma interface de rede.

Todas as sub-redes têm um atributo modificável que determina se às interfaces de rede criadas naquela sub-rede (e, portanto, em instâncias executadas nessa sub-rede) é atribuído automaticamente um endereço de público IPv6 do intervalo da sub-rede. Para obter mais informações, consulte Configurações de sub-redes no Guia do usuário da Amazon VPC. Quando você executa uma instância, o endereço IPv6 é atribuído à interface de rede primária criada.

Para obter mais informações, consulte Endereços IPv6.

Delegação de prefixo

Um prefixo de Delegação de Prefixo é um intervalo de CIDR IPv4 ou IPv6 privado reservado que você aloca para atribuição automática ou manual a interfaces de rede associadas a uma instância. Usando prefixos delegados, é possível iniciar serviços mais rapidamente atribuindo um intervalo de endereços IP como um único prefixo.

Comportamento de encerramento

É possível definir o comportamento de encerramento para uma interface de rede que está anexada a uma instância. É possível especificar se a interface de rede deve ser excluída automaticamente quando você encerrar a instância à qual está anexada.

Verificação de origem/destino

É possível ativar ou desativar as verificações de origem/destino, que garantem que a instância seja a origem ou o destino de qualquer tráfego recebido. A verificação da origem/destino está ativada por padrão. É necessário desabilitar as verificações de origem/destino se a instância executa serviços como tradução de endereço de rede, roteamento ou firewalls.

Monitoramento do tráfego de IP

É possível ativar um log de fluxo de VPC na sua interface de rede para capturar informações sobre o tráfego IP que vai e volta da interface de rede. Depois que você tiver criado um log de fluxo, pode visualizar e recuperar esses dados no Amazon CloudWatch Logs. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Atribuição automática de endereço IPv4 público

É possível habilitar e desabilitar a atribuição automática de um endereço IPv4 público a uma interface de rede. Essa opção pode ser habilitada para qualquer interface de rede, mas se aplicará somente à interface de rede primária (eth0). Para ter mais informações, consulte Gerenciar endereços IP.

Placas de rede

As instâncias com várias placas de rede oferecem maior performance de rede, incluindo recursos de largura de banda acima de 100 Gbps e maior performance da taxa de pacotes. Cada interface de rede é conectada a uma placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede.

Se você ativar Elastic Fabric Adapter (EFA) ao executar uma instância compatível com várias placas de rede, todas as placas de rede estarão disponíveis. É possível atribuir até uma EFA por placa de rede. Uma EFA conta como uma interface de rede.

As instâncias a seguir suportam várias placas de rede. Todos os outros tipos de instância suportam uma placa de rede.

Tipo de instância	Quantidade de placas de rede
c6in.32xlarge	2
c6in.metal	2
dl1.24xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2

Tipo de instância	Quantidade de placas de rede
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2

Endereços IP por interface de rede por tipo de instância

Cada tipo de instância oferece suporte a um número máximo de interfaces de rede, um número máximo de endereços IPv4 privados por interface de rede e um número máximo de endereços IPv6 por interface de rede. O limite de endereços IPv6 é separado do limite para endereços IPv4 privados por interface de rede. Nem todos os tipos de instância são compatíveis com endereçamento IPv6.

Interfaces de rede disponíveis

O Guia de tipos de instância do Amazon EC2 fornece informações sobre as interfaces de rede disponíveis para cada tipo de instância. Para obter mais informações, consulte as informações a seguir.

- Network specifications: General purpose
- Network specifications: Compute optimized
- Network specifications: Memory optimized
- Network specifications: Storage optimized
- Network specifications: Accelerated computing
- Network specifications: High-performance computing
- Network specifications: Previous generation

Como recuperar informações da interface de rede usando a AWS CLI

É possível usar o comando describe-instance-types da AWS CLI para exibir informações sobre um tipo de instância, como as interfaces de rede compatíveis e os endereços IP por interface. O exemplo a seguir exibe essas informações para todas as instâncias C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].{ \
        Type: InstanceType, \
        MaxENI: NetworkInfo.MaximumNetworkInterfaces, \
        IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" \
    --output table
```

Saída esperada

```
-------------------------------------
|        DescribeInstanceTypes        |
```

```
+----------+----------+---------------+
| IPv4addr | MaxENI   |     Type      |
+----------+----------+---------------+
|  30      |  8       |  c5.4xlarge   |
|  50      |  15      |  c5.24xlarge  |
|  15      |  4       |  c5.xlarge    |
|  30      |  8       |  c5.12xlarge  |
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

Como recuperar informações da interface de rede usando a AWS Tools for PowerShell

É possível usar o comando Get-EC2InstanceType do PowerShell para exibir informações sobre um tipo de instância, como as interfaces de rede compatíveis e os endereços IP por interface. O exemplo a seguir exibe essas informações para todas as instâncias C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
Select-Object `
    @{Name = 'Ipv4AddressesPerInterface'; Expression =
 {($_.Networkinfo.Ipv4AddressesPerInterface)}},
    @{Name = 'MaximumNetworkInterfaces'; Expression =
 {($_.Networkinfo.MaximumNetworkInterfaces)}},
    InstanceType | `
Format-Table -AutoSize
```

Saída esperada

```
Ipv4AddressesPerInterface MaximumNetworkInterfaces InstanceType
------------------------- ------------------------ ------------
                       30                        8 c5.4xlarge
                       15                        4 c5.xlarge
                       30                        8 c5.12xlarge
                       50                       15 c5.24xlarge
                       30                        8 c5.9xlarge
                       50                       15 c5.metal
                       15                        4 c5.2xlarge
                       10                        3 c5.large
                       50                       15 c5.18xlarge
```

Trabalhar com interfaces de rede

É possível trabalhar com interfaces de rede usando o console ou a linha de comando do Amazon EC2.

Tópicos

- Criar uma interface de rede
- Visualizar detalhes sobre uma interface de rede
- Anexar uma interface de rede a uma instância.
- Desanexar uma interface de rede de uma instância
- Gerenciar endereços IP
- Modificar atributos da interface de rede
- Adicionar ou editar tags
- Excluir uma interface de rede

Criar uma interface de rede

É possível criar uma interface de rede em uma sub-rede. Não é possível mover a interface de rede para outra sub-rede depois que ela é criada. É necessário associar uma interface de rede a uma instância na mesma zona de disponibilidade.

Para criar uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Clique em Create network interface (Criar interface de rede).
4. (Opcional) Em Description (Descrição), insira um nome descritivo.
5. Em Subnet (Sub-rede), selecione uma sub-rede. As opções disponíveis nas etapas subsequentes mudam dependendo do tipo de sub-rede selecionada [somente IPv4, somente IPv6 ou pilha dupla (IPv4 e IPv6)].
6. Em Private IPv4 address (Endereço IPv4 privado), siga um dos seguintes procedimentos:
   - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv4 na sub-rede.
   - Clique em Custom (Personalizado) e insira um endereço IPv4 selecionado na sub-rede.

7. (Somente sub-redes com endereços IPv6) Para IPv6 address (Endereço IPv6), execute um dos seguintes procedimentos:
   - Clique em None (Nenhum) se você não quiser atribuir um endereço IPv6 à interface de rede.
   - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv6 na sub-rede.
   - Clique em Custom (Personalizado) e insira um endereço IPv6 selecionado na sub-rede.
8. (Opcional) Se estiver criando uma interface de rede em uma sub-rede de pilha dupla ou somente IPv6, você terá a opção de Atribuir IP IPv6 primário. Isso atribui um endereço unicast global (GUA) IPv6 primário à interface de rede. A atribuição de um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Escolha Habilitar se a instância à qual essa ENI será anexada depender do seu endereço IPv6 permanecer inalterado. A AWS atribuirá automaticamente um endereço IPv6 associado à ENI anexada à sua instância como o endereço IPv6 primário. Após habilitar um endereço GUA IPv6 para ser um IPv6 primário, não será possível desabilitá-lo. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se tornará o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada. Se você tiver vários endereços IPv6 associados a uma ENI anexada à sua instância e habilitar um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à ENI se tornará o endereço IPv6 primário.
9. (Opcional) Para criar um Elastic Fabric Adapter, clique em Elastic Fabric Adapter e em Enable (Habilitar).
10. (Opcional) Em Configurações avançadas, para Tempo limite de rastreamento de conexão ociosa, modifique os tempos limite de conexão ociosa padrão. Para obter mais informações sobre essas opções, consulte Tempo limite de rastreamento de conexão ociosa.
    - Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido. Mín: 60 segundos. Máx: 432.000 segundos (5 dias) Padrão: 432.000 segundos. Recomendado: menos de 432.000 segundos.
    - Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta. Mín: 30 segundos. Máx: 60 segundos. Padrão: 30 segundos.
    - Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta. Mín: 60 segundos. Máx: 180 segundos (3 minutos). Padrão: 180 segundos.
11. Para Security groups, selecione um ou mais security groups.

12. (Opcional) Para cada tag, escolha Add new tag (Adicionar nova tag) e insira uma chave de tag e um valor de tag opcional.
13. Clique em Create network interface (Criar interface de rede).

Para criar uma interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- create-network-interface (AWS CLI)
- New-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Visualizar detalhes sobre uma interface de rede

É possível visualizar todas as interfaces de rede em sua conta.

Para descrever uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Para visualizar a página de detalhes de uma interface de rede, selecione o ID da interface de rede. Como alternativa, para visualizar informações sem sair da página de interfaces de rede, marque a caixa de seleção para a interface de rede.

Para descrever uma interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Para descrever um atributo de interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-network-interface-attribute (AWS CLI)

- Get-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Anexar uma interface de rede a uma instância.

É possível associar uma interface de rede a alguma instância na mesma zona de disponibilidade da interface de rede usando a página de Instâncias ou Interfaces de rede do console do Amazon EC2. Se preferir, é possível associar uma interface de rede existente ao iniciar instâncias.

> **Important**
>
> Para instâncias do EC2 em uma sub-rede somente IPv6, se você anexar uma interface de rede secundária à instância, o hostname de DNS privado da segunda interface de rede será resolvido como o primeiro endereço IPv6 na primeira interface de rede da instância. Para obter mais informações sobre hostnames de DNS privados de instância do EC2, consulte Tipos de nome de host de instância do Amazon EC2.

Se o endereço IPv4 público da sua instância for liberado, ele não receberá um novo se houver mais de uma interface de rede associada à instância. Para obter mais informações sobre o comportamento dos endereços IPv4 públicos, consulte Endereços IPv4 públicos.

Instances page

Para associar uma interface de rede a uma instância usando a página Instances (Instâncias)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da instância.
4. Escolha Actions (Ações), Networking (Redes), Attach network interface (Associar interface de rede).
5. Escolha uma VPC. Se você estiver anexando uma interface de rede secundária à instância, a interface de rede poderá residir na mesma VPC da sua instância ou em outra VPC que seja sua (desde que a interface de rede esteja em uma sub-rede na mesma zona de disponibilidade da sua instância). Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança.
6. Selecione uma interface de rede. Se a instância suportar várias placas de rede, será possível escolher uma placa de rede.

7. Escolha Associar.

Network Interfaces page

Para associar uma interface de rede a uma instância usando a página Network Interfaces (Interfaces de rede)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Attach (Associar).
5. Escolha uma instância. Se a instância suportar várias placas de rede, será possível escolher uma placa de rede.
6. Escolha Associar.

Para associar uma interface de rede à instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

> **Note**
>
> Você pode anexar uma interface de rede que esteja em outra VPC (mas na mesma zona de disponibilidade) a uma instância usando o comando da AWS CLI attach-network-interface. Não é possível fazer isso usando o AWS Management Console.

- attach-network-interface (AWS CLI)
- Add-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Desanexar uma interface de rede de uma instância

É possível separar uma interface de rede secundária associada a uma instância do EC2 a qualquer momento usando a página Instances (Instâncias) ou Network Interfaces (Interfaces de rede) do console do Amazon EC2.

Se você tentar separar uma interface de rede associada a um recurso de outro serviço, como um load balancer do Elastic Load Balancing, uma função do Lambda, um WorkSpace ou um gateway NAT, você receberá um erro informando que você não tem permissão para acessar o recurso. Para localizar qual serviço criou o recurso anexado a uma interface de rede, verifique a descrição da interface de rede. Se você excluir o recurso, sua interface de rede será excluída.

Instances page

Para separar uma interface de rede de uma instância usando a página Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da instância. Verifique a seção Network interfaces (Interfaces de rede) da guia Networking (Rede) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Escolha Actions (Ações), Networking (Redes), Detach network interface (Separar interface de rede).
5. Selecione a interface de rede e escolha Separar.

Network Interfaces page

Para separar uma interface de rede de uma instância usando a página Interfaces de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede. Verifique a seção Instance details (Detalhes da instância) da guia Details (Detalhes) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Clique em Actions (Ações) e em Detach (Desanexar).
5. Quando a confirmação for solicitada, selecione Detach (Desanexar).
6. Se a interface de rede não conseguir se separar da instância, escolha Force detachment (Forçar desanexação), Enable (Ativar) e tente novamente. Recomendamos a desanexação forçada somente como último recurso. Forçar a separação pode impedir que você associe outra interface de rede no mesmo índice até reiniciar a instância. Isso também pode impedir que os metadados da instância reflitam que a interface de rede foi separada até que você reinicie a instância.

Para separar uma interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- detach-network-interface (AWS CLI)
- Dismount-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Gerenciar endereços IP

É possível gerenciar os seguintes endereços IP para suas interfaces de rede:

- Endereços IP elásticos (um por endereço IPv4 privado)
- Endereços IPv4
- Endereços IPv6
- Endereço IPv6 primário

Para gerenciar endereços IP elásticos de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Para associar um endereço IP elástico, faça o seguinte:
    a. Clique em Actions (Ações) e em Associate address (Associar endereço).
    b. Para Elastic IP address (Endereço IP elástico), selecione o endereço IP elástico.
    c. Para Private IPv4 address (Endereço IPv4 privado), selecione o endereço IPv4 privado a ser associado ao endereço IP elástico.
    d. (Opcional) Escolha Allow the Elastic IP address to be reassociated (Permitir que o endereço IP elástico seja reassociado) se a interface de rede estiver atualmente associada a outra instância ou interface de rede.
    e. Escolha Associate.
5. Para desassociar um endereço IP elástico, faça o seguinte:
    a. Escolha Actions e Disassociate address.

b. Em Public IP address (Endereço IP público), selecione o endereço IP elástico.

c. Escolha Disassociate (Desassociar).

Como gerenciar os endereços IPv4 e IPv6 de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede.
4. Clique em Actions (Ações) e em Manage IP addresses (Gerenciar endereços IP).
5. Expanda a interface de rede.
6. Para IPv4 addresses (Endereços IPv4), modifique os endereços IP conforme necessário. Para atribuir um endereço IPv4, selecione Assign new IP address (Atribuir novo endereço IP) e especifique um endereço IPv4 do intervalo de sub-rede ou deixe que AWS escolha um para você. Para cancelar a atribuição de um endereço IPv4, escolha Unassign (Desatribuir) ao lado do endereço.
7. Para atribuir ou cancelar a atribuição de um endereço IPv4 público a uma interface de rede, escolha Atribuir IP público automaticamente. Essa opção pode ser habilitada ou desabilitada para qualquer interface de rede, mas só se aplicará à interface de rede primária (eth0).
8. Para IPv6 addresses (Endereços IPv6), modifique os endereços IP conforme necessário. Para atribuir um endereço IPv6, escolha Assign new IP (Atribuir novo IP) e especifique um endereço IPv6 do intervalo de sub-rede ou deixe que AWS escolha um para você. Para cancelar a atribuição de um endereço IPv6, escolha Unassign (Desatribuir) ao lado do endereço.
9. (Opcional) Se estiver modificando uma interface de rede em uma sub-rede de pilha dupla ou somente IPv6, você terá a opção de Atribuir IP IPv6 primário. A atribuição de um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Escolha Habilitar se a instância à qual essa ENI será anexada depender do seu endereço IPv6 permanecer inalterado. A AWS atribuirá automaticamente um endereço IPv6 associado à ENI anexada à sua instância como o endereço IPv6 primário. Após habilitar um endereço GUA IPv6 para ser um IPv6 primário, não será possível desabilitá-lo. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se tornará o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada. Se você tiver vários endereços IPv6 associados a uma ENI anexada à sua instância e habilitar um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à ENI se tornará o endereço IPv6 primário.
10. Escolha Salvar.

Como gerenciar os endereços IP de uma interface de rede usando a AWS CLI

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- assign-ipv6-addresses
- associate-address
- disassociate-address
- unassign-ipv6-addresses

Como gerenciar os endereços IP de uma interface de rede usando o Tools for Windows PowerShell

É possível usar um dos comandos a seguir.

- Register-EC2Address
- Register-EC2Ipv6AddressList
- Unregister-EC2Address
- Unregister-EC2Ipv6AddressList

Modificar atributos da interface de rede

É possível alterar os seguintes atributos de interface de rede:

- Descrição
- Grupos de segurança
- Excluir no encerramento
- Verificação de origem/destino

Como alterar a descrição de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change description (Alterar a descrição).

5. Em Description (Descrição), insira uma descrição para a interface da rede.
6. Escolha Save (Salvar).

Como alterar os grupos de segurança de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change security groups (Alterar grupos de segurança).
5. Para Associated security groups (Grupos de segurança associados), selecione os grupos de segurança a serem usados e clique em Save (Salvar).

   O grupo de segurança e a interface de rede devem ser criados para a mesma VPC. Para alterar o grupo de segurança para interfaces de propriedade de outros serviços, como o Elastic Load Balancing, faça isso por meio desse serviço.

Como alterar o comportamento de encerramento de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change termination behavior (Alterar comportamento de encerramento).
5. Selecione ou desmarque Delete on termination (Excluir no encerramento), Enable (Habilitar) conforme necessário, e depois clique em Save (Salvar).

Para alterar a verificação de origem/destino de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações), Change source/dest check (Alterar verificação de origem/destino).

5. Selecione ou desmarque Source/destination check (Verificação de origem/destino), Enable (Habilitar) conforme necessário, e depois clique em Save (Salvar).

Para alterar os tempos limite de rastreamento de conexões ociosas:

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Escolha Ações, Modificar tempo limite de conexão.
5. Modifique os tempos limite de rastreamento da conexão ociosa. Para obter mais informações sobre essas opções, consulte Tempo limite de rastreamento de conexão ociosa.
   - Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido. Mín: 60 segundos. Máx: 432.000 segundos (5 dias) Padrão: 432.000 segundos. Recomendado: menos de 432.000 segundos.
   - Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta. Mín: 30 segundos. Máx: 60 segundos. Padrão: 30 segundos.
   - Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta. Mín: 60 segundos. Máx: 180 segundos (3 minutos). Padrão: 180 segundos.
6. Escolha Salvar.

Como modificar atributos de interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- modify-network-interface-attribute (AWS CLI)
- Edit-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Adicionar ou editar tags

Tags são metadados que é possível adicionar a uma interface de rede. As tags são privadas e só podem ser vistas pela sua conta. Cada tag consiste em uma chave e um valor opcional. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2.

Para adicionar ou editar tags para uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
5. Para cada tag a ser criada, clique em Add new tag (Adicionar nova tag) e insira uma chave e um valor opcional. Quando você terminar, selecione Salvar.

Para adicionar ou editar tags para uma interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Excluir uma interface de rede

A exclusão de uma interface de rede libera todos os atributos associados com a interface e todos os endereços IP privados ou endereços IP elásticos a serem usados por outra instância.

Você não pode excluir uma interface de rede que está em uso. Primeiro, você devedesanexar a interface de rede.

Para excluir uma interface de rede usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede e selecione Actions (Ações), Delete (Excluir).

4. Quando a confirmação for solicitada, escolha Excluir.

Para excluir uma interface de rede usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- delete-network-interface (AWS CLI)
- Remove-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Melhores práticas para configurar interfaces de rede

- É possível associar uma interface de rede a uma instância quando ela estiver sendo executada (associação a quente), quando parou (associação em espera ativa) ou quando a instância está sendo executada (associação a frio).
- É possível desanexar as interfaces de rede secundárias quando a instância estiver sendo executada ou estiver parada. No entanto, não é possível desanexar a interface de rede primária.
- É possível mover uma interface de rede secundária de uma instância para outra se as instâncias estiverem na mesma zona de disponibilidade e VPC, mas em sub-redes diferentes.
- Ao executar uma instância usando a CLI, a API ou um SDK, é possível especificar a interface de rede primária e interfaces de rede adicionais.
- Executando a instância do Amazon Linux ou do Windows com várias interfaces de rede configura automaticamente interfaces, os endereços IPv4 privados, e tabelas de rotas no sistema operacional da instância.
- Uma associação com espera passiva ou a quente de uma interface de rede adicional pode exigir que você acesse manualmente a segunda interface, configure o endereço IPv4 privado e modifique a tabela de rotas de acordo. As instâncias executadas em Amazon Linux ou Windows Server reconhecem automaticamente a associação com espera passiva ou a quente e se configuram.
- Não é possível associar outra interface de rede a uma instância (por exemplo, uma configuração de teaming de NIC) como método para aumentar ou dobrar a largura de banda quem vem ou vai para a instância dual-homed.
- Se você associar duas ou mais interfaces de rede da mesma sub-rede a uma instância, poderá encontrar problemas de rede, como roteamento assimétrico. Se possível, use um endereço IPv4 privado secundário na interface de rede primária.

- Instâncias do Windows: caso use diversas interfaces de rede, você deverá configurar as interfaces de rede para usar o roteamento estático.

Configurar a interface de rede usando ec2-net-utils para Amazon Linux 2

> **Note**
>
> Para o AL2023, o `amazon-ec2-net-utils` pacote gera configurações específicas da interface no diretório `/run/systemd/network`. Para obter mais informações, consulte Networking service (serviço de networking) no Amazon Linux 2023 User Guide (Guia do usuário do Amazon Linux 2023).

As AMIs do Amazon Linux 2 podem conter scripts adicionais instalados pela AWS, conhecidos como ec2-net-utils. Esses scripts opcionalmente automatizam a configuração das suas interfaces de rede. Esses scripts estão disponíveis somente para Amazon Linux 2.

Use o comando instalar o pacote no Amazon Linux 2, caso ainda não esteja instalado, ou atualize-o se ele estiver instalado e houver atualizações adicionais disponíveis:

```
$ yum install ec2-net-utils
```

Os componentes a seguir fazem parte de ec2-net-utils:

Regras udev (`/etc/udev/rules.d`)

Identifica interfaces de rede quando são associadas, separadas ou religadas a uma instância em execução, e garante que o script de hotplug seja executado (`53-ec2-network-interfaces.rules`). Mapeia o endereço MAC para um nome de dispositivo (`75-persistent-net-generator.rules`, que gera `70-persistent-net.rules`).

Script de hotplug

Gera um arquivo de configuração de interface apropriado para uso com DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Gera também um arquivo de configuração de rota (`/etc/sysconfig/network-scripts/route-ethN`).

Script de DHCP

Sempre que a interface de rede receber um novo lease do DHCP, esse script consultará os metadados da instância para endereços IP elásticos. Para cada endereço IP elástico, ele adiciona

uma regra ao banco de dados de políticas de roteamento para garantir que o tráfego de saída desse endereço use a interface de rede correta. Ele também adiciona cada endereço IP privado à interface de rede como um endereço secundário.

ec2ifup ethN (`/usr/sbin/`)

Estende a funcionalidade de padrão ifup. Depois de o script reescrever os arquivos de configuração `ifcfg-ethN` e `route-ethN`, ele executará o ifup.

ec2ifdown ethN (`/usr/sbin/`)

Estende a funcionalidade de padrão ifdown. Depois de o script eliminar todas as regras da interface de rede do banco de dados de políticas de roteamento, ele executará o ifdown.

ec2ifscan (`/usr/sbin/`)

Verifica se há interfaces de rede que não foram configuradas e as configura.

Este script não está disponível na versão inicial de ec2-net-utils.

Para listar todos os arquivos de configuração gerados por ec2-net-utils, use o seguinte comando:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Para desabilitar a automação, é possível adicionar `EC2SYNC=no` ao arquivo `ifcfg-ethN` correspondente. Por exemplo, use o comando a seguir para desabilitar a automação da interface eth1:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Para desativar completamente a automação, pode remover o pacote usando o seguinte comando:

```
$ yum remove ec2-net-utils
```

Cenários para interfaces de rede

Associar várias interfaces de rede a uma instância é útil quando você deseja:

- Criar uma rede de gerenciamento.

- Usar dispositivos de rede e segurança na sua nuvem privada virtual (VPC).
- Criar instâncias dual-homed com workloads/funções em sub-redes distintas.
- Criar uma solução de baixo orçamento e alta disponibilidade.

Criar uma rede de gerenciamento.

Esse cenário descreve como você pode criar uma rede de gerenciamento com interfaces de rede, considerando os seguintes critérios e configurações (imagem a seguir).

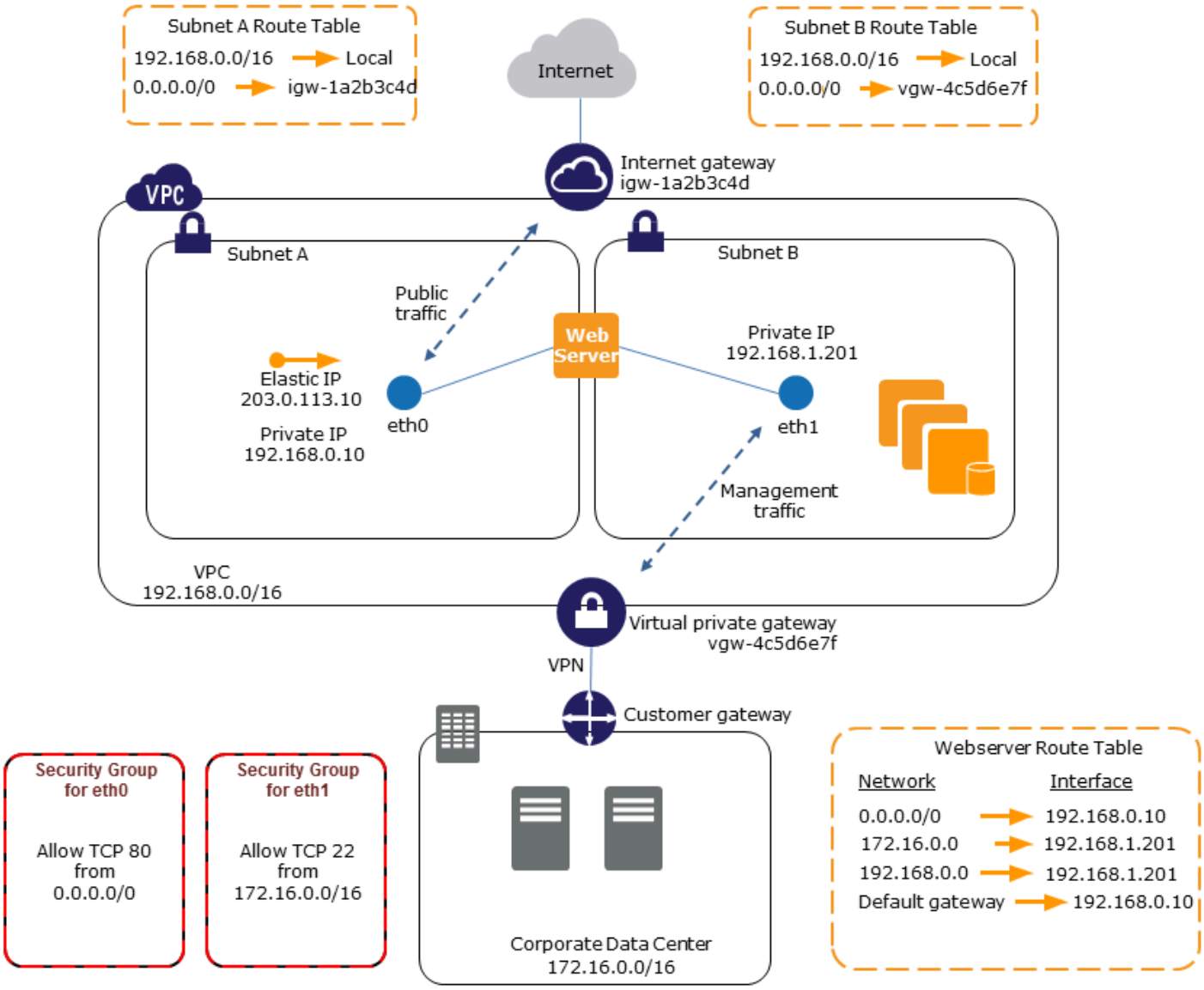
Critérios

- A interface de rede primária na instância (eth0) lida com o tráfego público.
- A interface de rede secundária na instância (eth1) lida com o tráfego de gerenciamento de backend. Ela está conectada a uma sub-rede separada com controles de acesso mais restritivos e está localizada na mesma zona de disponibilidade (AZ) que a interface de rede primária.

Configurações

- A interface de rede primária, que pode ou não estar por trás de um balanceador de carga, tem um grupo de segurança associado que permite acesso ao servidor a partir da Internet. Por exemplo, permitir as portas TCP 80 e 443 de `0.0.0.0/0` ou do balanceador de carga.
- A interface de rede secundária tem um grupo de segurança associado que permite somente o acesso SSH, iniciado usando um dos seguintes locais:
  - Um intervalo permitido de endereços IP, dentro da VPC ou da Internet.
  - Uma sub-rede privada na mesma AZ que a interface de rede primária.
  - Um gateway privado virtual.

> **Note**
>
> Para garantir recursos de failover, considere usar um IPv4 privado secundário para o tráfego de entrada em uma interface de rede. No caso de falha de instância, é possível mover a interface e/ou o endereço IPv4 privado secundário para uma instância standby.



Usar dispositivos de rede e segurança na VPC

Algumas ferramentas de rede e segurança, como load balancers, servidores de tradução de endereço de rede (NAT) e servidores proxy preferem ser configurados com várias interfaces de rede. É possível criar e associar interfaces de rede secundárias às instâncias em uma VPC que executa esses tipos de aplicações e configurar interfaces adicionais com seus próprios endereços IP públicos e privados, grupos de segurança e verificação de origem/destino.

Criar instâncias dual-homed com workloads/funções em sub-redes distintas

É possível colocar uma interface de rede em cada um dos servidores Web que se conecta a uma rede mid-tier na qual reside o servidor de aplicações. O servidor de aplicações também pode ser dual-homed para uma rede backend (sub-rede) no servidor onde reside o banco de dados. Em vez de rotear pacotes de rede pelas instâncias dual-homed, cada instância dual-homed recebe e processa solicitações no front-end, inicia uma conexão ao backend e, então, envia solicitações aos servidores na rede backend.

Criar instâncias de hospedagem dupla com workloads/perfis em VPCs distintas dentro da mesma conta

Você pode iniciar uma instância do EC2 em uma VPC e anexar à instância uma ENI secundária de outra VPC (mas na mesma zona de disponibilidade). Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança. Você não pode criar instâncias de múltiplas hospedagens em VPCs entre contas diferentes da AWS.

Você pode usar instâncias de múltiplas hospedagens em VPCs nos seguintes casos de uso:

- Superar sobreposições de CIDR entre duas VPCs que não podem ser emparelhadas: você pode aproveitar um CIDR secundário em uma VPC e permitir que uma instância se comunique em dois intervalos de IP não sobrepostos.
- Conectar várias VPCs em uma única conta: habilitar a comunicação entre recursos individuais que normalmente seriam separados pelos limites da VPC.

Criar uma solução de baixo orçamento e alta disponibilidade

Se uma das suas instâncias que atende uma função específica falhar, sua interface de rede poderá ser associada a uma instância de substituição ou standby a quente pré-configurada para a mesma função a fim de recuperar rapidamente o serviço. Por exemplo, é possível usar uma interface de rede como interface de rede primária ou secundária para um serviço crítico como uma instância de banco de dados ou instância NAT. Se a instância falhar, você (ou, mais provavelmente, o código em execução em seu nome) pode associar a interface de rede a uma instância de standby a quente. Como a interface mantém os endereços IP privados, endereços IP elásticos e endereço MAC, o tráfego de rede começa a fluir para a instância standby assim que você associar a interface de rede à instância de substituição. Os usuários experimentam uma breve perda de conectividade entre o momento em que a instância falha e a hora em que a interface de rede é associada à instância em standby, mas não é necessária nenhuma alteração na tabela de rotas da VPC no seu servidor DNS.

Interfaces de rede gerenciadas pelo solicitante

Uma interface de rede gerenciada pelo solicitante é uma interface de rede que um AWS service (Serviço da AWS) cria na VPC em seu nome. A interface de rede está associada a um recurso de outro serviço, como uma instância de banco de dados do Amazon RDS, um gateway NAT ou um endpoint da VPC de interface de AWS PrivateLink.

Considerações

- Você pode visualizar as interfaces de rede gerenciadas pelo solicitante em sua conta. Você pode adicionar ou remover etiquetas, mas não pode alterar outras propriedades de uma interface de rede gerenciada pelo solicitante.
- Não é possível desvincular uma interface de rede gerenciada pelo solicitante.
- Ao excluir o recurso associado à interface de rede gerenciada pelo solicitante, o AWS service (Serviço da AWS) desvinculará e excluirá a interface de rede. Se o serviço desvinculou uma interface de rede, mas não a excluiu, você poderá excluir a interface de rede desvinculada.

Para visualizar interfaces de rede gerenciadas pelo solicitante usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Network & Security (Rede e segurança), Network Interfaces (Interfaces de rede).
3. Selecione o ID da interface de rede para abrir sua página de detalhes.
4. Estes são os principais campos que podem ser usados para determinar a finalidade da interface de rede:

   - Descrição: uma descrição fornecida pelo serviço da AWS que criou a interface. Por exemplo, "VPC Endpoint Interface vpce 089f2123488812123".
   - Gerenciado pelo solicitante: indica se a interface de rede é gerenciada pela AWS.
   - Requester ID (ID do solicitante): o alias ou ID da conta da AWS da entidade principal ou serviço que criou a interface de rede. Se você criou uma interface de rede, este campo exibirá o ID de sua Conta da AWS. Caso contrário, ele terá sido criado por outra entidade principal ou serviço.

Para visualizar interfaces de rede gerenciadas pelo solicitante usando a AWS CLI

Use o comando describe-network-interfaces como indicado a seguir.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

Veja a seguir um exemplo de saída que mostra os principais campos que é possível usar para determinar a finalidade da interface de rede: `Description` e `InterfaceType`.

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

Para visualizar interfaces de rede gerenciadas pelo solicitante usando Tools for Windows PowerShell (Ferramentas do Windows PowerShell)

Use o cmdlet Get-EC2NetworkInterface como indicado a seguir.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

Veja a seguir um exemplo de saída que mostra os principais campos que é possível usar para determinar a finalidade da interface de rede: `Description` e `InterfaceType`.

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType      : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Atribuir prefixos a interfaces de rede do Amazon EC2

É possível atribuir um intervalo de CIDR IPv4 ou IPv6 privado, automático ou manualmente, às suas interfaces de rede. Ao atribuir prefixos, você dimensiona e simplifica o gerenciamento de aplicações, incluindo aplicações de contêiner e rede que exigem vários endereços IP em uma instância. Para obter mais informações sobre endereços IPv4 e IPv6, consulte Endereçamento IP de instâncias do Amazon EC2.

As seguintes opções estão disponíveis:

- Atribuição automática: a AWS escolhe o prefixo do bloco CIDR IPv4 ou IPv6 de sua sub-rede VPC e o atribui à sua interface de rede.
- Atribuição manual: você especifica o prefixo do bloco CIDR IPv4 e IPv6 da sub-rede da VPC e a AWS verifica se o prefixo ainda não está atribuído a outros recursos antes de atribuí-lo à interface de rede.

Atribuir prefixos apresenta os seguintes benefícios:

- Endereços IP aumentados em uma interface de rede — Quando você usa um prefixo, atribui um bloco de endereços IP em vez de endereços IP individuais. Isso aumenta o número de endereços IP para uma interface de rede.
- Gerenciamento simplificado da VPC para contêineres — em aplicações de contêiner, cada contêiner requer um endereço IP exclusivo. A atribuição de prefixos à instância simplifica o gerenciamento de suas VPCs, pois é possível iniciar e encerrar contêineres sem precisar chamar APIs do Amazon EC2 para atribuições de IP individuais.

Conteúdo

- Noções básicas para atribuição de prefixos
- Considerações e limites para prefixos
- Trabalhar com prefixos

Noções básicas para atribuição de prefixos

- É possível atribuir um prefixo a interfaces de rede novas ou existentes.
- Para usar prefixos, atribua um prefixo à interface de rede, depois anexe a interface de rede à instância e configure o sistema operacional.

- Quando você escolhe a opção para especificar um prefixo, o prefixo deve atender aos seguintes requisitos:
  - O prefixo IPv4 que é possível especificar é `/28`.
  - O prefixo IPv6 que é possível especificar é `/80`.
  - O prefixo está na sub-rede CIDR da interface de rede e não se sobrepõe a outros prefixos ou endereços IP atribuídos a recursos existentes na sub-rede.
- É possível atribuir um prefixo à interface de rede primária ou secundária.
- É possível atribuir um endereço IP elástico a uma interface de rede que tenha um prefixo atribuído a ela.
- Também é possível atribuir um endereço IP elástico à parte do endereço IP do prefixo atribuído.
- Um nome de host DNS privado (interno) é resolvido para o endereço IPv4 privado da instância.
- Atribuímos cada endereço IPv4 privado para uma interface de rede, incluindo os de prefixos, usando o seguinte formato:
  - `us-east-1`Região da

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Todas as outras regiões

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Considerações e limites para prefixos

Leve o seguinte em consideração ao usar endpoints do :

- As interfaces de rede com prefixos são compatíveis com as instâncias desenvolvidas no AWS Nitro System.
- Os prefixos para interfaces de rede são limitados a endereços IPv4 e endereços IPv6 privados.
- O número máximo de endereços IP que podem ser atribuídos a uma interface de rede depende do tipo de instância. Todo prefixo que você atribui a uma interface de rede conta como um endereço IP. Por exemplo, uma instância `c5.large` tem um limite de `10` endereços IPv4 por interface de rede. Toda interface de rede para essa instância tem um endereço IPv4 primário. Se uma interface de rede não tiver endereços IPv4 secundários, será possível atribuir até nove prefixos à interface de rede. Para cada endereço IPv4 adicional que você atribuir a uma interface de rede, poderá

atribuir um prefixo a menos à interface de rede. Para ter mais informações, consulte Endereços IP por interface de rede por tipo de instância.

- Os prefixos são incluídos nas verificações de origem/destino.

Trabalhar com prefixos

É possível usar prefixos com suas interfaces de rede conforme descrito a seguir.

Tarefas

- Atribuir prefixos durante a criação da interface de rede
- Atribuir prefixos a interfaces de rede existentes
- Configure seu sistema operacional para interfaces de rede com prefixos
- Exibir os prefixos atribuídos às suas interfaces de rede
- Remover prefixos de suas interfaces de rede

Atribuir prefixos durante a criação da interface de rede

Se você usar a opção de atribuição automática, poderá reservar um bloco de endereços IP na sua sub-rede. A AWS escolhe os prefixos deste bloco. Para obter mais informações, consulte Comportamento do endereçamento IP para sua sub-rede no Guia do usuário da Amazon VPC.

Depois de criar a interface de rede, use o comando attach-network-interface AWS CLI para anexar a interface de rede à sua instância. Configure seu sistema operacional para trabalhar com interfaces de rede com prefixos. Para ter mais informações, consulte Configure seu sistema operacional para interfaces de rede com prefixos.

Tarefas

- Atribuir prefixos automáticos durante a criação da interface de rede
- Atribuir prefixos específicos durante a criação da interface de rede

Atribuir prefixos automáticos durante a criação da interface de rede

É possível atribuir prefixos automáticos durante a criação da interface de rede usando um dos métodos a seguir.

Console

Para atribuir prefixos automáticos durante a criação da interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione Criar interface de rede.
3. Especifique uma descrição para a interface de rede, selecione a sub-rede na qual deseja criar a interface de rede e configure os endereços IPv4 e IPv6 privados.
4. Amplie as Configurações avançadas e faça o seguinte:

   a. Para atribuir automaticamente um prefixo IPv4, para Delegação de prefixo IPv4, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv4, especifique o número de prefixos a serem atribuídos.

   b. Para atribuir automaticamente um prefixo IPv6, para Delegação de prefixo IPv6, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv6, especifique o número de prefixos a serem atribuídos.

   > **Note**
   >
   > Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Selecione os grupos de segurança a serem associados à interface de rede e atribua marcações de recursos, se necessário.
6. Clique em Criar interface de rede.

AWS CLI

Para atribuir prefixos IPv4 automáticos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv4-prefix-count` para o número de prefixos que você deseja que a AWS atribua. No exemplo a seguir, a AWS atribui o prefixo 1.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Para atribuir prefixos IPv6 automáticos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv6-prefix-count` para o número de prefixos que você deseja que a AWS atribua. No exemplo a seguir, a AWS atribui o prefixo 1.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
```

```
}
```

Atribuir prefixos específicos durante a criação da interface de rede

É possível atribuir prefixos específicos durante a criação da interface de rede usando um dos métodos a seguir.

Console

Para atribuir prefixos específicos durante a criação da interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione Criar interface de rede.
3. Especifique uma descrição para a interface de rede, selecione a sub-rede na qual deseja criar a interface de rede e configure os endereços IPv4 e IPv6 privados.
4. Amplie as Configurações avançadas e faça o seguinte:
   a. Para atribuir um prefixo IPv4 específico, para Delegação de prefixo IPv4, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.
   b. Para atribuir um prefixo IPv6 específico, para Delegação de prefixo IPv6, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.

   > **Note**
   >
   > Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Selecione os grupos de segurança a serem associados à interface de rede e atribua marcações de recursos, se necessário.
6. Clique em Criar interface de rede.

AWS CLI

Para atribuir prefixos IPv4 específicos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv4-prefixes` para os prefixos. A AWS seleciona endereços IP desse intervalo. No exemplo a seguir, o prefixo CIDR é`10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Exemplo de saída

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 manual example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

Para atribuir prefixos IPv6 específicos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv6-prefixes` para os prefixos. A AWS seleciona endereços IP desse intervalo. No exemplo a seguir, o prefixo CIDR é`2600:1f13:fc2:a700:1768::/80`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Exemplo de saída


```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
```

```
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

Atribuir prefixos a interfaces de rede existentes

Depois de atribuir os prefixos, use o comando AWS CLI attach-network-interface para anexar a interface de rede à sua instância. Configure seu sistema operacional para trabalhar com interfaces de rede com prefixos. Para ter mais informações, consulte Configure seu sistema operacional para interfaces de rede com prefixos.

Tarefas

- Atribuir prefixos automáticos a uma interface de rede existente
- Atribuir prefixos específicos a uma interface de rede existente

Atribuir prefixos automáticos a uma interface de rede existente

É possível atribuir prefixos automáticos a uma interface de rede existente usando um dos métodos a seguir.

Console

Para atribuir prefixos automáticos a uma interface de rede existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede à qual atribuir os prefixos e escolha Ações, Gerenciar prefixos.
4. Para atribuir automaticamente um prefixo IPv4, para Delegação de prefixo IPv4, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv4, especifique o número de prefixos a serem atribuídos.
5. Para atribuir automaticamente um prefixo IPv6, para Delegação de prefixo IPv6, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv6, especifique o número de prefixos a serem atribuídos.

> **Note**
>
> Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

6. Escolha Salvar.

AWS CLI

É possível usar oassign-ipv6-addressespara atribuir prefixos IPv6 e o comandoassign-private-ip-addressespara atribuir prefixos IPv4 a interfaces de rede existentes.

Para atribuir prefixos IPv4 automáticos a uma interface de rede existente

Use o comando assign-private-ip-addresses e defina `--ipv4-prefix-count` para o número de prefixos que você deseja que a AWS atribua. No exemplo a seguir, a AWS atribui o prefixo 1 IPv4.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
        }
    ]
}
```

Para atribuir prefixos IPv6 automáticos a uma interface de rede existente

Use o comando assign-ipv6-addresses e defina `--ipv6-prefix-count` para o número de prefixos que você deseja que a AWS atribua. No exemplo a seguir, a AWS atribui o prefixo 1 IPv6.

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Exemplo de saída

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

Atribuir prefixos específicos a uma interface de rede existente

É possível atribuir prefixos específicos a uma interface de rede existente usando um dos métodos a seguir.

Console

Para atribuir prefixos específicos a uma interface de rede existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede à qual atribuir os prefixos e escolha Ações, Gerenciar prefixos.
4. Para atribuir um prefixo IPv4 específico, para Delegação de prefixo IPv4, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.
5. Para atribuir um prefixo IPv6 específico, para Delegação de prefixo IPv6, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.

   > **Note**
   >
   > Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

6. Escolha Salvar.

AWS CLI

Atribuir prefixos IPv4 específicos a uma interface de rede existente

Use o comando assign-private-ip-addresses e defina `--ipv4-prefixes` para o prefixo. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é `10.0.0.208/28`.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Exemplo de saída

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.208/28"
        }
    ]
}
```

Atribuir prefixos IPv6 específicos a uma interface de rede existente

Usar o comando assign-ipv6-addresses e defina `--ipv6-prefixes`para o prefixo. A AWS seleciona endereços IPv6 desse intervalo. No exemplo a seguir, o prefixo CIDR é`2600:1f13:fc2:a700:18bb::/80`.

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Exemplo de saída

```
{
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",
    "AssignedIpv6Prefixes": [
        {
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"
        }
    ]
```

```
}
```

Configure seu sistema operacional para interfaces de rede com prefixos

As AMIs do Amazon Linux poderão conter outros scripts instalados pela AWS, conhecidos como `ec2-net-utils`. Esses scripts opcionalmente automatizam a configuração das suas interfaces de rede. Esses scripts estão disponíveis somente para Amazon Linux.

Se você não estiver usando o Amazon Linux, poderá usar uma CNI (Container Network Interface) para o plugin Kubernetes, ou`docker`se você usar o Docker para gerenciar seus contêineres.

Exibir os prefixos atribuídos às suas interfaces de rede

É possível visualizar os prefixos atribuídos às interfaces de rede usando um dos métodos a seguir.

Console

Para visualizar os prefixos automáticos a uma interface de rede existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede para a qual os prefixos serão visualizados e escolha a guia Detalhes.
4. O campo Delegação de prefixo IPv4 lista os prefixos IPv4 atribuídos, e o campo Delegação de prefixo IPv6 lista os prefixos IPv6 atribuídos.

AWS CLI

É possível usar o comando describe-network-interfaces da AWS CLI para visualizar os prefixos atribuídos às interfaces de rede.

```
$ C:\> aws ec2 describe-network-interfaces
```

Exemplo de saída

```
{
    "NetworkInterfaces": [
        {
            "AvailabilityZone": "us-west-2a",
```

```
            "Description": "IPv4 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "Ipv6Prefixes": [],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b2146bf252"
        },
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c411c91b5"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
```

```
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv4Prefixes": [],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    ]
}
```


Remover prefixos de suas interfaces de rede

É possível remover prefixos de suas interfaces de rede usando um dos métodos a seguir.

Console

Para remover os prefixos de uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede da qual remover os prefixos e escolha Ações, Gerenciar prefixos.
4. Execute um destes procedimentos:

- Para remover todos os prefixos atribuídos, para a Delegação de prefixo IPv4 e Delegação de prefixo IPv6, escolha Não atribuir.
- Para remover prefixos específicos atribuídos, em IPv4 prefix delegation (Delegação de prefixo IPv4) ou IPv6 prefix delegation (Delegação de prefixo IPv6), escolha Custom (Personalizado) e, em seguida, escolha Unassign (Cancelar atribuição) ao lado dos prefixos que deseja remover.

> **Note**
>
> Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Escolha Salvar.

AWS CLI

É possível usar ounassign-ipv6-addressespara remover prefixos IPv6 e o comandounassign-private-ip-addressespara remover prefixos IPv4 de suas interfaces de rede existentes.

Para remover prefixos IPv4 de uma interface de rede

Use o comando unassign-private-ip-addresses e defina `--ipv4-prefix` para o endereço que você deseja remover.

```
$ C:\> aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

Para remover prefixos IPv6 de uma interface de rede

Use o comando unassign-ipv6-addresses e defina `--ipv6-prefix` para o endereço que você deseja remover.

```
$ C:\> aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Largura de banda de rede de instâncias do Amazon EC2

As especificações de largura de banda da instância se aplicam tanto ao tráfego de entrada quanto de saída da instância. Por exemplo, se uma instância especificar até 10 Gbps de largura de banda, isso significa que ela tem até 10 Gbps de largura de banda para tráfego de entrada e até 10 Gbps para tráfego de saída. A largura de banda da rede disponível para uma instância do EC2 depende de vários fatores, como se segue.

Tráfego de vários fluxos

A largura de banda para tráfego multifluxo agregado disponível para uma instância depende do destino do tráfego.

- Dentro da região: o tráfego pode utilizar toda a largura de banda da rede disponível para a instância.
- Para outras regiões, um gateway da Internet, Direct Connect ou gateways locais (LGW): o tráfego pode utilizar até 50% da largura de banda da rede disponível para uma instância da geração atual com um mínimo de 32 vCPUs. A largura de banda para uma instância de geração atual com menos de 32 vCPUs é limitada a 5 Gbps.

Tráfego de fluxo único

A largura de banda de base para tráfego de fluxo único é limitada a 5 Gbps quando as instâncias não estão no mesmo grupo de posicionamento de cluster. Para reduzir a latência e aumentar a largura de banda de fluxo único, experimente uma dos seguintes opções:

- Use um grupo de posicionamento de cluster para conseguir uma largura de banda de até 10 Gbps para instâncias dentro do mesmo grupo de posicionamento.
- Configure vários caminhos entre dois endpoints para conseguir uma maior largura de banda usando Multipath TCP (MPTCP).
- Configure o ENA Express para as instâncias elegíeis na mesma sub-rede para conseguir até 25 Gbps entre essas instâncias.

Largura de banda disponível da instância

A largura de banda de rede disponível de uma instância depende do número de vCPUs que ela possui. Por exemplo, um`m5.8xlarge`tem 32 vCPUs e largura de banda de rede de 10 Gbps, e

umam5.16xlargetem 64 vCPUs e 20 Gbps de largura de banda de rede. As instâncias podem não atingir essa largura de banda, por exemplo, se excederem as permissões de rede no nível da instância, como pacote por segundo ou número de conexões controladas. A quantidade de largura de banda disponível que o tráfego pode utilizar depende do número de vCPUs e do destino. Por exemplo, uma instância `m5.16xlarge` tem 64 vCPUs, portanto, o tráfego para outra instância na região pode utilizar a largura de banda total disponível (20 Gbps). No entanto, o tráfego para outra instância em uma região diferente pode utilizar apenas 50% da largura de banda disponível (10 Gbps).

Normalmente, instâncias com 16 vCPUs ou menos (tamanho `4xlarge` e inferiores) são documentadas como tendo “até” uma largura de banda especificada; por exemplo, “até 10 Gbps”. Essas instâncias têm uma largura de banda de base. Para atender a demanda adicional, eles podem usar um mecanismo de crédito de E/S para explodir além da largura de banda de base. As instâncias podem usar largura de banda expansível por um tempo limitado, geralmente de 5 a 60 minutos, dependendo do tamanho da instância.

Uma instância recebe o número máximo de créditos de E/S de rede no lançamento. Se a instância esgotar seus créditos de E/S de rede, ela retornará à largura de banda da linha de base. Uma instância em execução ganha créditos de E/S de rede sempre que usa menos largura de banda de rede do que sua largura de banda de base. Uma instância interrompida não ganha créditos de E/S de rede. A expansão de instância é feita com base no melhor esforço, mesmo quando a instância tem créditos disponíveis, já que a largura de banda expansível é um recurso compartilhado.

Existem buckets de crédito de E/S de rede separados para o tráfego de entrada e de saída.

Performance de rede base e intermitente

O Guia de tipos de instância do Amazon EC2 descreve a performance de rede para cada tipo de instância, além de fornecer a largura de banda da rede de linha de base disponível para as instâncias que podem usar a largura de banda intermitente. Para obter mais informações, consulte as informações a seguir.

- Network specifications: General purpose
- Network specifications: Compute optimized
- Network specifications: Memory optimized
- Network specifications: Storage optimized
- Network specifications: Accelerated computing

- Network specifications: High-performance computing
- Network specifications: Previous generation

Para visualizar a performance da rede usando o AWS CLI

É possível usar o comando describe-instance-types da AWS CLI para exibir informações sobre um tipo de instância, como a performance da rede. O exemplo a seguir exibe as informações de performance de redes para todas as instâncias C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[ \
        InstanceType, \
        NetworkInfo.NetworkPerformance, \
        NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps]" \
    --output table
```

Saída esperada

```
-----------------------------------------------
|           DescribeInstanceTypes             |
+--------------+--------------------+---------+
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0    |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25   |
|  c5.12xlarge |  12 Gigabit        |  12.0   |
|  c5.24xlarge |  25 Gigabit        |  25.0   |
|  c5.metal    |  25 Gigabit        |  25.0   |
|  c5.9xlarge  |  12 Gigabit        |  12.0   |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5    |
|  c5.large    |  Up to 10 Gigabit  |  0.75   |
|  c5.18xlarge |  25 Gigabit        |  25.0   |
+--------------+--------------------+---------+
```

Para visualizar a performance da rede usando o AWS Tools for PowerShell

Você pode usar o comando Get-EC2InstanceType do PowerShell para exibir informações sobre um tipo de instância. O exemplo a seguir exibe as informações de performance de redes para todas as instâncias C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
```

```
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Saída esperada

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                    5.00
c5.xlarge    Up to 10 Gigabit                    1.25
c5.12xlarge  12 Gigabit                         12.00
c5.9xlarge   12 Gigabit                         12.00
c5.24xlarge  25 Gigabit                         25.00
c5.metal     25 Gigabit                         25.00
c5.2xlarge   Up to 10 Gigabit                    2.50
c5.large     Up to 10 Gigabit                    0.75
c5.18xlarge  25 Gigabit                         25.00
```

Monitorar largura de banda da instância

É possível usar métricas do CloudWatch para monitorar a largura de banda da instância e os pacotes enviados e recebidos. É possível usar as métricas de performance de rede fornecidas pelo driver Elastic Network Adapter (ENA) para monitorar quando o tráfego excede as permissões de rede definidas pelo Amazon EC2 no nível da instância.

É possível configurar se o Amazon EC2 envia dados de métrica para a instância ao CloudWatch usando períodos de um ou cinco minutos. É possível que as métricas de performance da rede mostrem que uma permissão foi excedida e os pacotes foram descartados enquanto as métricas da instância do CloudWatch não o fazem. Isso pode acontecer quando a instância tem um pico curto na demanda por recursos de rede (conhecido como micropico de tráfego), mas as métricas do CloudWatch não são detalhadas o suficiente para refletir esses picos de microssegundos.

Saiba mais

- Métricas de instância
- Métricas de performance da rede

Redes aperfeiçoadas no Amazon EC2

A rede avançada usa virtualização de E/S raiz (SR-IOV) para fornecer recursos de rede de alta performance em tipos de instâncias com suporte. A SR-IOV é um método de virtualização de dispositivos que fornece performance de E/S mais elevado e menor utilização de CPU em comparação com interfaces de redes virtualizadas tradicionais. A rede avançada fornece uma largura de banda maior, uma performance melhor de pacotes por segundo (PPS) e latências consistentemente menores entre instâncias. Não há nenhuma cobrança adicional pelo uso da rede avançada.

Para obter mais informações sobre a velocidade de rede compatível com cada tipo de instância, consulte Tipos de instância do Amazon EC2.

Tópicos

- Suporte a redes avançadas
- Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2
- Aprimoramento do desempenho da rede com o ENA Express nas instâncias do EC2
- Habilitação de redes aperfeiçoadas com a interface Intel 82599 VF nas instâncias do EC2
- Monitorar a performance de rede de sua instância do EC2
- Solução de problemas do Adaptador de Rede Elástica no Linux
- Solução de problemas do driver do Adaptador de Rede Elástica do Windows
- Aprimore a latência de rede para instâncias do Amazon EC2 baseadas em Linux
- Considerações sobre o Nitro System para ajuste de performance
- Otimização do desempenho da rede em instâncias do Windows

Suporte a redes avançadas

Todos os tipos de instância da geração atual são compatíveis com redes avançadas, exceto as instâncias T2.

É possível habilitar redes avançadas usando um dos seguintes mecanismos:

Elastic Network Adapter (ENA)

O Elastic Network Adapter (ENA) oferece suporte a velocidades de rede de até 100 Gbps para tipos de instâncias compatíveis.

Todas as instâncias desenvolvidas no AWS Nitro System usam o ENA para obter redes aprimoradas. Além disso, os seguintes tipos de instância Xen são compatíveis com o ENA: H1, I3, G3, `m4.16xlarge`, P2, P3, P3dn e R4.

Para ter mais informações, consulte Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2.

Interface Intel 82599 Virtual Function (VF)

A interface Intel 82599 Virtual Function oferece suporte a velocidades de rede de até 10 Gbps para tipos de instâncias compatíveis.

Os seguintes tipos de instância usam a interface Intel 82599 VF para redes aprimoradas: C3, C4, D2, I2, M4 (excluindo o m4.16xlarge) e R3.

Para ter mais informações, consulte Habilitação de redes aperfeiçoadas com a interface Intel 82599 VF nas instâncias do EC2.

Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2

O Amazon EC2 oferece recursos de rede avançada pelo Elastic Network Adapter (ENA). Para usar a rede aprimorada, é necessário instalar o módulo ENA necessário e habilitar o suporte ENA.

Conteúdo

- Requisitos
- Performance da rede avançada
- AMIs do Linux com o módulo necessário
- Testar se a rede avançada está habilitada
- Habilitar redes avançadas na instância
- Notas de release do driver

Requisitos

Para se preparar para a rede avançada com o ENA, configure a instância da seguinte forma:

- Inicie uma instância desenvolvida no AWS Nitro System.
- Verifique se a instância tem conectividade com a Internet.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização de kernels e módulos de kernel e a habilitação do atributo `enaSupport` podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.
- Instâncias do Linux: inicie a instância usando uma versão compatível do kernel do Linux e uma distribuição com suporte, para que as redes aperfeiçoadas do ENA sejam habilitadas automaticamente para a instância. Para obter mais informações, consulte Notas de release do driver ENA do kernel do Linux.
- Instâncias do Windows: se a instância estiver executando o Windows Server 2008 R2 SP1, verifique se ela tem a atualização de suporte à assinatura de código SHA-2.
- Use o AWS CloudShell do AWS Management Console ou instale e configure a AWS CLI ou o AWS Tools for Windows PowerShell em qualquer computador que desejar, de preferência em seu desktop ou notebook local. Para obter mais informações sobre o ACM, consulte Acessar o Amazon EC2 ou o Guia do usuário do AWS CloudShell. A rede avançada não pode ser gerenciada no console do Amazon EC2.

Performance da rede avançada

A documentação a seguir fornece um resumo da performance da rede para os tipos de instância que oferecem suporte às redes avançadas do ENA:

- Network specifications for accelerated computing instances
- Network specifications for compute optimized instances
- Network specifications for general purpose instances
- Network specifications for high-performance computing instances
- Network specifications for memory optimized instances
- Network specifications for storage optimized instances

AMIs do Linux com o módulo necessário

As AMIs a seguir incluem o módulo ENA necessário e o suporte para ENA habilitado:

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 e posteriores
- Ubuntu 14.04 ou posterior com kernel `linux-aws`

> **Note**
>
> Os tipos de instância baseados no AWS Graviton requerem o Ubuntu 18.04 ou posterior com kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Para testar se as redes aperfeiçoadas já estão habilitadas, verifique se o módulo `ena` está instalado na instância e se o atributo `enaSupport` está definido. Em caso afirmativo, o comando ethtool -i eth*n* deverá mostrar que o módulo está em uso na interface de rede.

Módulo de kernel (ena)

Para verificar se o módulo `ena` está instalado, use o comando modinfo conforme mostrado no exemplo a seguir.

```
[ec2-user ~]$ modinfo ena
filename:    /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:  1.5.0g
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  692C7C68B8A9001CB3F31D0
```

```
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:   Y
intree:   Y
name:     ena
...
```

Na instância do Amazon Linux, o módulo `ena` está instalado.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

Na instância do Ubuntu, o módulo não está instalado. Portanto, é necessário instalá-lo primeiro. Para ter mais informações, consulte Ubuntu.

Testar se a rede avançada está habilitada

É possível testar se as redes aperfeiçoadas estão habilitadas nas instâncias ou nas AMIs.

Atributo de instância

Para verificar se uma instância tem o atributo `enaSupport` de rede avançada definido, use um dos seguintes comandos. Se o atributo estiver definido, a resposta será verdadeira.

- describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance (ferramentas para o Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Atributo de imagem

Para verificar se uma AMI tem o atributo `enaSupport` de rede avançada definido, use um dos seguintes comandos. Se o atributo estiver definido, a resposta será verdadeira.

- describe-images (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image (ferramentas para o Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

Driver da interface de rede do Linux

Use o comando a seguir para verificar se o módulo `ena` está sendo usado em uma interface específica, substituindo o nome da interface que você deseja verificar. Se estiver usando uma única interface (padrão), ela será a `eth0`. Se o sistema operacional oferecer suporte a nomes de rede previsíveis, esse poderá ser um nome como `ens5`.

No exemplo acima, o módulo `ena` não está carregado porque o driver listado é `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Nesse exemplo, o módulo `ena` está carregado e na versão mínima recomendada. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
```

```
supports-register-dump: no
supports-priv-flags: no
```

Habilitar redes avançadas na instância

O procedimento usado dependerá do sistema operacional da instância.

Amazon Linux

O Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI incluem o módulo necessário para a rede aprimorada com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com uma versão HVM do Amazon Linux em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Se você executou a instância usando uma AMI do Amazon Linux mais antiga e ela ainda não tiver a rede avançada habilitada, use o seguinte procedimento para habilitar a rede avançada.

Para habilitar a rede avançada na Amazon Linux AMI

1. Conecte-se à sua instância.
2. Na instância, execute o seguinte comando para atualizar a instância com o kernel e os módulos de kernel mais recentes incluindo `ena`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. No computador local, reinicialize a instância usando o console do Amazon EC2 ou um dos seguintes comandos: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Conecte-se à instância novamente e verifique se o módulo `ena` está instalado e na versão mínima recomendada usando o comando modinfo ena em Testar se a rede avançada está habilitada.
5. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar a rede avançada na Amazon Linux AMI (instâncias compatíveis com o armazenamento de instâncias).

6. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute (ferramentas para o Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

7. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
8. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
9. Conecte-se à instância e verifique se o módulo `ena` está instalado e carregado na interface de rede usando o comando ethtool -i eth*n* em Testar se a rede avançada está habilitada.

   Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte Solução de problemas do Adaptador de Rede Elástica no Linux.

Para habilitar a rede avançada na Amazon Linux AMI (instâncias compatíveis com o armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias, habilitando o atributo de rede avançada ao registrar a AMI.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

As AMIs do HVM do Ubuntu mais recentes incluem o módulo necessário para a rede aprimorada com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI do HVM do Ubuntu mais recente em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Se tiver executado a instância usando uma AMI mais antiga e ela ainda não tiver as redes avançadas habilitadas, será possível instalar o pacote do kernel `linux-aws` para obter os drivers de redes avançadas mais recentes e atualizar o atributo necessário.

Para instalar o pacote do kernel **`linux-aws`** (Ubuntu 16.04 ou posterior)

O Ubuntu 16.04 e o 18.04 são fornecidos com o kernel personalizado do Ubuntu (pacote do kernel `linux-aws`). Para usar um kernel diferente, entre em contato com o AWS Support.

Para instalar o pacote do kernel **`linux-aws`** (Ubuntu Trusty 14.04)

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes e os pacotes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se, durante o processo de atualização, for solicitada a instalação do `grub`, use o `/dev/xvda` para instalar o `grub` e, em seguida, escolha manter a versão atual do `/boot/grub/menu.lst`.

3. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário

parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar a rede avançada no Ubuntu (instâncias com suporte do armazenamento de instâncias).

4. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   - modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
   ```

   - Edit-EC2InstanceAttribute (ferramentas para o Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
   ```

5. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
6. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

Para habilitar a rede avançada no Ubuntu (instâncias com suporte do armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias, habilitando o atributo de rede avançada ao registrar a AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE e CentOS

As AMIs mais recentes para Red Hat Enterprise Linux, SUSE Linux Enterprise Server e CentOS incluem o módulo necessário para redes aprimoradas com ENA e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI mais recente em um tipo de instância compatível, a rede aprimorada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

O procedimento a seguir fornece as etapas gerais para habilitar a rede aprimorada em uma distribuição do Linux diferente do Amazon Linux AMI ou do Ubuntu. Para obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou o suporte para o pacote e a ferramenta, consulte a documentação da sua distribuição do Linux.

Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.
2. Clone o código-fonte do módulo `ena` na instância a partir do GitHub em https://github.com/amzn/amzn-drivers. (Como o SUSE Linux Enterprise Server 12 SP2 e posterior incluem ENA 2.02 por padrão, não é necessário fazer download e compilar o driver ENA. Para o SUSE Linux Enterprise Server 12 SP2 e posterior, é necessário registrar uma solicitação para adicionar a versão do driver que deseja ao kernel comercial).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Compile e instale o módulo `ena` na instância. Essas etapas dependem da distribuição Linux. Para obter mais informações sobre a compilação do módulo no Red Hat Enterprise Linux, consulte How do I install the latest ENS driver for enhanced network support on an Amazon EC2 instance that runs RHEL?
4. Execute o comando sudo depmod para atualizar as dependências do módulo.
5. Atualize o `initramfs` na instância para garantir que o novo módulo seja carregado na hora da inicialização. Por exemplo, se a distribuição oferecer suporte a dracut, será possível usar o comando a seguir.

   ```
   dracut -f -v
   ```

6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do systemd ou udev podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse

comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte Nomes previsíveis de interface de rede no site freedesktop.org.

a. É possível verificar as versões do systemd ou udev em sistemas baseados em RPM com o comando a seguir.

```
rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
systemd-208-11.el7_0.2.x86_64
```

No exemplo do Red Hat Enterprise Linux 7 acima, a versão do systemd é a 208, portanto, os nomes previsíveis de interface de rede devem ser desativados.

b. Desabilite nomes previsíveis de interface de rede adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no `/etc/default/grub`.

```
sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
grub
```

c. Recompile o arquivo de configuração do grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar as redes avançadas no Linux (instâncias compatíveis com o armazenamento de instância).

8. No computador local, ative o atributo de rede avançada `enaSupport` usando um dos seguintes comandos:

   - modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
   ```

   - Edit-EC2InstanceAttribute (ferramentas para o Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

9. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

   Se o sistema operacional da instância contiver um arquivo `/etc/udev/rules.d/70-persistent-net.rules`, você deverá excluí-lo antes de criar a AMI. Esse arquivo contém o endereço MAC do adaptador de Ethernet da instância original. Se outra instância for iniciada com esse arquivo, o sistema operacional será incapaz de localizar o dispositivo e o `eth0` poderá falhar causando problemas de inicialização. Esse arquivo é gerado novamente no próximo ciclo de inicialização, e todas as instâncias executadas na AMI criam sua própria versão do arquivo.

10. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

11. (Opcional) Conecte-se à instância e verifique se o módulo está instalado.

    Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte Solução de problemas do Adaptador de Rede Elástica no Linux.

Para habilitar as redes avançadas no Linux (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias, habilitando o atributo de rede avançada ao registrar a AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu com DKMS

Esse método é apenas para fins de teste e feedback. Não é destinado ao uso com implantações de produção. Para implantações de produção, consulte Ubuntu.

> **Important**
>
> O uso do DKMS anula o acordo de suporte da sua assinatura. Ele não deve ser usado para implantações de produção.

Para habilitar a rede avançada com o ENA no Ubuntu (instâncias com suporte do EBS)

1. Siga as etapas 1 e 2 em Ubuntu.
2. Instale os pacotes do `build-essential` para compilar o módulo de kernel e o pacote `dkms` para que o módulo `ena` seja recompilado sempre que o kernel for atualizado.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clone a fonte do módulo `ena` na instância a partir do GitHub em https://github.com/amzn/amzn-drivers.

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Mova o pacote `amzn-drivers` para o diretório `/usr/src/` para que o DKMS possa localizá-lo e compilá-lo para cada atualização de kernel. Adicione o número da versão (é possível localizar o número da versão atual nas notas de release) do código-fonte ao nome do diretório. Por exemplo, a versão `1.0.0` é mostrada no exemplo a seguir.

   ```
   ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
   ```

5. Crie o arquivo de configuração do DKMS com os valores a seguir substituindo a versão do `ena`.

   Criar o arquivo.

   ```
   ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

   Edite o arquivo e adicione os valores a seguir.

   ```
   ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

```
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Adicione, compile e instale o módulo `ena` na instância usando o DKMS.

   Adicione o módulo ao DKMS.

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   Compile o módulo usando o comando dkms.

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   Instale o módulo usando o dkms.

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. Compile o `initramfs` novamente para que o módulo correto seja carregado na hora da inicialização.

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. Verifique se o módulo `ena` está instalado usando o comando modinfo ena em Testar se a rede avançada está habilitada.

   ```
   ubuntu:~$ modinfo ena
   filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:  1.0.0
   license:  GPL
   description: Elastic Network Adapter (ENA)
   author:   Amazon.com, Inc. or its affiliates
   srcversion:  9693C876C54CA64AE48F0CA
   alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
   alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
   ```

```
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
     0 - Automatically choose according to device capability (default)
     1 - Don't push anything to device memory
     3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
 (array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
 (int)
```

9. Passe para a etapa 3 em Ubuntu.

Habilitar redes avançadas no Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `enaSupport` da instância para ativar a rede avançada. Você somente poderá ativar esse atributo em tipos de instância compatíveis e somente se o driver ENA estiver instalado. Para obter mais informações, consulte Suporte a redes avançadas.

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e 2019 apenas] Execute o seguinte script do PowerShell do EC2Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Na instância, instale o driver da seguinte forma:
   a. Faça download do driver mais recente para a instância.
   b. Extraia o arquivo zip.
   c. Instale o driver executando o script `install.ps1` do PowerShell.

> **Note**
>
> Se você receber um erro de política de execução, defina a política como `Unrestricted` (por padrão, ela é definida como `Restricted` ou `RemoteSigned`). Em uma linha de comando, execute `Set-ExecutionPolicy -ExecutionPolicy Unrestricted` e, depois, execute o script `install.ps1` do PowerShell novamente.

4. No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
5. Ative o suporte ao ENA na instância da seguinte maneira:

   a. No computador local, verifique o atributo de suporte ao ENA da instância do EC2 em sua instância executando um dos seguinte comandos. Se o atributo não estiver habilitado, a saída será “[]” ou em branco. `EnaSupport` será definido como `false` por padrão.

   - describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

   - Get-EC2Instance (ferramentas para o Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

   b. Para ativar o suporte ao ENA, execute um dos seguintes comandos:

   - modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

   - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

Se encontrar problemas ao reiniciar a instância, também é possível desativar o suporte ao ENA com um dos seguintes comandos:

- modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

c. Verifique se o atributo foi definido como `true` usando describe-instances ou Get-EC2Instance conforme mostrado anteriormente. Você agora deve ver a seguinte saída:

```
[
 true
]
```

6. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI/AWS CloudShell), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, você deverá iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
7. Na instância, valide se o driver do ENA está instalado e ativado da seguinte maneira:

   a. Clique com o botão direito do mouse no ícone de rede e escolha Abrir Central de Rede e Compartilhamento.

   b. Escolha o adaptador de Ethernet (por exemplo, Ethernet 2).

   c. Escolha Detalhes. Para Detalhes da conexão de rede, verifique se a Descrição é Amazon Elastic Network Adapter.

8. (Opcional) Crie uma AMI na instância. A AMI herda o atributo `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com ENA ativado por padrão.

Notas de release do driver

Driver do ENA para o Linux

Para obter informações sobre as versões do driver do ENA para Linux, consulte as notas de release do driver do kernel do ENA para Linux.

Driver do ENA para o Windows

As AMIs do Windows incluem o driver do Amazon ENA para habilitar a rede avançada.

A tabela a seguir mostra a versão correspondente do driver ENA a ser baixada para cada versão do Windows Server.

Versão Windows Server	Versão do driver ENA
Windows Server 2022	2.4.0 e versões posteriores
Windows Server 2019	mais recente
Windows Server 2016	mais recente
Windows Server 2012 R2	2.6.0 e anterior
Windows Server 2012	2.6.0 e anterior
Windows Server 2008 R2	2.2.3 e anterior

A tabela a seguir resume as alterações de cada versão.

Versão do driver	Detalhes	Data de lançamento
2.7.0	Novos atributos • Removido o suporte ao Windows Server 2012 (Windows 8) e ao Windows Server 2012 R2 (Windows	1º de maio de 2024

Versão do driver	Detalhes	Data de lançamento
	8.1). A AWS não oferece mais suporte a essas versões do sistema operacional. A instalação do driver falhará no Windows Server 2012 e versões anteriores. • Adicionado suporte a descarrega do cálculo da soma de verificação IPv6 Tx para o dispositivo. • Adicionado amplo suporte a Low Latency Queuing (LLQ). Isso é habilitado dinamicamente com base na recomendação do dispositivo. Você pode substitui r essa configuração pela nova chave de registro "WideLLQ". • Adicionado relatório de descarte de pacotes devido a sobrecarga de Rx, o que indica espaço insuficiente no ring Rx para pacotes recebidos. • Adicionado suporte para notificações do dispositivo sobre configurações não ideais. Veja o ID de evento `59000` no visualizador de eventos do Windows. Correções de bugs • Evite a reinicialização desnecessária do dispositivo causada por pacotes Tx com cabeçalhos que excedem o tamanho máximo de cabeçalho de Low Latency Queuing (LLQ).	

Versão do driver	Detalhes	Data de lançamento

2.6.0	Novos atributos
	• Adiciona as seguintes métricas de desempenho de rede para tipos de instância que oferecem suporte ao ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Adiciona uma métrica de performance de rede `conntrack_allowance_available` para tipos de instância baseados em Nitro.
	• Adiciona um novo motivo de reinicialização do adaptador devido à detecção de corrupção de dados RX.
	• Atualiza a infraestrutura de registro de drivers.
	
	Correções de bugs
	• Impede a reinicialização do adaptador caso a falta de CPU faça com que uma atualização das métricas de performance da rede falhe.
	•
		20 de junho de 2023

Versão do driver	Detalhes	Data de lançamento
	Impede a falsa detecção de uma interrupção no heartbeat do dispositivo. • Corrige o script de instalação do driver para ser compatível com a operação de downgrade. • Corrige a estatística de contagem de erros de recebimento.	
2.5.0	Comunicado O driver do ENA Windows versão 2.5.0 foi revertido devido à falha na inicialização da controladora de domínio Windows. O Windows Client e o Windows Server não são afetados.	17 de fevereiro de 2023

Versão do driver	Detalhes	Data de lançamento
2.4.0	Novos atributos • Acrescenta suporte para Windows Server 2022. • Remove o suporte para Windows Server 2008 R2. • Define o enfileiramento de baixa latência (LLQ) como sempre ativo para melhorar a performance em instâncias do Amazon EC2 de sexta geração. Correção de bugs • Corrige uma falha na publicação de métricas de performance de rede no sistema de contadores de performance do Windows (PCW). • Corrige uma perda de memória durante a operação de leitura da chave de registro. • Impede um loop de reinicialização infinito em caso de erro irrecuperável durante o processo de redefinição do adaptador.	28 de abril de 2022

Versão do driver	Detalhes	Data de lançamento
2.2.4	Comunicado O driver ENA Windows versão 2.2.4 foi revertido devido à possível degradação da performance nas instâncias do EC2 de sexta geração. Recomendamos que você faça o downgrade do driver usando um dos seguintes métodos: • Instalar a versão anterior 1. Baixe o pacote da versão anterior pelo link nesta tabela (versão 2.2.3). 2. Execute o script de instalação do PowerShell install.ps1. Para obter mais detalhes sobre as etapas de pré e pós-instalação, consulte Habilitar redes avançadas no Windows. Usar o Amazon EC2 Systems Manager para uma atualização em massa • Execute uma atualização em massa por meio do documento SSM `AWS-ConfigureAWSPackage` com os seguintes parâmetros: • Name (Nome): AwsEnaNetworkDriver • Version (Versão): 2.2.3	26 de outubro de 2021

Versão do driver	Detalhes	Data de lançamento
2.2.3	Novo recurso • Adiciona suporte para novos Nitro Cards com rede de instâncias de até 400 Gbps. Correção de bugs • Corrige um comportamento de disputa entre a mudança de hora do sistema e a consulta de hora do sistema pelo driver do ENA, que causa a detecção falso-positiva de falta de resposta de HW. O driver ENA versão 2.2.3 para Windows é a versão final compatível com Windows Server 2008 R2. Os tipos de instância atualmente disponíveis que usam ENA continuarão tendo suporte no Windows Server 2008 R2, e os drivers estarão disponíveis por download. Nenhum tipo futuro de instância será compatível com Windows Server 2008 R2 e você não poderá executar, importar ou migrar imagens do Windows Server 2008 R2 para tipos futuros de instância.	25 de março de 2021

Versão do driver	Detalhes	Data de lançamento
2.2.2	Novo recurso • Adiciona suporte para consultar métricas de performance do adaptador de rede com o CloudWatch e os Contadores de performance para consumidores do Windows. Correção de bugs • Corrige problemas de performance em instâncias bare metal.	21 de dezembro de 2020
2.2.1	Novo recurso • Adiciona um método para permitir que o host consulte o Elastic Network Adapter para obter métricas de performance da rede.	1º de outubro de 2020

Versão do driver	Detalhes	Data de lançamento
2.2.0	Novos recursos • Adiciona suporte aos tipos de hardware de próxima geração. • Melhora o tempo de inicialização da instância após retomar de uma parada de hibernação e elimina mensagens de erro de falsos positivos de ENA. Otimizações da performance • Otimiza o processamento do tráfego de entrada. • Melhora o gerenciamento de memória compartilhada em um ambiente de recursos escassos. Correção de bugs • Evita a falha do sistema após a remoção do dispositivo do ENA em um cenário raro em que há falha na redefinição do driver.	12 de agosto de 2020
2.1.5	Correção de bugs • Corrige falhas ocasionais de inicialização do adaptador de rede em instâncias bare metal.	23 de junho de 2020

Versão do driver	Detalhes	Data de lançamento
2.1.4	Correções de bugs • Evite problemas de conectividade causados por metadados de pacotes LSO corruptos chegando da pilha da rede. • Evite falha no sistema causada por uma condição de corrida rara que resulta no acesso de uma memória de pacote já liberada.	25 de novembro de 2019
2.1.2	Novo recurso • Adição de suporte para que o relatório do ID do fornecedor permita que o SO gere UUIDs baseadas em MAC. Correções de bugs • Melhoria na performance da configuração de rede DHCP durante a inicialização. • Calcule corretamente a soma de verificação L4 no tráfego IPv6 de entrada quando a unidade de transmissão máxima (MTU) exceder 4K. • Melhorias gerais na estabilidade do driver e correções de erros secundárias.	4 de novembro de 2019

Versão do driver	Detalhes	Data de lançamento
2.1.1	Correções de bugs • Previnem a chegada de pacotes LSO TCP altamente fragmentados do sistema operacional. • Lidam corretamente com o protocolo Encapsulating Security Payload (ESP) dentro do IPSec em redes IPv6.	16 de setembro de 2019

Versão do driver	Detalhes	Data de lançamento

2.1.0	O driver ENA v2.1 do Windows apresenta novos recursos do dispositivo ENA, dá um impulso à performance, adiciona novos recursos e inclui várias melhorias de estabilidade.
	• Novos recursos
	  • Use a chave do Registro do Windows padronizada para configuração dos frames jumbo.
	  • Permitir a configuração do ID da VLAN via a GUI das propriedades do driver ENA.
	  • Fluxos de recuperação melhorados
	  • Melhora no mecanismo de identificação de falhas.
	  • Adicionado suporte para parâmetros de recuperação ajustáveis.
	  • Compatibilidade para até 32 filas de E/S para instâncias do EC2 mais novas, que têm mais de 8 vCPUs.
	  • Redução de ~90% da presença de memória do driver.
	• Otimizações da performance
	  • Redução na latência do caminho de transmissão.
	  • Suporte para receber o descarregamento da soma de verificação.
	  •
		1 de julho de 2019

Versão do driver	Detalhes	Data de lançamento
	Otimização da performance para um sistema pesadamente carregado (uso otimizado dos mecanismos de bloqueio). • Outras melhorias para reduzir a utilização da CPU e melhorar a responsividade do sistema em carga. • Correções de bugs • Corrigir a falha devido à análise inválida de cabeçalhos Tx não contíguos. • Corrija a falha do driver v1.5 durante o desvincul amento da interface de rede elástica em instâncias bare metal. • Corrigir o erro de cálculo da soma de verificação do pseudocabeçalho do LSO sobre IPv6. • Corrigir o vazamento de recursos de memória em potencial na falha da inicialização. • Desabilitar o descarregamento da soma de verificaç ão de TCP/UDP para fragmentos de IPv4. • Corrigir para configuração da VLAN. A VLAN foi desabilitada incorretamente quando somente a prioridade da VLAN deveria ter sido desabilitada. • Habilitar a análise das mensagens do driver personalizado pelo visualizador de eventos. • Corrigir a falha em inicializar o driver devido a tratamento de timestamp inválido.	

Versão do driver	Detalhes	Data de lançamento
	• Corrigir a condição da corrida entre o processamento de dados e a desabilitação do dispositivo ENA.	
1.5.0	• Estabilidade aprimorada e correções de performance. • Os buffers de recebimento agora podem ser configura dos até um valor de 8192 em Advanced Properties (Propriedades avançadas) de NIC do ENA. • Buffers de recebimento padrão de 1 k.	4 de outubro de 2018
1.2.3	Inclui correções de confiabilidade e unifica o suporte para o Windows Server 2008 R2 por meio do Windows Server 2016.	13 de fevereiro de 2018
1.0.8	A versão inicial. Incluída em AMIs do Windows Server 2008, do Windows Server 2012 RTM, do Windows Server 2012 R2 e do Windows Server 2016.	Julho de 2016

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Para assinar as notificações do EC2

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:

a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

   arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. Para Protocolo, selecione `Email`.

c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.

d. Selecione Create subscription.

6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Subscriptions.
3. Marque a caixa de seleção da assinatura e, depois, selecione Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Aprimoramento do desempenho da rede com o ENA Express nas instâncias do EC2

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). SRD é um protocolo de transporte de rede de alta performance que usa roteamento dinâmico para aumentar o throughput e minimizar a latência final. Com o ENA Express, é possível estabelecer a comunicação entre duas instâncias do EC2 na mesma zona de disponibilidade.

Benefícios do ENA Express

- Aumenta a largura de banda máxima que um único fluxo pode usar de 5 Gbps para 25 Gbps na sub-rede, até o limite da instância agregado.
- Reduz a latência final do tráfego de rede entre instâncias do EC2, especialmente durante períodos de grande carga na rede.
- Detecta e evita caminhos de rede congestionados.

- Executa algumas tarefas diretamente na camada da rede, como a reordenação de pacotes na extremidade receptora e a maioria das retransmissões necessárias. Isso libera a camada de aplicação para outros trabalhos.

> **Note**
>
> Se a aplicação enviar ou receber um grande volume de pacotes por segundo e precisar otimizar a latência a maioria das vezes, especialmente durante períodos em que não há congestionamento na rede, o Redes avançadas pode ser mais adequado para a sua rede.

Durante períodos em que o tráfego de rede é leve, você pode notar um ligeiro aumento na latência de pacote (dezenas de microssegundos) quando o pacote usa o ENA Express. Durante esses períodos, as aplicações que priorizam características específicas de performance de rede podem se beneficiar do ENA Express da seguinte forma:

- Os processos podem se beneficiar do aumento da largura de banda máxima de um único fluxo de 5 Gbps para 25 Gbps na mesma zona de disponibilidade, até o limite da instância agregada. Por exemplo, se um tipo de instância específico for compatível com até 12,5 Gbps, a largura de banda de um único fluxo também será limitada a 12,5 Gbps.
- Processos mais longos devem ter uma latência de cauda reduzida durante períodos de congestionamento da rede.
- Os processos podem se beneficiar de uma distribuição mais suave e padrão dos tempos de resposta da rede.

Pré-requisitos para instâncias Linux

Para garantir que o ENA Express possa operar de forma eficaz, atualize as configurações da instância da maneira apresentada a seguir.

- Se sua instância usar frames jumbo, execute o comando a seguir para definir a unidade máxima de transmissão (MTU) como `8900`.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Aumente o tamanho do anel do receptor (Rx), da seguinte forma:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Para maximizar a largura de banda do ENA Express, configure seus limites de fila TCP da seguinte forma:

  1. Defina o limite de fila pequena do TCP para 1 MB ou mais. Isso aumenta a quantidade de dados enfileirados para transmissão em um soquete.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Desabilite os limites da fila de bytes no enésimo dispositivo se eles estiverem habilitados para sua distribuição Linux. Fazer isso aumenta os dados enfileirados para transmissão para a fila do dispositivo.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

     > **Note**
     >
     > O driver do ENA para a distribuição Amazon Linux desabilita os limites da fila de bytes por padrão.

Como o ENA Express funciona

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). O mecanismo distribui pacotes para cada fluxo de rede em diferentes caminhos de rede da AWS e ajusta dinamicamente a distribuição quando detecta sinais de congestionamento. Ele também gerencia a reordenação de pacotes na extremidade receptora.

Para garantir que o ENA Express possa gerenciar o tráfego de rede conforme previsto, as instâncias de envio e recebimento e a comunicação entre elas devem atender a todos os seguintes requisitos:

- Os tipos de instâncias de envio e de recebimento são compatíveis. Para obter mais informações, consulte a tabela Tipos de instâncias compatíveis com o ENA Express.
- As instâncias de envio e de recebimento devem ter o ENA Express configurado. Se houver diferenças na configuração, você pode se deparar com situações em que o tráfego use a transmissão ENA padrão. O cenário a seguir mostra o que pode acontecer.

Cenário: diferenças na configuração

Instância	ENA Express habilitado	O UDP usa o ENA Express
Instância 1	Sim	Sim
Instância 2	Sim	Não

Nesse caso, o tráfego TCP entre as duas instâncias pode usar o ENA Express, pois ambas as instâncias o habilitaram. No entanto, como uma das instâncias não usa o ENA Express para tráfego UDP, a comunicação entre essas duas instâncias por UDP usa a transmissão ENA padrão.

- As instâncias de envio e recebimento devem ser executadas na mesma zona de disponibilidade.
- O caminho da rede entre as instâncias não deve incluir caixas de middleware. No momento, o ENA Express não é compatível com caixas de middleware.
- (Somente para instâncias do Linux) Para utilizar todo o potencial da largura de banda, use a versão 2.2.9 ou versões posteriores do driver.
- (Somente para instâncias do Linux) Para produzir métricas, use a versão 2.8 ou versões posteriores do driver.

Se algum requisito não for atendido, as instâncias usarão o protocolo TCP/UDP padrão, mas sem o SRD para comunicação.

Para garantir que o driver de rede da instância esteja configurado para performance ideal, analise as melhores práticas recomendadas para drivers do ENA. Essas práticas recomendadas também se aplicam ao ENA Express. Para obter mais informações, consulte ENA Linux Driver Best Practices and Performance Optimization Guide (Guia de Práticas Recomendadas e Otimização de Performance do Driver) no GitHub.

> **Note**
>
> O Amazon EC2 se refere à relação entre uma instância e uma interface de rede que está anexada a ela como um anexo. As configurações do ENA Express se aplicam ao anexo. Se a interface de rede for separada da instância, o anexo deixará de existir e as configurações

do ENA Express aplicadas a ele não estarão mais em vigor. O mesmo acontece quando uma instância é encerrada, mesmo que a interface de rede permaneça.

Tipos de instâncias compatíveis com o ENA Express

As guias a seguir mostram os tipos de instância compatíveis com o ENA Express.

General purpose

Tipo de instância	Arquitetura
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64

Tipo de instância	Arquitetura
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Tipo de instância	Arquitetura
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64

Tipo de instância	Arquitetura
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64

Tipo de instância	Arquitetura
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64

Memory optimized

Tipo de instância	Arquitetura
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64

Tipo de instância	Arquitetura
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64

Tipo de instância	Arquitetura
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Tipo de instância	Arquitetura
g6.48xlarge	x86_64

Storage optimized

Tipo de instância	Arquitetura
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Listar e visualizar as configurações do ENA Express

Esta seção aborda como listar e visualizar as informações do ENA Express no AWS Management Console ou na AWS CLI. Para obter mais informações, escolha a guia que corresponda ao método que você usará.

Console

Essa guia explica como encontrar informações sobre as configurações atuais do ENA Express e como visualizar os tipos de instância compatíveis no AWS Management Console.

Visualizar os tipos de instância compatíveis

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione um tipo de instância para ver os detalhes dessa instância. Você pode escolher o link Instance type (Tipo de instância) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista para ver os detalhes no painel de detalhes na parte inferior da página.
4. Na guia Networking (Rede) ou nessa seção na página de detalhes, ENA Express support (Compatibilidade do ENA Express) mostra um valor verdadeiro ou falso para indicar se o tipo de instância é compatível com esse recurso.

Visualizar configurações na lista de interfaces de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces (Interfaces de rede).
3. Selecione uma interface de rede para ver os detalhes dessa instância. Você pode escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista para ver os detalhes no painel de detalhes na parte inferior da página.
4. Na seção Network interface attachment (Anexo da interface de rede) na guia Details (Detalhes) ou na página de detalhes, revise as configurações do ENA Express e do UDP do ENA Express.

Visualizar configurações em instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione uma instância para ver os detalhes dessa instância. Você pode escolher o link Instance ID (ID da instância) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista para ver os detalhes no painel de detalhes na parte inferior da página.
4. Na seção Network interfaces (Interfaces de rede) na guia Networking (Rede), role para a direita para revisar as configurações do ENA Express e do UDP do ENA Express.

AWS CLI

Essa guia explica como encontrar informações sobre as configurações atuais do ENA Express e como visualizar os tipos de instância compatíveis no AWS CLI.

Descrever tipos de instância

Para obter informações sobre as configurações de um tipo de instância específico, execute o comando describe-instance-types na AWS CLI e substitua o tipo de instância da seguinte forma:

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
"InstanceTypes": [
{
 "InstanceType": "m6i.metal",
 "CurrentGeneration": true,
 ...
 },
 "NetworkInfo": {
  ...
  "EnaSrdSupported": true
 },
 ...
}
]
}
```

Descrever instâncias

Para obter informações sobre a configuração do ENA Express para instâncias especificadas, execute o comando describe-instances na AWS CLI conforme mostrado a seguir. Esse exemplo de comando retorna uma lista de configurações do ENA Express para as interfaces de rede associadas a cada uma das instâncias em execução especificadas pelo parâmetro `--instance-ids`.

```
[ec2-user ~]$ aws ec2 describe-instances --instance-
ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].
[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'[
 [
  [
   "i-1234567890abcdef0",
   [
```

```
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ],
 [
  [
   "i-0598c7d356eba48d7",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ]
]
```

Describe network interfaces

Para obter informações sobre as configurações do ENA Express para uma interface de rede, execute o comando describe-network-interfaces na AWS CLI da seguinte forma:

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
{
 "Association": {
  ....IPs, DNS...
 },
 "Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
```

```
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
   "EnaSrdEnabled": true,
   "EnaSrdUdpSpecification": {
    "EnaSrdUdpEnabled": true
   }
  }
 },
 ...
 "NetworkInterfaceId": "eni-1234567890abcdef0",
 "OwnerId": "111122223333",
 ...
}
]
}
```

PowerShell

Esta guia explica como encontrar informações sobre as configurações atuais do ENA Express e como visualizar os tipos de instância compatíveis usando o PowerShell.

Descrever tipos de instância

Para obter informações sobre configurações de tipo de instância para uma instância específica, execute o comando Get-EC2InstanceType Cmdlet no Tools for PowerShell e substitua o tipo de instância da seguinte forma:

```
PS C:\> Get-EC2InstanceType -InstanceType m6i.metal | `
Select-Object `
    InstanceType,
    CurrentGeneration,
    @{Name = 'EnaSrdSupported'; Expression = { $_.NetworkInfo.EnaSrdSupported } } |
 `
Format-List

InstanceType      : m6i.metal
CurrentGeneration : True
EnaSrdSupported   : True
```

Se o ENA Express estiver habilitado um valor de `True` será devolvido.

Describe network interfaces

Para obter informações sobre as configurações do ENA Express para uma interface de rede, execute o comando Get-EC2NetworkInterface Cmdlet com o Tools for PowerShell da seguinte forma:

```
PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-0d1234e5f6a78901b
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Definir as configurações do ENA Express

Você pode configurar o ENA Express para os tipos de instância do EC2 compatíveis sem precisar instalar qualquer software adicional.

Esta seção aborda como configurar o ENA Express no AWS Management Console ou na AWS CLI. Para obter mais informações, escolha a guia que corresponda ao método que você usará.

Console

Essa guia explica como gerenciar as configurações do ENA Express para interfaces de rede anexadas a uma instância.

Gerenciar o ENA Express na lista de interfaces de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces (Interfaces de rede).
3. Selecione uma interface de rede que é anexada a uma instância. Você pode escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Escolha Manage ENA Express (Gerenciar o ENA Express) no menu Action (Ação) no canto superior direito da página. Isso abre a caixa de diálogo Manage ENA Express (Gerenciar o ENA Express), com o ID da interface de rede selecionado e as configurações atuais exibidas.

   > **Note**
   >
   > Se a interface de rede selecionada não estiver anexada a uma instância, essa ação não aparecerá no menu.

5. Para usar o ENA Express, marque a caixa de seleção Enable (Habilitar).
6. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Enable (Habilitar).
7. Para salvar suas configurações, escolha Save (Salvar).

Gerenciar o ENA Express na lista de instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância que você quer gerenciar. Você pode escolher o link Instance ID (ID da instância) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Selecione a Network interface (Interface de rede) a ser configurada para sua instância.
5. Escolha Manage ENA Express (Gerenciar o ENA Express) no menu Action (Ação) no canto superior direito da página.

6. Para configurar o ENA Express para uma interface de rede anexada à instância, selecione-a na lista Network interface (Interface de rede).
7. Para usar o ENA Express para o anexo de interface de rede selecionado, marque a caixa de seleção Enable (Habilitar).
8. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Enable (Habilitar).
9. Para salvar suas configurações, escolha Save (Salvar).

Configurar o ENA Express ao anexar uma interface de rede a uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces (Interfaces de rede).
3. Selecione uma interface que não esteja anexada a uma instância (o Status é Available [Disponível]). Você pode escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Selecione a Instance (Instância) à qual você vai anexar.
5. Para usar o ENA Express depois de anexar a interface de rede à instância, marque a caixa de seleção Enable (Habilitar).
6. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Enable (Habilitar).
7. Para anexar a interface de rede à instância e salvar as configurações do ENA Express, escolha Attach (Anexar).

AWS CLI

Essa guia explica como definir as configurações do ENA Express na AWS CLI.

Configurar o ENA Express ao anexar uma interface de rede

Para configurar o ENA Express ao anexar uma interface de rede a uma instância, execute o comando attach-network-interface na AWS CLI, conforme mostrado nos seguintes exemplos:

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` como true (verdadeiro) e permitimos que `EnaSrdUdpEnabled` assuma o padrão false (falso).

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` e `EnaSrdUdpEnabled` como true (verdadeiros).

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Atualizar as configurações do ENA Express para o anexo da interface de rede

Para atualizar as configurações do ENA Express para uma interface de rede anexada a uma instância, execute o comando modify-network-interface-attribute na AWS CLI, conforme mostrado nos seguintes exemplos:

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` como true (verdadeiro) e permitimos que `EnaSrdUdpEnabled` assuma o padrão de false (falso) se nunca tiver sido definido antes.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` e `EnaSrdUdpEnabled` como true (verdadeiros).

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Exemplo 3: parar de usar o ENA Express para tráfego UDP

Neste exemplo, configuramos `EnaSrdUdpEnabled` como false (falso).

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Esta guia explica como definir as configurações do ENA Express usando o PowerShell.

Configurar o ENA Express ao anexar uma interface de rede

Para definir as configurações do ENA Express para uma interface de rede, execute o comando Add-EC2NetworkInterface Cmdlet com o Tools for PowerShell conforme mostrado nos seguintes exemplos:

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` como true (verdadeiro) e permitimos que `EnaSrdUdpEnabled` assuma o padrão false (falso).

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true

eni-attach-012c3d45e678f9012
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` e `EnaSrdUdpEnabled` como true (verdadeiros).

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true
```

```
eni-attach-012c3d45e678f9012
```

Atualizar as configurações do ENA Express para o anexo da interface de rede

Para atualizar as configurações do ENA Express para uma interface de rede anexada a uma instância, execute o comando Add-EC2NetworkInterface Cmdlet no Tools for PowerShell conforme mostrado nos seguintes exemplos:

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` como true (verdadeiro) e permitimos que `EnaSrdUdpEnabled` assuma o padrão de false (falso) se nunca tiver sido definido antes.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Neste exemplo, configuramos `EnaSrdEnabled` e `EnaSrdUdpEnabled` como true (verdadeiros).

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
```

```
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True
```

Exemplo 3: parar de usar o ENA Express para tráfego UDP

Neste exemplo, configuramos `EnaSrdUdpEnabled` como false (falso).

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Configuração do ENA Express na inicialização

Você pode usar um dos métodos a seguir para configurar o ENA Express para uma AMI ao iniciar uma instância usando o AWS Management Console.

- Você pode configurar o ENA Express para a AMI ao iniciar uma instância com o assistente de inicialização de instâncias. Para obter detalhes sobre a configuração, consulte Configuração avançada de rede nas Configurações de rede para o assistente de inicialização de instâncias.
- Você pode configurar o ENA Express para sua AMI ao usar um modelo de inicialização. Para obter mais informações sobre a configuração do modelo de inicialização, consulte Configuração avançada de rede no Configurações de rede para modelos de inicialização.

Monitorar a performance do ENA Express

Depois de habilitar o ENA Express para as anexos de interface de rede na instância de envio e na instância de recebimento, você pode usar as métricas do ENA Express para ajudar a garantir que as instâncias aproveitem ao máximo as melhorias de performance que a tecnologia SRD oferece.

Para ver uma lista de métricas filtradas para o ENA Express, execute o seguinte comando ethtool para a interface de rede (mostrado aqui como `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Verificar as configurações do ENA Express para uma instância

Para verificar as configurações atuais do ENA Express para o anexo de interface de rede na instância, execute o comando `ethtool` para listar as métricas do ENA Express e anote o valor da métrica `ena_srd_mode`. Os valores são os seguintes:

- `0` = ENA Express desativado, UDP desativado
- `1` = ENA Express ativado, UDP desativado
- `2` = ENA Express desativado, UDP ativado

> **Note**
>
> Isso só acontece quando o ENA Express foi originalmente habilitado e o UDP foi configurado para usá-lo. O valor anterior é retido para tráfego UDP.

- `3` = ENA Express ativado, UDP ativado

Depois de habilitar o ENA Express para a conexão da interface de rede em uma instância, a instância de envio inicia a comunicação com a instância de recebimento e o SRD detecta se o ENA Express está operando tanto na instância de envio quanto na instância de recebimento. Se o ENA Express estiver operando, a comunicação poderá usar transmissão SRD. Se o ENA Express não estiver operando, a comunicação retornará para a transmissão por ENA padrão. Para confirmar se

a transmissão de pacotes está usando SRD, você pode comparar o número de pacotes elegíveis (métrica `ena_srd_eligible_tx_pkts`) com o número de pacotes por SRD transmitidos (métrica `ena_srd_tx_pkts`) durante um determinado período.

Você pode monitorar a utilização do recursos SRD usando a métrica `ena_srd_resource_utilization`. Se a instância estiver prestes a esgotar seus recursos de SRD, você saberá que está na hora de aumentar a escala da instância horizontalmente.

Para obter mais informações sobre as métricas do ENA Express, consulte Métricas do ENA Express.

Ajuste do desempenho para as configurações do ENA Express

Para verificar a configuração da sua instância Linux a fim de extrair a performance ideal do ENA Express, é possível executar o seguinte script que está disponível no repositório do Amazon GitHub:

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh

O script executa uma série de testes e sugere as alterações de configuração recomendadas e necessárias.

Habilitação de redes aperfeiçoadas com a interface Intel 82599 VF nas instâncias do EC2

O Amazon EC2 fornece recursos de redes avançadas por meio da interface Intel 82599 VF, que usa o driver `ixgbevf` da Intel.

Conteúdo

- Requisitos
- Verificação da instalação do driver
- Testar se a rede avançada está habilitada
- Habilitar redes avançadas na instância
- Solucionar problemas de conectividade

Requisitos

Para se preparar para a rede avançada com a interface Intel 82599 VF, configure a instância da seguinte forma:

- Selecione um dos seguintes tipos de instância compatíveis: C3, C4, D2, I2, M4 (exceto `m4.16xlarge`) e R3.
- Verifique se a instância tem conectividade com a Internet.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização de kernels e módulos de kernel e a habilitação do atributo `sriovNetSupport` podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.
- Instâncias do Linux: inicie a instância usando uma AMI de HVM com a versão 2.6.32 ou com versões posteriores do kernel do Linux. As AMIs HVM do Amazon Linux mais recentes têm os módulos necessários para a rede avançada instalada e também têm os atributos necessários definidos. Portanto, se você executar uma instância compatível com redes avançadas com Amazon EBS que usa uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância.

  > **Warning**
  >
  > A rede avançada é compatível apenas com instâncias de HVM. A habilitação da rede avançada com uma instância PV pode torná-la inacessível. A configuração desse atributo sem o módulo ou a versão do módulo adequados também pode tornar a instância inacessível.

- Instâncias do Windows: inicie a instância usando uma AMI de HVM de 64 bits. Não é possível habilitar as redes aperfeiçoadas no Windows Server 2008. A rede avançada já está habilitada para AMIs do Windows Server 2012 R2 e do Windows Server 2016 e posterior. O Windows Server 2012 R2 inclui o driver 1.0.15.3 da Intel e recomendamos atualizar esse driver para a versão mais recente usando o utilitário Pnputil.exe.
- Use o AWS CloudShell do AWS Management Console ou instale e configure a AWS CLI ou o AWS Tools for Windows PowerShell em qualquer computador que desejar, de preferência em seu desktop ou notebook local. Para obter mais informações sobre o ACM, consulte Acessar o Amazon EC2 ou o Guia do usuário do AWS CloudShell. A rede avançada não pode ser gerenciada no console do Amazon EC2.

Verificação da instalação do driver

Verifique se o driver está instalado na instância.

Driver da interface de rede do Linux

Use o comando a seguir para verificar se o módulo está sendo usado em uma interface específica, substituindo o nome da interface que você deseja verificar. Se estiver usando uma única interface (padrão), ela será `eth0`. Se o sistema operacional oferecer suporte a nomes de rede previsíveis, esse poderá ser um nome como `ens5`.

No exemplo acima, o módulo `ixgbevf` não está carregado porque o driver listado é `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Nesse exemplo, o módulo `ixgbevf` está carregado. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Adaptador de rede do Windows

Para verificar se o driver está instalado, conecte-se à instância e abra o Gerenciador de dispositivos. É necessário ver a “Intel (R 82599) Virtual Function” listada em Network adapters.

Testar se a rede avançada está habilitada

Verifique se o atributo `sriovNetSupport` está definido.

Atributo de instância (sriovNetSupport)

Para verificar se uma instância tem o atributo `sriovNetSupport` de rede avançada definido, use um dos seguintes comandos. Se o atributo estiver definido, o valor será `simple`.

- describe-instance-attribute (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
 sriovNetSupport
```

- Get-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Atributo de imagem (sriovNetSupport)

Para verificar se uma AMI já tem o conjunto de atributos de redes aperfeiçoadas `sriovNetSupport`, use um dos comandos apresentados a seguir. Se o atributo estiver definido, o valor será `simple`.

- describe-images (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Habilitar redes avançadas na instância

O procedimento usado dependerá do sistema operacional da instância.

> **Warning**
>
> Não há nenhuma maneira de desabilitar o atributo de rede avançada depois de ele ser habilitado.

Amazon Linux

As AMIs de HVM do Amazon Linux têm o módulo `ixgbevf` necessário para a rede avançada instalado e também têm o atributo necessário `sriovNetSupport` definido. Portanto, se você executar um tipo de instância que use uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Se você executou a instância usando uma AMI do Amazon Linux mais antiga e ela ainda não tiver a rede avançada habilitada, use o seguinte procedimento para habilitar a rede avançada.

Para habilitar a rede avançada

1. Conecte-se à sua instância.
2. Na instância, execute o seguinte comando para atualizar a instância com o kernel e os módulos de kernel mais recentes incluindo `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. No computador local, reinicialize a instância usando o console do Amazon EC2 ou um dos seguintes comandos: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Conecte-se à instância novamente e verifique se o módulo `ixgbevf` está instalado e na versão mínima recomendada usando o comando modinfo ixgbevf em Testar se a rede avançada está habilitada.
5. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar a rede avançada (instâncias compatíveis com o armazenamento de instâncias).
6. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
 simple
```

PowerShell

Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
8. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
9. Conecte-se à instância e verifique se o módulo `ixgbevf` está instalado e carregado na interface de rede usando o comando ethtool -i eth***n*** em Testar se a rede avançada está habilitada.

Para habilitar a rede avançada (instâncias compatíveis com o armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias, habilitando o atributo de rede avançada ao registrar a AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Antes de começar, o verifica se a rede avançada já está habilitada em sua instância.

As AMIs do Ubuntu HVM Quick Start incluem os drivers necessários para redes aprimoradas. Se você tiver uma versão de `ixgbevf` anterior a 2.16.4, poderá instalar o `linux-aws` pacote do kernel para obter os drivers de rede aprimorados mais recentes.

O procedimento a seguir fornece as etapas gerais para compilar o módulo `ixgbevf` em uma instância do Ubuntu.

Para instalar o pacote do kernel **`linux-aws`**

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes e os pacotes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se, durante o processo de atualização, for solicitada a instalação do `grub`, use o `/dev/xvda` para instalar o `grub` e, em seguida, escolha manter a versão atual do `/boot/grub/menu.lst`.

Outras distribuições do Linux

Antes de começar, o verifica se a rede avançada já está habilitada em sua instância. As AMIs do HVM Quick Start mais recentes incluem os drivers necessários para rede avançada, portanto, você não precisa executar etapas adicionais.

O procedimento a seguir fornece as etapas gerais se precisar habilitar a rede avançada com a interface Intel 82599 VF em uma distribuição do Linux diferente do Amazon Linux ou do Ubuntu. Para obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou suporte para o pacote e a ferramenta, consulte a documentação específica à sua distribuição do Linux.

Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.

2. Faça download da fonte para o módulo `ixgbevf` na instância do Sourceforge em https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Versões do `ixgbevf` anteriores à 2.16.4, incluindo a versão 2.14.2, não são compiladas adequadamente em algumas distribuições do Linux, incluindo certas versões do Ubuntu.

3. Compile e instale o módulo `ixgbevf` na instância.

   > **Warning**
   >
   > Se você compilar o módulo `ixgbevf` para o kernel atual e, depois, atualizar o kernel sem recompilar o driver para o novo kernel, o sistema poderá reverter o módulo `ixgbevf` específico à distribuição na próxima reinicialização. Isso poderá tornar o sistema inacessível se a versão específica à distribuição for incompatível com a rede avançada.

4. Execute o comando sudo depmod para atualizar as dependências do módulo.

5. Atualize o `initramfs` na instância para garantir que o novo módulo seja carregado na hora da inicialização.

6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do systemd ou udev podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte Nomes previsíveis de interface de rede no site freedesktop.org.

   a. É possível verificar as versões do systemd ou udev em sistemas baseados em RPM com o seguinte comando:

      ```
      [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
      systemd-208-11.el7_0.2.x86_64
      ```

      No exemplo do Red Hat Enterprise Linux 7 acima, a versão do systemd é a 208, portanto, os nomes previsíveis de interface de rede devem ser desativados.

   b. Desabilite nomes previsíveis de interface de rede adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
etc/default/grub
```

c. Recompile o arquivo de configuração do grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar as redes avançadas (instâncias compatíveis com o armazenamento de instância).

8. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

9. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

   Se o sistema operacional da instância contiver um arquivo `/etc/udev/rules.d/70-persistent-net.rules`, você deverá excluí-lo antes de criar a AMI. Esse arquivo contém o endereço MAC do adaptador de Ethernet da instância original. Se outra instância for iniciada com esse arquivo, o sistema operacional será incapaz de localizar o dispositivo e o `eth0` poderá

falhar causando problemas de inicialização. Esse arquivo é gerado novamente no próximo ciclo de inicialização, e todas as instâncias executadas na AMI criam sua própria versão do arquivo.

10. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
11. (Opcional) Conecte-se à instância e verifique se o módulo está instalado.

Para habilitar as redes avançadas (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias, habilitando o atributo de rede avançada ao registrar a AMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `sriovNetSupport` da instância para ativar a rede avançada. Você só pode habilitar esse atributo em tipos de instâncias compatíveis. Para ter mais informações, consulte Suporte a redes avançadas.

> **Important**
>
> Para ver as atualizações de driver mais recentes nas AMIs do Windows, consulte o histórico de versões da AMI do Windows na Referência da AMI do AWS Windows.

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e posterior] Execute o seguinte script PowerShell do EC2 Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> A senha do administrador será redefinida quando você habilitar o script de inicialização do EC2 da instância. É possível modificar o arquivo de configuração para desabilitar a redefinição da senha do administrador especificando-a nas configurações das tarefas de inicialização.

3. Na instância, faça download do driver do adaptador de rede da Intel para seu sistema operacional:

   - Windows Server 2022

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2019, inclusive para a versão de servidor 1809 e posterior*

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2016, inclusive para a versão de servidor 1803 e anterior*

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2012 R2

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2012

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2008 R2

     Visite a página de download e faça download do `PROWinx64Legacy.exe`.

*As versões de servidor 1803 e anteriores, bem como a 1809 e posterior, não são especificamente abordadas nas páginas de Drivers e Software da Intel.

4. Instale o driver do adaptador de rede da Intel para seu sistema operacional:

   - Windows Server 2008 R2

     1. Na pasta Downloads, localize o arquivo `PROWinx64Legacy.exe` e renomeie-o como `PROWinx64Legacy.zip`.
     2. Extraia o conteúdo do arquivo `PROWinx64Legacy.zip`.
     3. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute o comando a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 e Windows Server 2012

     1. Na pasta Downloads, extraia o conteúdo do arquivo `Wired_driver_`*`version`*`_x64.zip`.
     2. Na pasta com arquivos extraídos, localize o arquivo `Wired_driver_`*`version`*`_x64.exe` e renomeie-o como `Wired_driver_`*`version`*`_x64.zip`.
     3. Extraia o conteúdo do arquivo `Wired_driver_`*`version`*`_x64.zip`.
     4. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute os comandos a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.

        - Windows Server 2022

          ```
          C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxs.inf
          ```

        - Windows Server 2019

          ```
          C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
          ```

        - Windows Server 2016

          ```
          C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
          ```

        - Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

6. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
7. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo `ixgbevf` talvez seja incompatível com o kernel. Tente instalar a versão do módulo `ixgbevf` incluída com a distribuição do Linux para a instância.

Se você habilitar a rede avançada para uma instância de PV ou de AMI, poderá tornar a instância inatingível.

Para obter mais informações, consulte Como faço para ativar e configurar a rede aprimorada em minhas instâncias do EC2?

Monitorar a performance de rede de sua instância do EC2

O driver Elastic Network Adapter (ENA) publica métricas de performance de rede com base nas instâncias em que elas estão habilitadas. É possível usar essas métricas para solucionar problemas de performance da instância, escolher o tamanho certo da instância para uma workload, planejar atividades de dimensionamento proativamente e comparar aplicações para determinar se eles maximizam a performance disponível em uma instância.

O Amazon EC2 define os máximos de rede no nível da instância para garantir uma experiência de rede de alta qualidade, incluindo performance consistente da rede entre tamanhos de instância. A AWS fornece máximos para o seguinte em cada instância:

- Capacidade de largura de banda: cada instância do EC2 tem uma largura de banda máxima para tráfego agregado de entrada e saída, com base no tipo e no tamanho da instância. Algumas instâncias usam um mecanismo de crédito de E/S para alocar a largura de banda da rede com base na utilização média da largura de banda. O Amazon EC2 também tem largura de banda máxima para o tráfego da AWS Direct Connect e da Internet. Para ter mais informações, consulte Largura de banda de rede de instâncias do Amazon EC2.
- Performance de pacote por segundo (PPS): cada instância do EC2 tem uma performance máxima de PPS, com base no tipo e no tamanho da instância.
- Conexões rastreadas: o grupo de segurança rastreia cada conexão estabelecida para garantir que os pacotes de retorno sejam entregues como esperado. Há um número máximo de conexões que podem ser rastreadas por instância. Para obter mais informações, consulte Rastreamento de conexão do grupo de segurança
- Acesso ao serviço de link local: o Amazon EC2 fornece um PPS máximo por interface de rede para tráfego a serviços, como o serviço de DNS, o serviço de metadados da instância e o Amazon Time Sync Service.

Quando o tráfego de rede de uma instância excede um máximo, a AWS formata o tráfego que excede o máximo ao enfileirar e eliminar pacotes de rede. É possível monitorar quando o tráfego excede um máximo usando as métricas de performance de rede. Essas métricas informam sobre o impacto no tráfego da rede e possíveis problemas de performance da rede, em tempo real.

Conteúdo

- Requisitos
- Métricas para o driver ENA
- Exibir as métricas de performance de rede para sua instância do
- Métricas do ENA Express
- Métricas de performance de rede com o driver DPDK para ENA
- Métricas em instâncias que executam o FreeBSD

Requisitos

Instâncias do Linux

- Instale o driver ENA versão 2.2.10 ou posterior. Para verificar a versão instalada, use o comando ethtool. No exemplo a seguir, a versão atende ao requisito mínimo.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  Para atualizar seu driver ENA, consulte Redes avançadas.
- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte Coletar métricas de performance de rede no Guia do usuário do Amazon CloudWatch.
- Para oferecer suporte à métrica `conntrack_allowance_available`, instale a versão 2.8.1 do driver do ENA.

Instâncias do Windows

- Instalar o driver ENA versão 2.2.2 ou posterior. Para verificar a versão instalada, use o Gerenciador de dispositivos da seguinte forma.
  1. Abra o Gerenciador de dispositivos executando `devmgmt.msc`.
  2. Expanda Network Adapters (Adaptadores de rede).
  3. Escolha Amazon Elastic Network Adapter , Properties (Propriedades).
  4. Na guia Driver, localize Driver Version (Versão do driver).

  Para atualizar seu driver ENA, consulte Redes avançadas.

- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte Coletar métricas avançadas de rede no Guia do usuário do Amazon CloudWatch.

Métricas para o driver ENA

O driver ENA entrega as seguintes métricas para a instância em tempo real. Elas fornecem o número cumulativo de pacotes na fila ou descartados em cada interface de rede desde a última restauração do driver.

Métrica	Descrição	Com suporte para
`bw_in_allowance_exceeded`	Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.	Todos os tipos de instâncias
`bw_out_allowance_exceeded`	Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.	Todos os tipos de instâncias
`conntrack_allowance_exceeded`	Número de pacotes descartados porque o monitoramento da conexão excedeu o máximo para a instância e não foi possível estabelecer novas conexões. Isso pode resultar em perda de pacotes para tráfego indo para a instância ou vindo da instância	Todos os tipos de instâncias
`conntrack_allowance_available`	O número de conexões rastreadas que podem ser estabelecidas pela instância antes de atingir a cota de	Somente em instâncias criadas no AWS Nitro System

Métrica	Descrição	Com suporte para
	conexões rastreadas desse tipo de instância.	
`linklocal_allowance_exceeded`	Número de pacotes descartados porque o PPS do tráfego para os serviços de proxy local excedeu o máximo para a interface da rede. Isso afeta o tráfego para o serviço de DNS, o Instance Metadata Service e o Amazon Time Sync Service.	Todos os tipos de instâncias
`pps_allowance_exceeded`	Número de pacotes na fila ou descartados porque o PPS bidirecional excedeu o máximo para a instância.	Todos os tipos de instâncias

Exibir as métricas de performance de rede para sua instância do

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

É possível publicar métricas em suas ferramentas favoritas para visualizar os dados das métricas. Por exemplo, é possível publicar as métricas em Amazon CloudWatch usando o agente CloudWatch. O agente permite que você selecione métricas individuais e controle a publicação.

Também é possível usar o ethtool para recuperar as métricas para cada interface de rede, como eth0, conforme mostrado a seguir.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Instâncias do Windows

É possível visualizar as métricas usando qualquer consumidor de contadores de performance do Windows. Os dados podem ser analisados de acordo com o manifesto EnaperfCounters. Esse é um arquivo XML que define o provedor do contador de performance e seus countersets.

Para instalar o manifesto

Se você executou a instância usando uma AMI que contém o driver ENA 2.2.2 ou posterior ou usou o script de instalação no pacote de driver para o driver ENA 2.2.2, o manifesto já está instalado. Para instalar o manifesto manualmente, use as seguintes etapas:

1. Remova o manifesto existente usando o seguinte comando:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copie o arquivo manifesto `EnaPerfCounters.man` do pacote de instalação do driver para `%SystemRoot%\System32\drivers`.
3. Instale o novo manifesto usando o seguinte comando:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Para visualizar métricas usando o monitor de desempenho

1. Abra o Monitor de performance.
2. Pressione Ctrl+N para adicionar novos contadores.
3. Escolha ENA Packets Shaping (Modelagem de pacotes de ENA na lista.
4. Selecione as instâncias a serem monitoradas e escolha Add (Adicionar).
5. Escolha OK.

Métricas do ENA Express

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). SRD é um protocolo de transporte de rede de alta performance que usa roteamento dinâmico para aumentar o throughput e minimizar a latência final. Você pode usar as métricas do ENA Express para ajudar a garantir que suas instâncias aproveitem ao máximo as melhorias de performance que a tecnologia SRD oferece, por exemplo:

- Avalie os recursos para garantir que tenham capacidade suficiente para estabelecer mais conexões por SRD.
- Identifique onde existem potenciais problemas que impedem que pacotes de saída elegíveis usem o SRD.
- Calcule a porcentagem de tráfego de saída que usa SRD para a instância.
- Calcule a porcentagem de tráfego de entrada que usa SRD para a instância.

> **Note**
>
> Para produzir métricas, use a versão 2.8 ou superior do driver.

As seguintes métricas do ENA Express estão disponíveis por meio do comando ethtool para instâncias baseadas no Linux.

- `ena_srd_mode`: descreve quais recursos do ENA Express estão habilitados. Os valores são os seguintes:
  - `0` = ENA Express desativado, UDP desativado
  - `1` = ENA Express ativado, UDP desativado
  - `2` = ENA Express desativado, UDP ativado

    > **Note**
    >
    > Isso só acontece quando o ENA Express foi originalmente habilitado e o UDP foi configurado para usá-lo. O valor anterior é retido para tráfego UDP.

  - `3` = ENA Express ativado, UDP ativado
- `ena_srd_eligible_tx_pkts`: o número de pacotes de rede enviados em um determinado período que atendem aos requisitos de elegibilidade do SRD, como se segue:
  - Os tipos de instâncias de envio e de recebimento são compatíveis. Para obter mais informações, consulte a tabela Tipos de instâncias compatíveis com o ENA Express.
  - As instâncias de envio e de recebimento devem ter o ENA Express configurado.
  - As instâncias de envio e recebimento devem ser executadas na mesma zona de disponibilidade.
  - O caminho da rede entre as instâncias não deve incluir caixas de middleware. No momento, o ENA Express não é compatível com caixas de middleware.

> **Note**
>
> A métrica de elegibilidade do ENA Express abrange os requisitos de origem e destino e a rede entre os dois endpoints. Pacotes elegíveis ainda podem ser desqualificados depois de já terem sido contados. Por exemplo, se um pacote elegível estiver acima do limite da unidade de transmissão máxima (MTU), ele retornará para a transmissão ENA padrão, embora o pacote ainda apareça como elegível no contador.

- `ena_srd_tx_pkts`: o número de pacotes de SRD transmitidos em um determinado período.
- `ena_srd_rx_pkts`: o número de pacotes de SRD recebidos em um determinado período.
- `ena_srd_resource_utilization`: a porcentagem da utilização da memória máxima permitida para conexões por SRD simultâneas que a instância consumiu.

Para ver uma lista de métricas filtradas para o ENA Express, execute o seguinte comando ethtool para a interface de rede (mostrado aqui como `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

Tráfego de saída (pacotes de saída)

Para garantir que o tráfego de saída use SRD conforme esperado, compare o número de pacotes elegíveis para SRD (`ena_srd_eligible_tx_pkts`) com o número de pacotes SRD enviados (`ena_srd_tx_pkts`) em um determinado período.

Diferenças significativas entre o número de pacotes elegíveis e o número de pacotes SRD enviados geralmente são causadas por problemas de utilização de recursos. Quando a placa de rede anexada à instância esgota seus recursos máximos ou seus pacotes estão acima do limite de MTU, os pacotes elegíveis não podem ser transmitidos por SRD e devem retornar à transmissão ENA padrão. Os pacotes também podem apresentar essa diferença durante as migrações em tempo real ou as atualizações de servidores em tempo real. É necessária uma avaliação adicional para determinar a causa raiz.

> **Note**
>
> Você pode ignorar pequenas diferenças ocasionais entre o número de pacotes elegíveis e o número de pacotes SRD. Isso pode acontecer quando a instância estabelece uma conexão com outra instância para tráfego SRD, por exemplo.

Para descobrir qual porcentagem do tráfego total de saída em um determinado período usa SRD, compare o número de pacotes SRD enviados (`ena_srd_tx_pkts`) com o número total de pacotes enviados para a instância (`NetworkPacketOut`) durante esse período.

Tráfego de entrada (pacotes recebidos)

Para descobrir qual porcentagem do tráfego de entrada usa SRD, compare o número de pacotes SRD recebidos (`ena_srd_rx_pkts`) em um determinado período com o número total de pacotes recebidos para a instância (`NetworkPacketIn`) durante esse período.

Utilização de recursos

A utilização de recursos é baseada no número de conexões SRD simultâneas que uma única instância pode manter em um determinado momento. A métrica de utilização de recursos (`ena_srd_resource_utilization`) monitora a utilização atual da instância. À medida que a utilização se aproxima de 100%, você pode esperar problemas de performance. O ENA Express deixa de usar SRD e volta à transmissão ENA padrão, e a possibilidade de pacotes descartados aumenta. A alta utilização de recursos é um sinal de que está na hora de aumentar a escala da instância horizontalmente para melhorar a performance da rede.

> **Note**
>
> Quando o tráfego de rede de uma instância excede um máximo, a AWS formata o tráfego que excede o máximo ao enfileirar e eliminar pacotes de rede.

Persistência

As métricas de saída e entrada são cumulativas enquanto o ENA Express está habilitado para a instância. As métricas deixarão de ser acumulativas se o ENA Express for desativado, mas persistirão enquanto a instância ainda estiver em execução. As métricas serão redefinidas se a instância for reinicializada ou encerrada ou se a interface de rede for desconectada da instância.

Métricas de performance de rede com o driver DPDK para ENA

O driver ENA versão 2.2.0 e posterior oferece suporte a relatórios de métricas de rede. O DPDK 20.11 inclui o driver ENA 2.2.0 e é a primeira versão do DPDK a suportar esse recurso.

É possível usar uma aplicação de exemplo para visualizar estatísticas DPDK. Para iniciar uma versão interativa da aplicação de exemplo, execute o seguinte comando.

```
./app/dpdk-testpmd -- -i
```

Dentro desta sessão interativa, é possível inserir um comando para recuperar dados estatísticos estendidos para uma porta. O comando de exemplo a seguir recupera as estatísticas da porta 0.

```
show port xstats 0
```

Veja a seguir um exemplo de uma sessão interativa com a aplicação de exemplo DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
```

```
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Para obter mais informações sobre a aplicação de exemplo e usá-lo para recuperar dados estatísticos estendidos, consulte Guia do usuário da aplicação Testpmd na documentação do DPDK.

Métricas em instâncias que executam o FreeBSD

A partir da versão 2.3.0, o driver ENA FreeBSD suporta a coleta de métricas de performance de rede em instâncias que executam o FreeBSD. Para habilitar a coleção de métricas do FreeBSD, insira o seguinte comando e defina o *intervalo* como um valor entre 1 e 3.600. Isso especifica com que frequência, em segundos, serão coletadas métricas do FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Por exemplo, o comando a seguir define o driver para coletar métricas do FreeBSD na interface de rede 1 a cada 10 segundos:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Para desativar a coleta de métricas do FreeBSD, é possível executar o comando anterior e especificar `0` como o *interval* (intervalo).

Depois de habilitar a coleta de métricas do FreeBSD, é possível recuperar o conjunto mais recente de métricas coletadas ao executar o comando apresentado a seguir.

```
sysctl dev.ena.network_interface.eni_metrics
```

Solução de problemas do Adaptador de Rede Elástica no Linux

O Elastic Network Adapter (ENA) é projetado para melhorar a integridade do sistema operacional e reduzir as possibilidades de interrupção de longo prazo por conta de comportamento inesperado de hardware e/ou falhas. A arquitetura do ENA mantém falhas do dispositivo ou do driver o mais transparentes possível para o sistema. Este tópico fornece informações de solução de problemas para o ENA.

Caso você não consiga se conectar à sua instância, comece com a seção Solucionar problemas de conectividade.

Se você experimentar degradação de performance após migrar para um tipo de instância de sexta geração, consulte o artigo What do I need to do before I migrate my EC2 instance to a sixth generation instance to make sure that I get maximum network performance?

Se você for capaz de se conectar à sua instância, pode coletar informações de diagnóstico usando os mecanismos de detecção e recuperação de falhas, cobertos nas seções posteriores deste tópico.

Tópicos

- Solucionar problemas de conectividade
- Mecanismo de keep-alive
- Registre o tempo limite de leitura
- Statistics
- Logs de erro do driver no syslog
- Notificações de configuração abaixo do ideal

Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo `ena` talvez seja incompatível com o kernel atualmente em execução na sua instância. Isso pode acontecer se você instalar o módulo para uma versão específica do kernel (sem dkms ou com um arquivo dkms.conf configurado indevidamente) e o kernel da instância for atualizado. Se o kernel da instância que estiver carregado no momento da inicialização não tiver o módulo `ena` corretamente instalado, sua instância não reconhecerá o adaptador de rede e sua instância ficará inacessível.

Se você habilitar a rede avançada para uma instância de PV ou AMI, isso também poderá tornar a instância inatingível.

.Se sua instância tornar-se inacessível após habilitar a rede avançada com ENA, é possível desabilitar o atributo `enaSupport` para sua instância e cairá no adaptador de rede em estoque.

Para desabilitar a rede avançada com ENA (instâncias com suporte do EBS)

1. No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.

> **Important**
>
> Se estiver usando uma instância com armazenamento de instâncias, você não poderá parar a instância. Em vez disso, prossiga para Para desabilitar a rede avançada com o ENA (instâncias com suporte do armazenamento de instâncias).

2. No computador local, desative o atributo de rede avançada usando um o comando a seguir.

   - modify-instance-attribute (AWS CLI)

   ```
   $ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
   ```

3. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, é necessário iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
4. (Opcional) Conecte-se à sua instância e tente reinstalar o módulo `ena` com a versão atual do kernel seguindo as etapas em Habilitação de redes aperfeiçoadas com o Adaptador de Rede Elástica (ENA) nas instâncias do EC2.

Para desabilitar a rede avançada com o ENA (instâncias com suporte do armazenamento de instâncias)

Se sua instância for com armazenamento de instâncias, crie uma nova AMI como descrito em Criar uma AMI em Linux com armazenamento de instâncias. Desabilite o atributo de rede avançada `enaSupport` ao registrar a AMI.

- register-image (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Mecanismo de keep-alive

O dispositivo ENA posta eventos de keep-alive em uma taxa fixa (geralmente uma vez por segundo). O driver ENA implanta um mecanismo de watchdog, que verifica a presença dessas mensagens keep-alive. Se as mensagens estiverem presentes, o watchdog será rearmado; caso contrário, o driver concluirá que o dispositivo experimentou uma falha e fará o seguinte:

- Despejará as estatísticas atuais no syslog
- Redefinirá o dispositivo ENA
- Redefinirá o estado do driver do ENA

O procedimento de redefinição acima pode resultar em alguma perda de tráfego por um breve período (conexões TCP devem ser capazes recuperar), mas não deve afetar o usuário de outras formas.

O dispositivo ENA também pode indiretamente solicitar um procedimento de redefinição do dispositivo ao não enviar uma notificação de keep-alive, por exemplo, se o dispositivo ENA atingir um estado desconhecido depois de carregar uma configuração irrecuperável.

Exemplo do procedimento de redefinição:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
```

```
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Registre o tempo limite de leitura

A arquitetura de ENA sugere um uso específico limitado de operações de leitura de E/S (MMIO) mapeadas de memória. Os registros de MMIO são acessados pelo driver do dispositivo ENA somente durante o procedimento de inicialização.

Se os logs do driver (disponíveis na saída do dmesg) indicarem falhas nas operações de leitura, isso pode ser causado por um driver incompatível ou incorretamente compilado, um dispositivo de hardware ocupado ou falha de hardware.

As entradas intermitentes do log que indicam falhas nas operações de leitura não devem ser consideradas um problema; o driver fará novas tentativas nesse caso. Contudo, uma sequência de entradas de log contendo falhas de leitura indica problema de driver ou de hardware.

Abaixo está um exemplo de entrada de log do driver indicando falha na operação de leitura devido a um tempo limite:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistics

Se você tiver problemas de latência ou de performance de rede insuficiente, recupere as estatísticas dos dispositivos e examine-as. Essas estatísticas podem ser obtidas usando ethtool, como mostrado abaixo:

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Os parâmetros de saída de comando a seguir estão descritos abaixo:

`tx_timeout`: *N*

O número de vezes que o watchdog Netdev foi ativado.

`suspend`: *N*

O número de vezes que o driver realizou uma operação de suspensão.

`resume`: *N*

O número de vezes que o driver realizou uma operação de retomada.

`wd_expired`: *N*

O número de vezes que o driver não recebeu o evento de keep-alive nos três segundos anteriores.

`interface_up`: *N*

O número de vezes que a interface do ENA foi ativada.

`interface_down`: *N*

O número de vezes que a interface do ENA foi desativada.

`admin_q_pause`: *N*

O número de vezes que a fila do administrador não foi encontrada em um estado de execução.

`bw_in_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.

`bw_out_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.

`pps_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque o PPS bidirecional excedeu o máximo para a instância.

`conntrack_allowance_available`: *N*

O número de conexões rastreadas que podem ser estabelecidas pela instância antes de atingir a cota de conexões rastreadas desse tipo de instância. Disponível somente para instâncias baseadas em Nitro. Não é compatível com instâncias do FreeBSD ou ambientes DPDK.

`conntrack_allowance_exceeded`: *N*

Número de pacotes descartados porque o monitoramento da conexão excedeu o máximo para a instância e não foi possível estabelecer novas conexões. Isso pode resultar em perda de pacotes para tráfego indo para a instância ou vindo da instância

`linklocal_allowance_exceeded`: *N*

Número de pacotes descartados porque o PPS do tráfego para os serviços de proxy local excedeu o máximo para a interface da rede. Isso afeta o tráfego para o serviço de DNS, o Instance Metadata Service e o Amazon Time Sync Service.

`queue_`*N*`_tx_cnt`: *N*

O número de pacotes transmitidos para essa fila.

`queue_N_tx_bytes`: *N*

O número de bytes transmitidos para essa fila.

`queue_N_tx_queue_stop`: *N*

O número de vezes em que a fila *N* estava cheia e interrompida.

`queue_N_tx_queue_wakeup`: *N*

O número de vezes que a fila *N* foi retomada depois de ser interrompida.

`queue_N_tx_dma_mapping_err`: *N*

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_tx_linearize`: *N*

O número de vezes que a linearização de SKB foi tentada para essa fila.

`queue_N_tx_linearize_failed`: *N*

O número de vezes que a linearização de SKB apresentou falha para essa fila.

`queue_N_tx_napi_comp`: *N*

O número de vezes que o manipulador `napi` chamou `napi_complete` para essa fila.

`queue_N_tx_tx_poll`: *N*

O número de vezes que o manipulador `napi` foi programado para essa fila.

`queue_N_tx_doorbells`: *N*

O número de campainhas de transmissão para essa fila.

`queue_N_tx_prepare_ctx_err`: *N*

O número de vezes que `ena_com_prepare_tx` apresentou falha para essa fila.

`queue_N_tx_bad_req_id`: *N*

`req_id` inválido para essa fila. O `req_id` válido é zero, menos `queue_size`, menos 1.

`queue_N_tx_llq_buffer_copy`: *N*

O número de pacotes cujo tamanho dos cabeçalhos é maior do que a entrada llq para essa fila.

`queue_N_tx_missed_tx`: *N*

O número de pacotes deixados sem conclusão para essa fila.

`queue_N_tx_unmask_interrupt`: *N*

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`queue_N_rx_cnt`: *N*

O número de pacotes recebidos para essa fila.

`queue_N_rx_bytes`: *N*

O número de bytes recebidos para essa fila.

`queue_N_rx_rx_copybreak_pkt`: *N*

O número de vezes que a fila rx recebeu um pacote menor que o tamanho do pacote de rx_copybreak para essa fila.

`queue_N_rx_csum_good`: *N*

O número de vezes que a fila rx recebeu um pacote em que a soma de verificação foi verificada e estava correta para essa fila.

`queue_N_rx_refil_partial`: *N*

O número de vezes que o driver não teve sucesso ao reabastecer a parte vazia da fila rx com buffers para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_bad_csum`: *N*

O número de vezes que a fila `rx` teve uma soma de verificação errada para a fila (somente se o descarregamento da soma de verificação for compatível).

`queue_N_rx_page_alloc_fail`: *N*

O número de vezes que a alocação de página apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_skb_alloc_fail`: *N*

O número de vezes que a alocação de SKB apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de sistema baixos.

`queue_N_rx_dma_mapping_err`: *N*

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_rx_bad_desc_num`: *N*

Excesso de buffers por pacote. Se o valor não for 0, isso indica o uso de buffers muito pequenos.

`queue_N_rx_bad_req_id`: *N*

O req_id para essa fila não é válido. O req_id válido é de [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

O número de vezes que a fila rx estava vazia para essa fila.

`queue_N_rx_csum_unchecked`: *N*

O número de vezes que a fila rx recebeu um pacote cuja soma de verificação não foi verificada para essa fila.

`queue_N_rx_xdp_aborted`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_ABORT.

`queue_N_rx_xdp_drop`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_DROP.

`queue_N_rx_xdp_pass`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_PASS.

`queue_N_rx_xdp_tx`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_TX.

`queue_N_rx_xdp_invalid`: *N*

O número de vezes que o código de retorno XDP para o pacote não foi válido.

`queue_N_rx_xdp_redirect`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_REDIRECT.

`queue_N_xdp_tx_cnt`: *N*

O número de pacotes transmitidos para essa fila.

`queue_N_xdp_tx_bytes`: *N*

O número de bytes transmitidos para essa fila.

`queue_N_xdp_tx_queue_stop`: *N*

O número de vezes que essa fila estava cheia e interrompida.

`queue_N_xdp_tx_queue_wakeup`: *N*

O número de vezes que essa fila foi retomada depois de ser interrompida.

`queue_N_xdp_tx_dma_mapping_err`: *N*

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_xdp_tx_linearize`: *N*

O número de vezes que a linearização de buffer XDP foi tentada para essa fila.

`queue_N_xdp_tx_linearize_failed`: *N*

O número de vezes que a linearização do buffer XDP apresentou falha para essa fila.

`queue_N_xdp_tx_napi_comp`: *N*

O número de vezes que o manipulador napi chamou napi_complete para essa fila.

`queue_N_xdp_tx_tx_poll`: *N*

O número de vezes que o manipulador napi foi programado para essa fila.

`queue_N_xdp_tx_doorbells`: *N*

O número de campainhas de transmissão para essa fila.

`queue_N_xdp_tx_prepare_ctx_err`: *N*

O número de vezes que ena_com_prepare_tx apresentou falha para essa fila. Esse valor sempre deve ser zero; caso contrário, consulte os logs do driver.

`queue_N_xdp_tx_bad_req_id`: *N*

O req_id para essa fila não é válido. O req_id válido é de [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy`: *N*

O número de pacotes que tiveram seus cabeçalhos copiados usando a cópia do buffer llq para essa fila.

`queue_N_xdp_tx_missed_tx`: *N*

O número de vezes que uma entrada de fila tx perdeu um timeout de conclusão para essa fila.

`queue_N_xdp_tx_unmask_interrupt`: *N*

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`ena_admin_q_aborted_cmd`: *N*

O número de comandos de administrador que foram abortados. Isso normalmente acontece durante o procedimento de autorrecuperação.

`ena_admin_q_submitted_cmd`: *N*

O número de campainhas da fila do administrador.

`ena_admin_q_completed_cmd`: *N*

O número de conclusões da fila do administrador.

`ena_admin_q_out_of_space`: *N*

O número de vezes que o driver tentou enviar o novo comando de administrador, mas a fila estava cheia.

`ena_admin_q_no_completion`: *N*

O número de vezes o driver não obteve a conclusão de um administrador para um comando.

Logs de erro do driver no syslog

O driver do ENA grava mensagens de log para syslog durante a inicialização do sistema. É possível examinar esses logs para procurar erros se estiver enfrentando problemas. Abaixo está um exemplo de informações registradas pelo driver do ENA no syslog durante a inicialização do sistema, junto com alguns anotações para mensagens selecionadas.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Quais erros posso ignorar?

Os avisos a seguir que podem aparecer nos logs de erros do seu sistema podem ser ignorados para o Elastic Network Adapter:

Não há suporte para definição do atributo do host

> Este dispositivo não oferece suporte aos atributos do host.

falha em alocar buffer para a fila rx

> Esse é um erro recuperável e indica que pode ter havido um problema de pressão de memória quando o erro ocorreu.

Não há suporte para o recurso *X*

> O recurso mencionado não é compatível com o Elastic Network Adapter. Os valores possíveis para *X* incluem:
>
> - **10**: a configuração da função RSS Hash não é compatível para este dispositivo.
> - **12**: a tabela RSS Indirection não é compatível para este dispositivo.
> - **18**: a configuração de RSS Hash Input não é compatível para este dispositivo.

- **20**: a moderação de interrupção não é compatível para este dispositivo.
- **27**: o driver Elastic Network Adapter não oferece suporte à sondagem dos recursos de Ethernet de snmpd.

Falha ao configurar AENQ

O Elastic Network Adapter não oferece suporte à configuração de AENQ.

Tentativa de configurar eventos AENQ não compatíveis

Esse erro indica uma tentativa de configurar um grupo de eventos do AENQ que não são compatíveis com o Elastic Network Adapter.

Notificações de configuração abaixo do ideal

O dispositivo ENA detecta configurações abaixo do ideal no driver, as quais podem ser alteradas. O dispositivo notifica o driver ENA e registra um aviso no console. O exemplo a seguir mostra o formato da mensagem de aviso.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

A lista a seguir mostra detalhes do código de notificação e as ações recomendadas para descobertas de configurações abaixo do ideal.

- Código **1**: não é recomendado utilizar o ENA Express com configuração de LLQ amplo

  A ENI do ENA Express está configurada com LLQ amplo. Essa configuração está abaixo do ideal e pode afetar a performance do ENA Express. Recomendamos desabilitar as configurações de LLQ amplo ao usar ENIs do ENA Express conforme mostrado a seguir.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Para obter mais informações sobre a configuração ideal do ENA Express consulte Aprimoramento do desempenho da rede com o ENA Express nas instâncias do EC2.
- Código **2**: ENI do ENA Express com profundidade de fila Tx abaixo do ideal não é recomendada

  A ENI do ENA Express está configurada com profundidade de fila Tx abaixo do ideal. Essa configuração pode afetar a performance do ENA Express. Recomendamos aumentar todas as filas

Tx para o valor máximo para a interface de rede quando você usar ENIs do ENA Express como a seguir.

É possível pode executar os seguintes comandos ethtool para ajustar o tamanho do LLQ
Para saber mais sobre como controlar, consultar e habilitar o LLQ amplo, consulte o tópico Enfileiramento de baixa latência grande (Large LLQ) da documentação do driver do kernel Linux para ENA no Repositório de drivers da Amazon no GitHub.

```
ethtool -g interface
```

Defina suas filas Tx para a profundidade máxima:

```
ethtool -G interface tx depth
```

Para obter mais informações sobre a configuração ideal do ENA Express consulte Aprimoramento do desempenho da rede com o ENA Express nas instâncias do EC2.

- Código**3**: ENA com tamanho de LLQ normal e tráfego de pacotes Tx excede o tamanho máximo aceito pelo cabeçalho

  Por padrão, o LLQ do ENA oferece suporte a cabeçalhos de pacote Tx com até 96 bytes de tamanho. Se o tamanho do cabeçalho do pacote for maior que 96 bytes, o pacote será descartado. Para mitigar esse problema, recomendamos habilitar o LLQ amplo, o que aumenta o tamanho máximo do cabeçalho do pacote Tx para 224 bytes.

  No entanto, quando você ativa o LLQ amplo, o tamanho máximo do anel Tx é reduzido de 1000 para 512 entradas. O LLQ amplo é habilitado por padrão para todos os tipos de instância Nitro v4 e posteriores.

  - Os tipos de instância Nitro v4 têm um tamanho de anel Tx de LLQ amplo máximo padrão de 512 entradas, que não pode ser alterado.
  - Os tipos de instância Nitro v5 têm um tamanho de anel Tx de LLQ amplo padrão de 512 entradas, o qual pode ser alterado para até 1000 entradas.

  É possível pode executar os seguintes comandos ethtool para ajustar o tamanho do LLQ
  Para saber mais sobre como controlar, consultar e habilitar o LLQ amplo, consulte o tópico Enfileiramento de baixa latência grande (Large LLQ) da documentação do driver do kernel Linux para ENA no Repositório de drivers da Amazon no GitHub.

  Encontre a profundidade máxima para suas filas Tx:

```
ethtool -g interface
```

Defina suas filas Tx para a profundidade máxima:

```
ethtool -G interface tx depth
```

Solução de problemas do driver do Adaptador de Rede Elástica do Windows

O Elastic Network Adapter (ENA) é projetado para melhorar a integridade do sistema operacional e reduzir as possibilidades de interrupção na operação da sua instância de Windows por conta de comportamento inesperado de hardware ou falhas. A arquitetura do ENA mantém falhas do dispositivo ou do driver o mais transparentes possível para o sistema operacional.

Instalação do driver do Adaptador de Rede Elástica (ENA)

Se sua instância não for baseada em uma das mais recentes imagens de máquina da Amazon (AMIs) do Windows que a Amazon fornece, use o procedimento a seguir para instalar o driver ENA atual em sua instância. Execute esta atualização em um momento conveniente para reinicializar sua instância. Se o script de instalação não reinicializar automaticamente sua instância, recomendamos que você reinicie a instância como etapa final.

Se você usar um volume de armazenamento de instância para armazenar dados enquanto a instância estiver em execução, esses dados serão apagados quando você interromper a instância. Antes de interromper sua instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instância para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

Pré-requisitos

Para instalar ou atualizar o driver ENA, sua instância do Windows deve atender aos seguintes pré-requisitos:

- O PowerShell versão 3.0 ou posterior deve ser instalado

Etapa 1: fazer backup de seus dados

Recomendamos que você crie uma AMI de backup caso não consiga reverter suas alterações por meio do Gerenciador de dispositivos. Para criar uma AMI de backup com o AWS Management Console, siga estas etapas:

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer a atualização do driver e escolha Interromper instância no menu Estado da instância.
4. Depois de interromper a instância, selecione a instância novamente. Para criar seu backup, escolha Imagem e modelos no menu Ações e escolha Criar imagem.
5. Para reiniciar sua instância, escolha Iniciar instância no menu Estado da instância.

Etapa 2: instalar ou atualizar seu driver ENA

Você pode instalar ou atualizar seu driver ENA com o AWS Systems Manager Distributor ou com os cmdlets do PowerShell. Para obter mais instruções, selecione a guia que corresponde ao método que deseja utilizar.

Systems Manager Distributor

Você pode usar o recurso do Systems Manager Distributor para implantar pacotes nos nós gerenciados do Systems Manager. Com o Systems Manager Distributor, você pode instalar o pacote de driver ENA uma vez ou com atualizações programadas. Para obter mais informações sobre como instalar o pacote de driver ENA (`AwsEnaNetworkDriver`) com o Systems Manager Distributor, consulte Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager.

PowerShell

Esta seção aborda como fazer o download e instalar pacotes de drivers ENA em sua instância com cmdlets do PowerShell.

Opção 1: fazer o download e extrair a versão mais recente

1. Conecte-se à instância e faça login como administrador local.
2. Use o cmdlet invoke-webrequest para fazer o download do pacote de driver mais recente:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```
>
> Como alternativa, você pode fazer o download do pacote de driver mais recente em uma janela do navegador em sua instância.

3. Use o cmdlet expand-archive para extrair o arquivo zip que você baixou para sua instância:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opção 2: fazer o download e extrair uma versão específica

1. Conecte-se à instância e faça login como administrador local.
2. Faça o download do pacote do driver ENA para a versão específica desejada no link da versão na tabela Driver do ENA para o Windows.
3. Extraia o arquivo zip para sua instância.

Instalar o driver ENA com o PowerShell

As etapas de instalação são as mesmas, independentemente de você ter feito o download do driver mais recente ou de uma versão específica. Para instalar o driver ENA, siga estas etapas:

1. Instale o driver, execute o script `install.ps1` do PowerShell do diretório do `AwsEnaNetworkDriver` em sua instância. Se você receber um erro, verifique se está usando o PowerShell 3.0 ou posterior.
2. Se o instalador não reinicializar automaticamente sua instância, execute o cmdlet Restart-Computer do PowerShell.

```
PS C:\> Restart-Computer
```

Etapa 3 (opcional): verificar a versão do driver ENA após a instalação

Para garantir que o pacote do driver ENA tenha sido instalado com êxito em sua instância, você pode verificar a nova versão da seguinte forma:

1. Conecte-se à instância e faça login como administrador local.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.

> **Note**
>
> Todos os adaptadores ENA usam o mesmo driver. Caso tenha vários adaptadores ENA, você poderá selecionar qualquer um deles para atualizar o driver de todos os adaptadores ENA.

6. Para verificar a versão atual instalada, abra a guia Driver e verifique a Versão do driver. Se a versão atual não corresponder à sua versão de destino, consulte Solução de problemas do driver do Adaptador de Rede Elástica do Windows.

Reverter a instalação de um driver ENA

Se algo der errado com a instalação, talvez seja necessário reverter o driver. Siga estas etapas para reverter para a versão anterior do driver ENA que estava instalada em sua instância.

1. Conecte-se à instância e faça login como administrador local.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.

> **Note**
>
> Todos os adaptadores ENA usam o mesmo driver. Caso tenha vários adaptadores ENA, você poderá selecionar qualquer um deles para atualizar o driver de todos os adaptadores ENA.

6. Para reverter o driver, abra a guia Driver e escolha Reverter driver. Isso abre a janela de Reversão do pacote de driver.

> **Note**
>
> Se a guia Driver não mostrar a ação Reverter driver ou se a ação não estiver disponível, isso significa que o armazenamento de drivers em sua instância não contém o pacote de driver instalado anteriormente. Para solucionar esse problema, consulte Cenários de solução de problemas e expanda a seção Versão inesperada do driver ENA instalada. Para obter mais informações sobre o processo de seleção do pacote de driver de dispositivo, consulte Como o Windows seleciona um pacote de driver para um dispositivo no site de documentação da Microsoft.

Colete informações de diagnóstico sobre a instância

As etapas para abrir as ferramentas do sistema operacional (SO) Windows variam, dependendo da versão do sistema operacional instalada na instância. Nas seções a seguir, usamos a caixa de diálogo Run (Executar) para abrir as ferramentas, o que funciona da mesma forma em todas as versões do sistema operacional. No entanto, é possível acessar essas ferramentas usando qualquer método que preferir.

Acesse a caixa de diálogo Run (Executar)

- Usando a combinação de teclas do logo do Windows: `Windows` + `R`
- Usando a barra de pesquisa:
  - Insira `run` na barra de pesquisa.
  - Selecione a aplicação Run (Executar) a partir dos resultados da pesquisa.

Algumas etapas exigem que o menu de contexto acesse propriedades ou ações sensíveis ao contexto. Há várias maneiras de fazer isso, dependendo da versão do sistema operacional e do hardware.

Acesse o menu de contexto

- Usando o mouse: clique com o botão direito do mouse em um item para abrir seu menu de contexto.
- Usando o teclado:
  - Dependendo da versão do sistema operacional, use `Shift` + `F10`, ou `Ctrl` + `Shift` + `F10`.
  - Se você tiver a tecla de contexto no teclado (três linhas horizontais em uma caixa), selecione o item desejado e pressione a tecla de contexto.

Se você puder se conectar à instância, use as técnicas a seguir para coletar informações de diagnóstico para solução de problemas.

Verifique o status do dispositivo ENA

Para verificar o status do driver ENAdo Windows usando o Gerenciador de dispositivos do Windows, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.

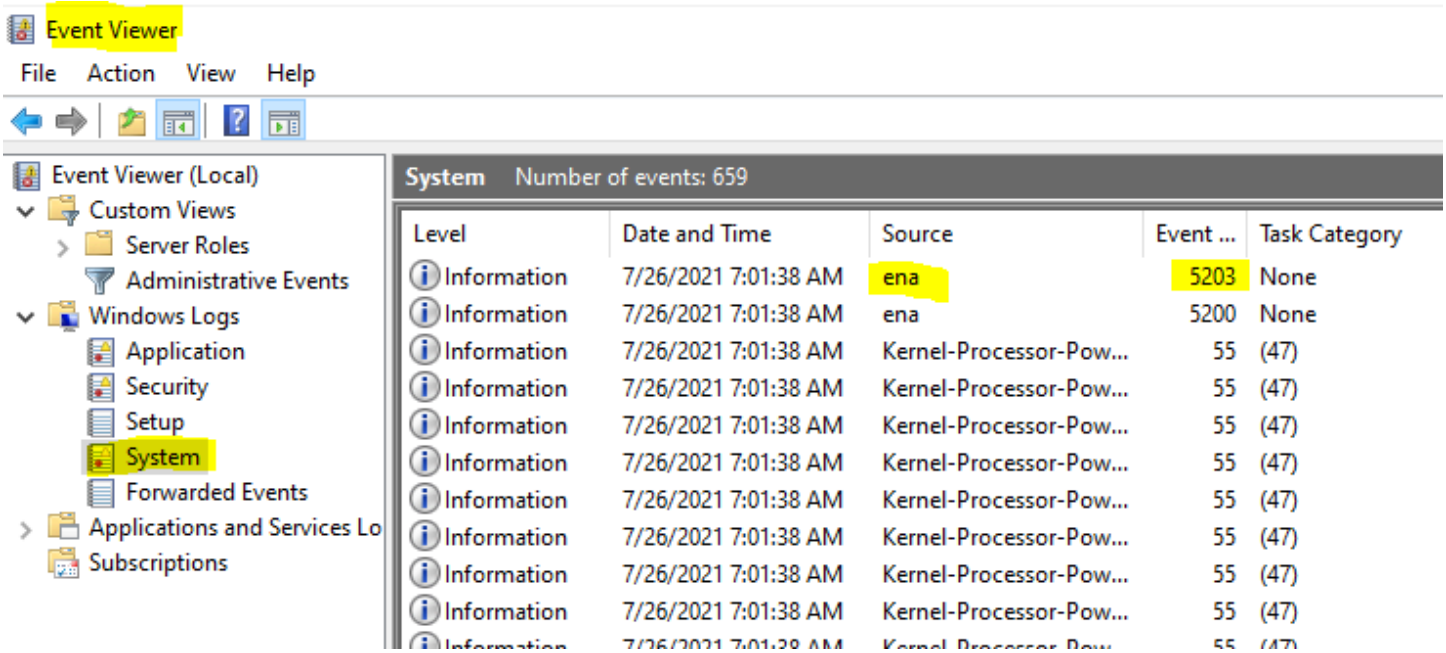
6. Verifique se a mensagem na guia Geral sinaliza "Este dispositivo está funcionando corretamente".

Investigue mensagens de evento do driver

Para revisar os logs de eventos do driver ENA do Windows usando o Visualizador de eventos do Windows, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Visualizador de eventos do Windows, insira `eventvwr.msc` na caixa Run (Executar).
3. Escolha OK. Isso abrirá a janela Event Viewer (Visualizador de eventos).
4. Expanda o menu Windows Logs (Logs do Windows) e, em seguida, escolha System (Sistema).
5. Em Actions (Ações), no painel superior direito, escolha Filter Current Log (Filtrar log atual). Isso exibe a caixa de diálogo de filtragem.
6. Na caixa Event sources (Origens de eventos), insira `ena`. Isso limita os resultados a eventos gerados pelo driver ENA do Windows.
7. Escolha OK. Isso mostra os resultados do log de eventos filtrados nas seções de detalhes da janela.
8. Para examinar os detalhes, selecione uma mensagem de evento na lista.

O exemplo a seguir mostra um evento de driver ENA na lista de eventos do sistema do Visualizador de eventos do Windows:



Resumo da mensagem do evento

A tabela a seguir mostra as mensagens de evento geradas pelo driver ENA do Windows.

Entrada

ID do evento	Descrição do evento do driver ENA	Tipo
5001	Hardware is out of resources (O hardware está sem recursos)	Erro
5002	Adapter has detected a hardware error (O adaptador detectou um erro de hardware)	Erro
5005	Adapter has timed out on NDIS operation that did not complete in a timely manner (O adaptador expirou o tempo limite na operação do NDIS	Erro

ID do evento	Descrição do evento do driver ENA	Tipo
	que não foi concluída em tempo hábil)	
5032	Adapter has failed to reset the device (Falha do adaptador ao redefinir o dispositivo)	Erro
5200	Adapter has been initialized (O adaptador foi inicializado)	Informativo
5201	Adapter has been halted (O adaptador foi interrompido)	Informativo
5202	Adapter has been paused (O adaptador foi pausado)	Informativo
5203	Adapter has been restarted (O adaptador foi reiniciado)	Informativo
5204	Adapter has been shut down (O adaptador foi desligado)	Informativo
5205	Adapter has been reset (O adaptador foi redefinido)	Erro
5206	Adapter has been surprise removed (O adaptador foi removido de surpresa)	Erro
5208	Adapter initialization routine has failed (A rotina de inicializ ação do adaptador falhou)	Erro

ID do evento	Descrição do evento do driver ENA	Tipo
5210	Adapter has encountered and successfully recovered an internal issue (O adaptador encontrou problema interno e recuperou com êxito)	Erro

Analise as métricas de performance

O driver ENA do Windows publica métricas de performance de rede de instâncias onde elas estão habilitadas. Você pode exibir e habilitar métricas na instância usando a aplicação nativa Monitor de performance. Para obter mais informações sobre as métricas que o driver ENA do Windows produz, consulte Monitorar a performance de rede de sua instância do EC2.

Em casos em que as métricas do ENA estão habilitadas e o agente do Amazon CloudWatch está instalado, o CloudWatch coleta as métricas associadas aos contadores no Monitor de performance do Windows, bem como algumas métricas avançadas para o ENA. Essas métricas são coletadas além das métricas habilitadas por padrão em instâncias do EC2. Para obter mais informações sobre as métricas, consulte Métricas coletadas pelo agente CloudWatch no Guia do usuário do Amazon CloudWatch.

> **Note**
>
> As métricas de performance estão disponíveis para as versões 2.4.0 e posteriores do driver ENA (também para a versão 2.2.3). O driver ENA versão 2.2.4 foi revertido devido à possível degradação da performance nas instâncias do EC2 de sexta geração. Recomendamos que você atualize para a versão atual do driver para garantir que tenha as últimas atualizações.

Algumas maneiras como usar métricas de performance são:

- Solucionar problemas de performance de instâncias.
- Escolher o tamanho certo de instância para um workload.
- Planejar atividades de escalabilidade proativamente.

- Fazer benchmark em aplicações para determinar se elas maximizam a performance disponível em uma instância.

Taxa de atualização

Por padrão, o driver atualiza métricas usando um intervalo de 1 segundo. No entanto, a aplicação que recupera as métricas pode usar um intervalo diferente para sondagem. Você pode alterar o intervalo de atualização no Gerenciador de dispositivos, usando as propriedades avançadas do driver.

Para alterar o intervalo de atualização de métricas para o driver ENA do Windows, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.
6. Abra a guia Advanced (Avançado) na janela suspensa.
7. Na lista Property (Propriedade), escolha Metrics Refresh Interval (Intervalo de atualização das métricas) para alterar o valor.
8. Quando tiver concluído, escolha OK.

Redefinição do adaptador ENA

O processo de redefinição é iniciado quando o driver ENA do Windows detecta um erro em um adaptador e marca o adaptador como não íntegro. O driver não pode redefinir a si mesmo, portanto, depende do sistema operacional verificar o status da integridade do adaptador e chamar o identificador de redefinição para o driver ENA do Windows. O processo de redefinição pode resultar em um breve período de tempo em que ocorre perda de tráfego. No entanto, as conexões TCP devem ser capazes de se recuperar.

O adaptador ENA também pode solicitar indiretamente um procedimento de redefinição do dispositivo, ao não enviar uma notificação de manutenção de atividade. Por exemplo, se o adaptador

ENA atingir um estado desconhecido depois de carregar uma configuração irrecuperável, poderá parar de enviar notificações de keep-alive.

Causas comuns para redefinição do adaptador ENA

- Mensagens de keep-alive estão ausentes

  O dispositivo ENA posta eventos de keep-alive em uma taxa fixa (geralmente uma vez por segundo). O driver ENA do Windows implanta um mecanismo de watchdog, que verifica a presença dessas mensagens keep-alive. Se detectar uma ou mais novas mensagens desde a última vez que foi verificada, ele registra um resultado de êxito. Caso contrário, o driver conclui que o dispositivo sofreu uma falha e inicia uma sequência de redefinição.
- Os pacotes estão presos em filas de transmissão

  O adaptador ENA verifica se os pacotes estão fluindo pelas filas de transmissão conforme esperado. O driver ENA do Windows detecta se os pacotes estão ficando presos e inicia uma sequência de redefinição caso estejam.
- Tempo limite de leitura para registros de E/S mapeados da memória (MMIO)

  Para limitar as operações de leitura de E/S mapeadas de memória (MMIO), o driver ENA do Windows acessa os registros do MMIO somente durante os processos de inicialização e redefinição. Se o driver detectar um tempo limite, ele executará uma das seguintes ações, dependendo do processo em execução:
  - Se um tempo limite for detectado durante a inicialização, ele falhará no fluxo, o que resulta na exibição de um ponto de exclamação amarelo pelo adaptador ENA no Gerenciador de dispositivos do Windows.
  - Se um tempo limite for detectado durante a reinicialização, ele falhará no fluxo. O sistema operacional inicia uma remoção surpresa do adaptador ENA e o recupera parando e iniciando o adaptador que foi removido. Para obter mais informações sobre a remoção surpresa de uma placa de interface de rede (NIC), consulte Como lidar com a remoção surpresa de uma NIC na documentação Desenvolvedor de hardware do Microsoft Windows.

Cenários de solução de problemas

Os cenários a seguir podem ajudar a solucionar problemas que possam ocorrer com o driver ENA do Windows. Recomendamos que você comece atualizando seu driver ENA, se você não tiver a versão

mais recente. Para encontrar o driver mais recente para a versão do sistema operacional Windows, consulte Driver do ENA para o Windows.

Versão inesperada do driver ENA instalada

Descrição

Depois de seguir as etapas para instalar uma versão específica do driver ENA, o gerenciador de dispositivos do Windows mostra que o Windows instalou uma versão diferente do driver ENA.

Causa

Quando você executa a instalação de um pacote de driver, o Windows classifica todos os pacotes de drivers válidos para determinado dispositivo no armazenamento de drivers local antes da execução. Em seguida, ele seleciona o pacote com o menor valor de classificação como a melhor correspondência. Isso pode ser diferente do pacote que você pretendia instalar. Para obter mais informações sobre o processo de seleção do pacote de driver de dispositivo, consulte Como o Windows seleciona um pacote de driver para um dispositivo no site de documentação da Microsoft.

Solução

Para garantir que o Windows instale a versão do pacote de driver escolhida, você pode remover pacotes de drivers de classificação inferior do armazenamento de drivers com a ferramenta de linha de comando PnPUtil.

Siga estas etapas para atualizar o driver ENA:

1. Conecte-se à instância e faça login como administrador local.
2. Abra a janela de propriedades do Gerenciador de dispositivos, conforme descrito na seção Verifique o status do dispositivo ENA. Isso abre a guia Geral da janela Propriedades do Adaptador de Rede Elástica da Amazon.
3. Abra a guia Driver.
4. Escolha Update Driver (Atualizar driver). Isso abre a caixa de diálogo Atualizar software do driver: Adaptador de Rede Elástica da Amazon.

    a. Na seção Como deseja pesquisar o software de driver?, escolha Procurar software de driver no computador.

    b. Na página Procurar software de driver no computador, escolha Permitir escolher em uma lista de drivers de dispositivo em meu computador, localizado abaixo da barra de pesquisa.

c. Na página Selecionar o driver do dispositivo que você deseja instalar para este hardware, escolha Ter disco....

d. Na janela Instalar do disco, escolha Procurar..., próximo à localização na lista suspensa.

e. Navegue até o local em que você fez o download do pacote de driver ENA de destino. Selecione o arquivo denominado `ena.inf` e escolha Abrir.

f. Para iniciar a instalação, escolha OK e, em seguida, escolha Avançar.

5. Se o instalador não reinicializar automaticamente sua instância, execute o cmdlet Restart-Computer do PowerShell.

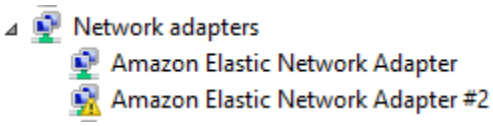
```
PS C:\> Restart-Computer
```

Aviso de dispositivo para driver ENA

Descrição

O ícone do adaptador ENA na seção Network adapters (Adaptadores de rede) do Gerenciador de dispositivos exibe um sinal de aviso (um triângulo amarelo com um ponto de exclamação dentro).

O exemplo a seguir mostra um adaptador ENA com o ícone de aviso no Gerenciador de dispositivos do Windows:



Causa

Esse aviso de dispositivo geralmente é causado por problemas de ambiente, o que pode exigir mais pesquisas, e muitas vezes exige um processo de eliminação para determinar a causa subjacente. Para obter uma lista completa de erros do dispositivo, consulte Mensagens de erro do Gerenciador de dispositivos na documentação Desenvolvedor de hardware do Microsoft Windows.

Solução

A solução para este aviso de dispositivo depende da causa raiz. O processo de eliminação descrito aqui inclui algumas etapas básicas para ajudar a identificar e resolver os problemas mais comuns que podem ter uma solução simples. É necessária uma análise de causa raiz adicional quando essas etapas não resolvem o problema.

Siga estas etapas para ajudar a identificar e resolver problemas comuns:

1. Interrompa e inicie o dispositivo.

   Abra a janela de propriedades do Gerenciador de dispositivos, conforme descrito na seção Verifique o status do dispositivo ENA. Isso abre a guia General (Geral) da janela Amazon Elastic Network Adapter Properties (Propriedades do adaptador do Amazon Elastic Network), onde Device status (Status do dispositivo) exibe o código de erro e uma mensagem curta.

   a. Abra a guia Driver.
   b. Selecione Disable Device (Desabilitar dispositivo) e responda Yes (Sim) para a mensagem de aviso exibida.
   c. Selecione Enable Device (Habilitar dispositivo).
2. Interrompa e inicie a instância do EC2

   Se o adaptador ainda mostrar o ícone de aviso no Gerenciador de dispositivos, a próxima etapa é interromper e iniciar a instância do EC2. Isso reinicia a instância em hardware diferente na maioria dos casos.
3. Investigue possível problema de recursos da instância

   Se você interrompeu e iniciou sua instância do EC2 e o problema persistir, isso pode indicar um problema de recurso na instância, como memória insuficiente.

Tempo limite de conexão com redefinição do adaptador (códigos de erro 5007, 5205)

Descrição

O Visualizador de eventos do Windows mostra o tempo limite do adaptador e os eventos de redefinição que ocorrem em combinação para adaptadores ENA. As mensagens são semelhantes aos exemplos a seguir:

- ID do evento 5007: adaptador do Amazon Elastic Network: Timed out during an operation (Tempo limite durante uma operação).
- ID do evento 5205: adaptador do Amazon Elastic Network Adapter: Adapter reset has been started (A redefinição do adaptador foi iniciada).

As redefinições do adaptador causam interrupção mínima no tráfego. Mesmo quando há várias redefinições, seria incomum que elas causem qualquer interrupção grave da rede.

Causa

Essa sequência de eventos indica que o driver ENA Windows iniciou uma redefinição para um adaptador ENA que não respondeu. No entanto, o mecanismo que o driver do dispositivo usa para detectar esse problema está sujeito a falsos positivos resultantes da falta de CPU 0.

Solução

Se essa combinação de erros ocorrer com frequência, verifique suas alocações de recursos para ver onde os ajustes podem ser úteis.

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Monitor de recursos do Windows, insira `resmon` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela do Monitor de recursos.
4. Abra a guia CPU. Gráficos de uso por CPU são mostrados ao longo do lado direito da janela Monitor de recursos.
5. Verifique os níveis de uso da CPU 0 para ver se eles estão muito altos.

Recomendamos que você configure o RSS para excluir a CPU 0 para o adaptador ENA em tipos de instância maiores (mais de 16 vCPU). Para tipos de instância menores, a configuração do RSS pode melhorar a experiência, mas devido ao menor número de núcleos disponíveis, o teste é necessário para garantir que a restrição dos núcleos da CPU não impacte negativamente a performance.

Use o comando Set-NetAdapterRss para configurar o RSS para seu adaptador ENA, conforme mostrado no exemplo a seguir.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

A migração para uma infra-estrutura de instância de sexta geração afeta a performance ou a anexação

Descrição

Se você migrar para uma instância do EC2 de sexta geração, poderá ter uma performance reduzida ou falhas de anexação do ENA se não tiver atualizado a versão do driver do ENA Windows.

Causa

Os tipos de instância do EC2 de sexta geração exigem a seguinte versão mínima do driver ENA para Windows, com base no sistema operacional da instância.

Versão mínima

Versão Windows Server	Versão do driver ENA
Windows Server 2008 R2	2.2.3 ou 2.4.0
Windows Server 2012 e posterior	2.2.3 e posterior
Estação de trabalho Windows	2.2.3 e posterior

Solução

Antes de fazer o upgrade para uma instância do EC2 de sexta geração, certifique-se de que a AMI a partir da qual você iniciar tenha os drivers compatíveis com base no sistema operacional da instância, como mostrado na tabela anterior. Para obter mais informações, consulte What do I need to do before migrating my EC2 instance to a sixth generation instance to make sure that I get maximum network performance? no AWS re:Post Knowledge Center.

Performance abaixo da ideal para a interface de rede elástica (ENI)

Descrição

A interface ENA não está funcionando conforme o esperado.

Causa

A análise de causa raiz para problemas de performance é um processo de eliminação. Existem muitas variáveis envolvidas para se nomear uma causa comum.

Solução

A primeira etapa na análise da causa raiz é revisar as informações de diagnóstico da instância que não está funcionando conforme o esperado, para determinar se há erros que podem estar causando

o problema. Para obter mais informações, consulte a seção Colete informações de diagnóstico sobre a instância.

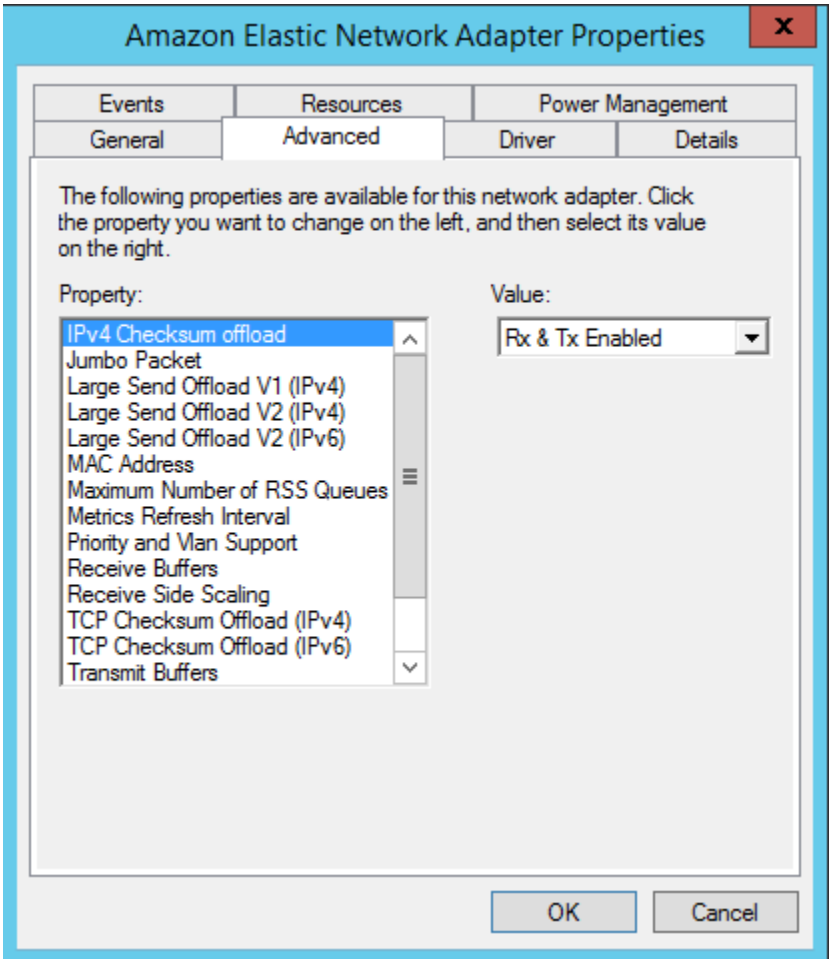
Para obter a máxima performance da rede em instâncias com redes avançadas, pode ser necessário modificar a configuração do sistema operacional padrão. Outras otimizações, como ativar o descarregamento de soma de verificação e a habilitação do RSS, por exemplo, já estão em vigor por padrão em AMIs oficiais do Windows. Para outras otimizações que você pode aplicar ao adaptador ENA, consulte os ajustes de performance mostrados em Ajustes de performance do adaptador ENA.

Recomendamos que você prossiga com cautela e limite os ajustes de propriedade do dispositivo àqueles listados nesta seção ou a alterações específicas recomendadas pela equipe de suporte da AWS.

Para alterar as propriedades do adaptador ENA, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.
6. Para fazer suas alterações, abra a guia Avançado.
7. Quando concluir, escolha OK para salvar suas alterações.

O exemplo a seguir mostra uma propriedade do adaptador ENA Gerenciador de dispositivos do Windows.



Ajustes de performance do adaptador ENA

A tabela a seguir inclui propriedades que podem ser ajustadas para melhorar a performance da interface ENA.

Entrada

Propriedade	Descrição	Valor padrão	Ajuste
Buffers de recebimento	Controla o número de entradas nas filas de recebimento do software.	1024	Pode ser aumentado até um máximo de 8192.
Receive Side Scaling (RSS)	Habilita a distribuição eficiente do	Habilitado	Você pode espalhar a carga em vários

Propriedade	Descrição	Valor padrão	Ajuste
	processamento de recebimento de rede em várias CPUs em sistemas multiproc essadores.		processadores. Para saber mais, consulte Otimização do desempenho da rede em instâncias do Windows.

Propriedade	Descrição	Valor padrão	Ajuste
Número máximo de filas de RSS	Define o número máximo de filas de RSS permitidas quando RSS está habilitado.	32	O número de filas de RSS é determinado durante a inicialização do driver e inclui as seguintes limitações (entre outras): • Limite de fila de RSS definido por esta propriedade • Limites de instância (contagem de vCPU) • Limites de geração de hardware (até oito filas de RSS no ENAv1 e até 32 filas de RSS no ENAv2) Você pode definir o valor de 1 a 32, dependendo dos limites de geração de instância e hardware. Para saber mais, consulte Otimização do desempenho da rede em instâncias do Windows.

Propriedade	Descrição	Valor padrão	Ajuste
Pacote jumbo	Permite o uso de frames jumbo ethernet (mais de 1500 bytes de carga útil).	Desabilitado (isso limita a carga útil a 1500 bytes ou menos)	O valor pode ser configurado para `9015`, o que se traduz em 9001 bytes de carga útil. Essa é a carga útil máxima para frames ethernet jumbo. Consulte Considerações sobre o uso de frames ethernet jumbo.

Considerações sobre o uso de frames ethernet jumbo

Os frames jumbo permitem mais de 1500 bytes de dados ao aumentar o tamanho da carga útil por pacote, o que aumenta o percentual do pacotes que não configura sobrecarga. São necessários menos pacotes para enviar a mesma quantidade de dados usáveis. No entanto, o tráfego é limitado a um MTU máximo de 1500 nos seguintes casos:

- Tráfego fora de uma determinada região da AWS para EC2 Classic.
- Tráfego fora de uma única VPC
- Tráfego em uma conexão de emparelhamento de VPC entre regiões
- Tráfego através de ligações de VPN
- Tráfego em um gateway de Internet

> **Note**
>
> Pacotes com mais de 1500 bytes são fragmentados. Se você tiver o sinalizador `Don't Fragment` definido no cabeçalho IP, esses pacotes são descartados.
> Os frames jumbo devem ser usados com cuidado para o tráfego voltado para Internet ou qualquer tráfego que saia de uma VPC. Os pacotes são fragmentados por sistemas

intermediários, que retarda o tráfego. Para usar frames jumbo dentro de uma VPC sem afetar o tráfego de saída que está saindo da VPC, tente uma das seguintes opções:

- Configure o tamanho da MTU por rota.
- Use várias interfaces de rede com diferentes tamanhos de MTU e rotas diferentes.

Casos de uso recomendados para frames jumbo

Frames jumbo podem ser úteis para tráfego dentro de e entre VPCs. Recomendamos usar frames jumbo para os seguintes casos de uso:

- Para instâncias posicionadas em um grupo de posicionamento de cluster, os frames jumbo ajudam a alcançar a throughput máxima de rede possível. Para ter mais informações, consulte Grupos de posicionamento.
- É possível usar quadros jumbo para tráfego entre suas VPCs e suas redes on-premises por meio do AWS Direct Connect. Para obter mais informações sobre o uso de AWS Direct Connect e a verificação da capacidade de frames jumbo, consulte Definir MTU de rede para interfaces virtuais privadas ou interfaces virtuais de trânsito no Guia do usuário do AWS Direct Connect.
- Para obter mais informações sobre tamanhos de MTU compatíveis com gateways de trânsito, consulte Cotas para seus gateways de trânsito em Gateways de trânsito da Amazon VPC.

Aprimore a latência de rede para instâncias do Amazon EC2 baseadas em Linux

A latência de rede corresponde à quantidade de tempo que um pacote de dados demora para se deslocar da origem até o destino. As aplicações que enviam dados pela rede dependem de respostas em tempo hábil para fornecer uma experiência positiva ao usuário. A alta latência de rede pode acarretar diversos problemas, como os seguintes:

- Tempos de carregamento lentos para páginas da Web.
- Atraso na transmissão de vídeo.
- Dificuldade de acesso aos recursos online.

Esta seção descreve as etapas que podem ser seguidas para aprimorar a latência de rede em instâncias do Amazon EC2 executadas em Linux. Para obter a latência ideal, siga estas etapas

para definir as configurações de sua instância, kernel e driver ENA. Para obter orientação de configurações adicionais, consulte o Guia de práticas recomendadas e otimização de performance para o driver ENA do Linux no GitHub.

> **Note**
>
> As etapas e configurações podem variar um pouco, dependendo do hardware de rede específico, da AMI da qual você executou a instância e do caso de uso da aplicação. Antes de realizar qualquer alteração, teste e monitore minuciosamente a performance da rede para garantir que esteja obtendo os resultados desejados.

Reduzir saltos de rede

Cada salto que um pacote de dados tem ao se mover de um roteador para outro aumenta a latência da rede. Normalmente, o tráfego passa por diversos saltos para chegar ao seu destino. Há duas maneiras de reduzir os saltos de rede para as instâncias do Amazon EC2, conforme apresentado a seguir:

- Grupo com posicionamento em cluster: ao especificar um grupo com posicionamento em cluster, o Amazon EC2 executa instâncias que estão com grande proximidade umas das outras, fisicamente na mesma zona de disponibilidade (AZ) comempacotamento mais restrito. A proximidade física das instâncias no grupo permite que elas aproveitem a conectividade de alta velocidade, resultando em baixa latência e alta throughput de fluxo único.
- Host dedicado: um host dedicado é um servidor físico dedicado para seu uso. Com um host dedicado, é possível executar as instâncias no mesmo servidor físico. A comunicação entre instâncias executada no mesmo host dedicado pode ocorrer sem nenhum salto extra de rede.

Configuração do kernel do Linux

A configuração do kernel do Linux pode aumentar ou diminuir a latência da rede. Para atingir suas metas de otimização de latência, é importante ajustar a configuração do kernel do Linux de acordo com os requisitos específicos de sua workload.

Existem várias opções de configuração para o kernel do Linux que podem ajudar a diminuir a latência da rede. As opções mais impactantes são as seguintes.

- Ativação do modo de pesquisa ocupada: o modo de pesquisa ocupada reduz a latência no caminho de recebimento da rede. Ao ativar o modo de pesquisa ocupada, o código da camada de soquete pode pesquisar diretamente a fila de recebimento de um dispositivo de rede. A desvantagem de uma sondagem ocupada é o maior uso da CPU no host, resultante da sondagem de novos dados em um ciclo restrito. Há duas configurações globais que controlam o número de microssegundos para aguardar os pacotes para todas as interfaces.

  `busy_read`

  Um tempo limite de sondagem ocupada de baixa latência para leituras de soquete. Ele controla o número de microssegundos a aguardar para camada de soquete ler os pacotes na fila de dispositivos. Para habilitar o recurso globalmente com o comando sysctl, a organização Linux Kernel recomenda um valor de 50 microssegundos. Para obter mais informações, consulte busy_read no Guia do usuário e do administrador do kernel doo Linux.

  ```
  $ C:\> sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Um tempo limite de sondagem ocupada de baixa latência para sondagem e seleção. Isso controla o número de microssegundos a aguardar por eventos. O valor recomendado está entre 50-100 microssegundos, dependendo do número de soquetes que você estiver sondando. Quanto mais soquetes você adicionar, maior deve ser o número.

  ```
  $ C:\> sudo sysctl -w net.core.busy_poll=50
  ```

- Configuração dos estados de energia da CPU (C-states): os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando está inativo. Você pode desejar controlar os C-states para ajustar o sistema em relação à latência versus performance. Em estados C mais profundos, a CPU está essencialmente “adormecida” e não poderá responder às solicitações até acordar e fazer a transição de volta ao estado ativo. Desativar núcleos leva tempo e, embora um núcleo desativado forneça mais espaço para um núcleo funcionar em uma frequência mais alta, leva tempo para que esse núcleo desativado seja reativado e execute o trabalho.

  Por exemplo, se um núcleo que receber a tarefa de lidar com interrupções de pacotes da Internet estiver desativado, poderá ocorrer um atraso em lidar com essa interrupção. É possível configurar o sistema para que ele não use estados C mais profundos. No entanto, embora essa configuração

reduza a latência de reação do processador, ela também reduz o espaço disponível para outros núcleos para o Turbo Boost.

Para reduzir a latência de reação do processador, é possível limitar mais profundamente os C-states. Para obter mais informações, consulte High performance and low latency by limiting deeper C-states no Amazon Linux 2 User Guide.

Configuração do driver ENA

O driver de rede ENA possibilita a comunicação entre uma instância e uma rede. O driver processa os pacotes de rede e os repassa à pilha de rede ou ao cartão Nitro. Quando um pacote de rede chega, o cartão Nitro gera uma interrupção para a CPU notificar o software sobre um evento.

Interromper

Uma interrupção é um sinal que um dispositivo ou aplicação envia ao processador. A interrupção informa ao processador que ocorreu um evento ou que foi atendida uma condição que requer atenção imediata. As interrupções podem lidar com tarefas urgentes, como receber dados de uma interface de rede, lidar com eventos de hardware ou atender a solicitações de outros dispositivos.

Moderação de interrupção

A moderação de interrupções é uma técnica que reduz o número de interrupções que um dispositivo gera agregando ou atrasando-as. O objetivo da moderação de interrupções é melhorar o desempenho do sistema, reduzindo a sobrecarga associada ao tratamento de um grande número de interrupções. Interrupções demais aumentam o uso da CPU, afetando negativamente a throughput, enquanto poucas interrupções aumentam a latência.

Moderação dinâmico de interrupções

A moderação dinâmica de interrupções é uma forma aprimorada de moderação de interrupção que ajusta dinamicamente a taxa de interrupções com base nos padrões atuais de carga e tráfego do sistema. O objetivo é encontrar um equilíbrio entre reduzir a sobrecarga de interrupções e os pacotes por segundo, ou a largura de banda.

> **Note**
>
> A moderação dinâmica de interrupções é habilitada por padrão em algumas AMIs (mas pode ser habilitada ou desabilitada em todas as AMIs).

Para minimizar a latência da rede, pode ser necessário desabilitar a moderação de interrupções. No entanto, isso também pode aumentar a sobrecarga do processamento de interrupção. É importante descobrir o balanceamento adequado entre reduzir a latência e minimizar a sobrecarga. Os comandos `ethtool` podem ajudar você a configurar a moderação de interrupção. Por padrão, `rx-usecs` está definido como `20` e `tx-usecs` está definido como `64`.

Para obter a configuração de modificação de interrupção atual, use o comando a seguir.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Para desativar a modificação de interrupções, use o comando a seguir.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considerações sobre o Nitro System para ajuste de performance

O Sistema Nitro é uma coleção de hardware e componentes de software desenvolvidos pela AWS que permitem alta performance, alta disponibilidade e alta segurança. O Nitro System fornece funcionalidades semelhantes às funcionalidades do bare metal que eliminam a sobrecarga de virtualização e são compatíveis com workloads que requerem acesso total ao hardware de host. Para obter informações mais detalhadas, consulte AWS Nitro System.

Todos os tipos de instância do EC2 da geração atual executam o processamento de pacotes de rede em cartões Nitro do EC2. Este tópico aborda a manipulação de pacotes de alto nível no cartão Nitro, os aspectos conhecidos da arquitetura e da configuração de rede que afetam a performance da manipulação de pacotes e as ações você pode executar para atingir a performance máxima para as instâncias baseadas no Nitro.

Os cartões Nitro lidam com todas as interfaces de entrada e saída (E/S), como aquelas necessárias para as nuvens privadas virtuais (VPCs). Para todos os componentes que enviam ou recebem informações pela rede, os cartões Nitro atuam como um dispositivo de computação independente para o tráfego de E/S que é fisicamente separado da placa principal do sistema na qual as workloads do cliente são executadas.

Fluxo de pacotes de rede em cartões Nitro

As instâncias do EC2 desenvolvidas no Nitro System têm funcionalidades de aceleração de hardware que facilitam um processamento de pacotes mais rápido, conforme medido pelas taxas de throughput de pacotes por segundo (PPS). Quando um cartão Nitro executa a avaliação inicial para um novo fluxo, ele salva informações semelhantes para todos os pacotes no fluxo, como os grupos de segurança, as listas de controle de acesso e as entradas da tabela de rotas. Ao processar pacotes adicionais para o mesmo fluxo, ele pode usar as informações salvas para reduzir a sobrecarga desses pacotes.

A taxa de conexão é medida pela métrica de conexões por segundo (CPS). Cada nova conexão requer uma sobrecarga de processamento adicional que deve ser considerada nas estimativas de capacidade para a workload. É importante considerar as métricas de CPS e de PPS ao projetar as workloads.

Como uma conexão é estabelecida

Quando uma conexão é estabelecida entre uma instância baseada no Nitro e outro endpoint, o cartão Nitro avalia o fluxo completo do primeiro pacote enviado ou recebido entre os dois endpoints. Em geral não é necessária uma reavaliação completa para pacotes subsequentes do mesmo fluxo. No entanto, existem exceções. Para obter mais informações sobre as exceções, consulte Pacotes que não usam a aceleração de hardware.

As propriedades apresentadas a seguir definem os dois endpoints e o fluxo de pacotes entre eles. Essas cinco propriedades em conjunto são conhecidas como um fluxo de cinco tuplas.

- IP de origem
- Porta de origem
- IP de destino
- Porta de destino
- Protocolo de comunicação

A direção do fluxo de pacotes é conhecida como ingress (entrada) e egress (saída). As descrições de alto nível apresentadas a seguir resumem o fluxo de pacotes de rede de ponta a ponta.

- Ingress: quando um cartão Nitro lida com um pacote de rede de entrada, ele avalia o pacote em relação a regras de firewall com estado e a listas de controle de acesso. Ele rastreia a conexão,

realiza a medição dela e executa outras ações, conforme aplicável. Em seguida, ele encaminha o pacote ao destino na CPU de host.

- Egress: quando um cartão Nitro lida com um pacote de rede de saída, ele procura o destino da interface remota, avalia diversas funções da VPC, aplica limites de taxa e executa outras ações aplicáveis. Em seguida, ele encaminha o pacote para o destino do próximo salto na rede.

Projeto para obtenção de uma performance ideal

Para aproveitar as funcionalidades de performance do Nitro System, é necessário compreender quais são as suas necessidades de processamento de rede e como elas afetam a workload dos seus recursos do Nitro. Em seguida, será possível realizar um projeto para obtenção de uma performance ideal para seu cenário de rede. As definições de infraestrutura, design e configuração da workload da aplicação podem afetar o processamento de pacotes e as taxas de conexão. Por exemplo, se a aplicação tiver uma alta taxa de estabelecimento de conexão, como um serviço de DNS, um firewall ou um roteador virtual, ela terá menos oportunidades de aproveitar a aceleração de hardware que ocorre somente após o estabelecimento da conexão.

É possível definir as configurações da aplicação e da infraestrutura para simplificar as workloads e aprimorar a performance da rede. No entanto, nem todos os pacotes que estão qualificados para a aceleração. O Nitro System utiliza todo o fluxo de rede para novas conexões e para pacotes que não estão qualificados para a aceleração.

O restante desta seção se concentrará nas considerações de projeto para a aplicação e para a infraestrutura com a finalidade de ajudar a garantir que os pacotes fluam dentro do caminho com aceleração, tanto quanto possível.

Considerações

Ao configurar o tráfego de rede para a instância, existem muitos aspectos a serem considerados que podem afetar a performance de PPS. Depois que um fluxo é estabelecido, a maioria dos pacotes que entram ou saem regularmente está qualificado para a aceleração. No entanto, existem exceções para garantir que os projetos de infraestrutura e os fluxos de pacotes continuem atendendo aos padrões dos protocolos.

Para obter a melhor performance do cartão Nitro, é necessário considerar com atenção os prós e os contras dos detalhes de configuração apresentados a seguir para a infraestrutura e para as aplicações.

Considerações sobre infraestrutura

A configuração da infraestrutura pode afetar o fluxo de pacotes e a eficiência do processamento. A lista apresentada a seguir inclui algumas considerações importantes.

Configuração da interface de rede com assimetria

Os grupos de segurança usam o rastreamento de conexão para rastrear informações sobre o tráfego que flui de e para a instância. O roteamento assimétrico, em que o tráfego entra em uma instância por meio de uma interface de rede e sai por meio de uma interface de rede diferente, pode reduzir a performance máxima que uma instância poderá alcançar se os fluxos forem rastreados. Para obter mais informações sobre o rastreamento de conexões para grupos de segurança, conexões não rastreadas e conexões rastreadas automaticamente, consulte Rastreamento de conexão do grupo de segurança.

Drivers de rede

Os drivers de rede são atualizados e lançados regularmente. A performance poderá ser significativamente prejudicada se os drivers estiverem desatualizados. Mantenha os drivers atualizados para garantir que você tenha os patches mais recentes e possa aproveitar as vantagens fornecidas pelos aprimoramentos de performance, como o recurso de caminho com aceleração que está disponível somente para a última geração de drivers. Os drivers anteriores não são compatíveis com o recurso de caminho com aceleração.

Para aproveitar o recurso de caminho com aceleração, recomendamos instalar o driver do ENA mais recente nas instâncias.

Instâncias do Linux: driver do ENA para o Linux na versão 2.2.9 ou em versões posteriores. Para instalar ou atualizar o driver do ENA para Linux usando o repositório Amazon Drivers no GitHub, consulte a seção Driver compilation do arquivo “leia-me”.

Instâncias do Windows: driver do ENA para o Windows na versão 2.0.0 ou em versões posteriores. Para instalar ou atualizar o driver do ENA para o Windows, consulte Instalação do driver do Adaptador de Rede Elástica (ENA).

Distância entre os endpoints

Uma conexão entre duas instâncias na mesma zona de disponibilidade pode processar mais pacotes por segundo do que uma conexão entre regiões, como resultado do janelamento de TCP na camada da aplicação, que define quantos dados podem estar em trânsito a qualquer momento. As longas distâncias entre as instâncias aumentam a latência e diminuem o número de pacotes que os endpoints podem processar.

Considerações sobre o projeto da aplicação

Existem aspectos do projeto e da configuração da aplicação que podem afetar a eficiência do processamento. A lista apresentada a seguir inclui algumas considerações importantes.

Tamanho do pacote

Os pacotes com tamanhos maiores podem aumentar o throughput para os dados que uma instância pode enviar e receber na rede. Os pacotes com tamanhos menores podem aumentar a taxa de processamento de pacotes, mas podem reduzir a largura de banda máxima alcançada quando o número de pacotes excede as permissões de PPS.

Se o tamanho de um pacote exceder a Unidade Máxima de Transmissão (MTU) de um salto de rede, um roteador ao longo do caminho poderá fragmentá-lo. Os fragmentos de pacotes resultantes são considerados exceções e são processados na taxa padrão (não acelerada). Isso pode causar variações na performance. O Amazon EC2 oferece suporte a frames jumbo de 9.001 bytes, mas não são todos os serviços que disponibilizam esse suporte. Recomendamos avaliar a topologia ao configurar a MTU.

Compensações de protocolo

Os protocolos confiáveis, como o TCP, têm mais sobrecarga do que os protocolos não confiáveis, como o UDP. A menor sobrecarga e o processamento de rede simplificado para o protocolo de transporte UDP podem resultar em uma taxa de PPS mais alta, mas às custas da entrega confiável de pacotes. Se a entrega confiável de pacotes não for crítica para a aplicação, o protocolo UDP pode ser uma boa opção.

Microexpansão

A Microexpansão ocorre quando o tráfego excede as permissões durante breves períodos de tempo, em vez de ser distribuído uniformemente. Isso costuma acontecer em uma escala de microssegundos.

Por exemplo, suponhamos que você tenha uma instância que pode enviar até 10 Gbps e a aplicação envie 10 Gb completos em meio segundo. Essa microexpansão excede o permitido durante a primeira metade do segundo e não deixa nada para o restante da segunda. Mesmo que você tenha enviado 10 Gb no período de um segundo, as permissões na primeira metade do segundo podem resultar em pacotes enfileirados ou descartados.

É possível usar um programador de rede, como o Traffic Control do Linux, para ajudar no controle do throughput e evitar provocar pacotes enfileirados ou descartados como resultado de uma microexpansão.

Número de fluxos

Um único fluxo é limitado a 5 Gbps, a menos que esteja em um grupo de posicionamento de cluster que oferece suporte para até 10 Gbps ou que use o ENA Express, que oferece suporte para até 25 Gbps.

Da mesma forma que um cartão Nitro pode processar mais pacotes em vários fluxos, em vez de usar um único fluxo. Para atingir a taxa máxima de processamento de pacotes por instância, recomendamos, no mínimo, cem fluxos em instâncias com largura de banda agregada de 100 Gbps ou superior. À medida que as funcionalidades agregadas de largura de banda aumentam, o número de fluxos necessários para atingir as taxas de processamento máximas também aumenta. A avaliação comparativa ajudará você a definir qual configuração é necessária para atingir as taxas máximas em sua rede.

Número de filas do Adaptador de Rede Elástica (ENA)

Por padrão, o número máximo de filas do ENA é alocado para uma interface de rede com base no tamanho e no tipo da instância. A redução da contagem de filas pode reduzir a taxa máxima de PPS alcançável. Recomendamos usar a alocação de fila padrão para obter a melhor performance.

Para o Linux, uma interface de rede é configurada com o máximo por padrão. Para as aplicações baseadas no Data Plane Development Kit (DPDK), recomendamos configurar o número máximo de filas disponíveis.

Sobrecarga no processamento de recursos

Os recursos, como o Espelhamento de Tráfego e o ENA Express, podem adicionar mais sobrecarga de processamento, o que pode reduzir a performance absoluta do processamento de pacotes. É possível limitar o uso de recursos ou desativá-los para aumentar as taxas de processamento de pacotes.

Rastreamento de conexão para manutenção do estado

Os grupos de segurança usam o rastreamento de conexão para armazenar as informações sobre o tráfego de entrada e de saída da instância. O rastreamento de conexão aplica regras a cada fluxo de tráfego de rede individual para determinar se o tráfego será permitido ou negado. O cartão Nitro usa o rastreamento de fluxo para realizar a manutenção do estado para o fluxo. À medida que mais regras do grupo de segurança são aplicadas, mais trabalho é necessário para avaliar o fluxo.

> **Note**
>
> Não são todos os fluxos de tráfego de rede que são rastreados. Se uma regra do grupo de segurança estiver configurada com Conexões não rastreadas, nenhum trabalho adicional será necessário, exceto para conexões que são rastreadas automaticamente a fim de garantir o roteamento simétrico quando houver vários caminhos de resposta válidos.

Pacotes que não usam a aceleração de hardware

Não são todos os pacotes que podem aproveitar a aceleração de hardware. O tratamento dessas exceções envolve alguma sobrecarga de processamento necessária para garantir a integridade dos fluxos de rede. Os fluxos de rede devem atender aos padrões de protocolo com confiabilidade, estar em conformidade com as alterações no projeto da VPC e rotear pacotes somente para destinos permitidos. No entanto, a sobrecarga reduz a performance.

Fragmentos de pacote

Conforme mencionado em Considerações da aplicação, os fragmentos de pacotes resultantes de pacotes que excedem a MTU da rede são tratados como exceções e não podem aproveitar a aceleração de hardware.

Conexões ociosas

Quando uma conexão não tiver atividade por um período, mesmo que não tenha atingido o tempo limite, o sistema pode deixar de priorizá-la. Assim, se os dados forem recebidos depois que a conexão deixar de ser priorizada, o sistema precisará tratá-los como uma exceção para se reconectar.

Para gerenciar as conexões, é possível usar tempos limite de rastreamento de conexão para fechar as conexões ociosas. Além disso, é possível usar a opção keep-alive do TCP para manter as conexões ociosas abertas. Para ter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

Mutação da VPC

As atualizações em grupos de segurança, tabelas de rotas e listas de controle de acesso precisam ser avaliadas novamente no caminho de processamento para garantir que as entradas de rota e as regras do grupo de segurança ainda sejam aplicadas conforme o esperado.

Fluxos ICMP

O Internet Control Message Protocol (ICMP) é um protocolo de camada de rede que os dispositivos de rede usam para diagnosticar problemas de comunicação de rede. Esses pacotes sempre usam o fluxo completo.

Maximização da performance da rede no Nitro System

Antes de tomar qualquer decisão em relação ao projeto ou ajustar quaisquer configurações de rede na instância, recomendamos que você siga etapas apresentadas a seguir para obter o melhor resultado:

1. Compreenda os prós e os contras das ações que você pode executar para aprimorar a performance ao analisar as Considerações.

   Para obter mais considerações e práticas recomendadas para a configuração da instância, consulte:

   Instâncias do Linux: ENA Linux Driver Best Practices and Performance Optimization Guide no site do GitHub.

   Instâncias do Windows: Melhores práticas para configurar interfaces de rede.
2. Faça uma avaliação comparativa das workloads com a contagem máxima de fluxo ativo para definir uma referência para a performance da aplicação. Com uma referência para a performance, é possível testar variações nas configurações ou no projeto da aplicação para compreender quais considerações terão maior impacto, sobretudo se você planeja aumentar a escala verticalmente ou aumentar a escala horizontalmente.

A seguinte lista contém ações que podem ser executadas para ajustar a performance de PPS, conforme as necessidades do sistema.

- Reduzir a distância física entre duas instâncias. Quando as instâncias de envio e de recebimento estão localizadas na mesma zona de disponibilidade ou usam grupos de posicionamento de cluster, é possível reduzir o número de saltos que um pacote precisa realizar para se deslocar de um endpoint para outro.
- Usar Conexões não rastreadas.
- Usar o protocolo UDP para o tráfego de rede.

- Para instâncias do EC2 com largura de banda agregada de 100 Gbps ou mais, distribuir a workload em cem ou mais fluxos individuais para distribuir o trabalho uniformemente pelo cartão Nitro.

Monitoramento da performance em instâncias do Linux

É possível usar métricas do plug-in Ethtool em instâncias do Linux para monitorar indicadores de performance de rede de instâncias, como a largura de banda, a taxa de pacotes e o rastreamento de conexão. Para ter mais informações, consulte Monitorar a performance de rede de sua instância do EC2.

Otimização do desempenho da rede em instâncias do Windows

Para obter o máximo desempenho da rede nas instâncias do Windows com redes aperfeiçoadas, pode ser necessário modificar a configuração padrão do sistema operacional. Recomendamos as seguintes alterações de configuração para aplicações que exigem alta performance de rede. Outras otimizações (como ativar o descarregamento de soma de verificação e habilitar RSS, por exemplo) já estão configuradas nas AMIs oficiais do Windows.

> **Note**
>
> O descarregamento do TCP chimney deve ser desabilitado na maioria dos casos de uso e se tornou obsoleto a partir do Windows Server 2016.

Além dessas otimizações do sistema operacional, você também deve considerar a unidade de transmissão máxima (MTU - maximum transmission unit) de seu tráfego de rede e ajustá-la de acordo com sua workload e arquitetura de rede. Para obter mais informações, consulte Unidade de transmissão máxima (MTU) de rede para a instância do EC2.

A AWS mede regularmente as latências médias de ida e volta entre instâncias iniciadas em um grupo de posicionamento de cluster de 50 us e latência final de 200 us no percentil 99,9. Se suas aplicações exigirem baixas latências de forma consistente, recomendamos usar a versão mais recente dos drivers ENA em instâncias de performance fixa criadas no sistema Nitro.

Configurar afinidade de CPU RSS

O Receive Side Scaling (RSS) é usado para distribuir a carga da CPU do tráfego de rede em vários processadores. Por padrão, as AMIs oficiais do Amazon Windows são configuradas com RSS

ativado. ENIs do ENA fornecem até oito filas RSS. Com a definição de afinidade de CPU para filas RSS, bem como para outros processos do sistema, é possível distribuir a carga de CPU pelos sistemas com vários núcleos, permitindo que mais tráfego de rede seja processado. Em tipos de instância com mais de 16 vCPUs, recomendamos que você use o cmdlet `Set-NetAdapterRSS` do PowerShell, que exclui manualmente o processador de inicialização (processador lógico 0 e 1 quando o hyper-threading está ativado) da configuração de RSS para todos os ENIs, a fim de evitar a contenção com vários componentes do sistema.

O Windows reconhece o hyper-thread e garantirá que as filas RSS de uma única NIC sejam sempre colocadas em diferentes núcleos físicos. Portanto, a menos que o hyper-threading esteja desabilitado, para evitar completamente a contenção com outras NICs, propague a configuração RSS de cada NIC entre um intervalo de 16 processadores lógicos. O cmdlet `Set-NetAdapterRss` permite que você defina o intervalo por NIC de processadores lógicos válidos definindo os valores de BaseProcessorGroup, BaseProcessorNumber, MaxProcessingGroup, MaxProcessorNumber e NumaNode (opcional). Se não houver núcleos físicos suficientes para eliminar completamente a contenção entre NICs, minimize os intervalos de sobreposição ou reduza o número de processadores lógicos nos intervalos de ENI dependendo da workload esperada da ENI (ou seja, uma ENI de rede administrativa de baixo volume pode não precisar de tantas filas RSS atribuídas). Além disso, como observado anteriormente, diversos componentes devem ser executados na CPU 0 e, por isso, recomendamos a exclusão em todas as configurações RSS quando houver vCPUs suficientes disponíveis.

Por exemplo, quando há três ENIs em uma instância de 72 vCPUs com 2 nós NUMA com o hyper-threading habilitado, os comandos a seguir distribuem a carga de rede entre as duas CPUs sem sobreposição e impedem completamente o uso do núcleo 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Observe que essas configurações são persistentes para cada adaptador de rede. Se uma instância for redimensionada para uma com um número diferente de vCPUs, você deverá reavaliar a configuração RSS para cada ENI habilitada. A documentação completa da Microsoft para o cmdlet `Set-NetAdapterRss` pode ser encontrada aqui: https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadapterrss.

Observação especial para workloads SQL: também recomendamos que você revise suas configurações de afinidade de thread de E/S juntamente com sua configuração RSS da ENI para minimizar a contenção de E/S e de rede para as mesmas CPUs. Consulte Opção de configuração do servidor de máscara de afinidade.

Elastic Fabric Adapter

O Elastic Fabric Adapter (EFA) é um dispositivo de rede que é possível anexar à instância do Amazon EC2 para acelerar as aplicações de machine learning e de Computação de Alta Performance (HPC). O EFA permite que você atinja a performance da aplicação de um cluster HPC on-premises, com a escalabilidade, a flexibilidade e a elasticidade fornecidas pela Nuvem AWS.

Os EFAs fornecem latência mais baixa e mais consistente e maior throughput que o transporte de TCP tradicionalmente usado em sistemas HPC baseados em nuvem. Ele aprimora a performance da comunicação entre instâncias, que é essencial para o dimensionamento de aplicações de machine learning e de HPC. Ele é otimizado para funcionar na infraestrutura de rede da AWS existente e pode ser dimensionado dependendo dos requisitos da aplicação.

Os EFAs se integram ao Libfabric 1.7.0 e versões posteriores, sendo compatíveis com Open MPI 5 e versões posteriores e Intel MPI 2019 Update 5 e versões posteriores para aplicações de HPC, além de Nvidia Collective Communications Library (NCCL) para aplicativos de machine learning.

> **Note**
>
> Os recursos de desvio de sistema operacional do EFAs não são compatíveis em instâncias do Windows. Se você anexar um EFA a uma instância do Windows, a instância funcionará como um Elastic Network Adapter, sem os recursos de EFA adicionais.

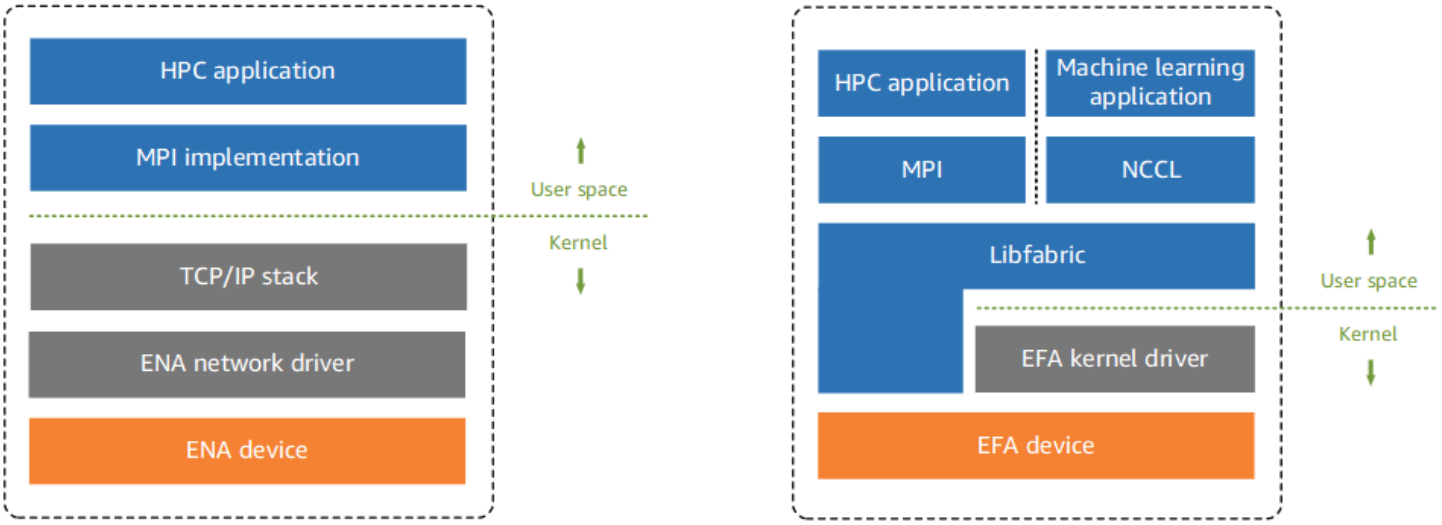
Tópicos

- Conceitos básicos de EFA
- Interfaces e bibliotecas compatíveis
- Tipos de instâncias compatíveis
- Sistemas operacionais compatíveis
- Limitações de EFA
- Preços do EFA

- Começar a usar instâncias P5 e EFA
- Conceitos básicos do EFA e MPI
- Conceitos básicos do EFA e NCCL
- Trabalhar com EFA
- Monitorar um EFA
- Verificar o instalador EFA usando uma soma de verificação

Conceitos básicos de EFA

Um EFA é um Elastic Network Adapter (ENA) com recursos adicionais. Ele fornece todas as funcionalidades de um ENA, com uma funcionalidade adicional de desvio de sistema operacional. O desvio de sistema operacional é um modelo de acesso que permite que as aplicações de machine learning e de HPC se comuniquem diretamente com o hardware da interface de rede para fornecer funcionalidade de transporte confiável e de baixa latência.



Traditional HPC software stack in EC2

HPC software stack in EC2 with EFA

Tradicionalmente, as aplicações HPC usam a Message Passing Interface (MPI) para fazer interface com o transporte de rede do sistema. Na Nuvem AWS, isso significa que as aplicações fazem interface com a MPI, que usa a pilha TCP/IP do sistema operacional e o driver de dispositivo ENA para habilitar a comunicação de rede entre as instâncias.

Com um EFA, aplicações HPC usam a MPI ou a NCCL para fazer interface com a API Libfabric. A API Libfabric ignora o kernel do sistema operacional e se comunica diretamente com o dispositivo EFA para colocar pacotes na rede. Isso reduz a sobrecarga e permite que a aplicação HPC seja executado com mais eficiência.

> **Note**
>
> O libfabric é um componente central do framework OpenFabrics Interfaces (OFI), que define e exporta a API do espaço do usuário do OFI. Para obter mais informações, consulte o site Libfabric OpenFabrics.

Diferenças entre EFAs e RIs

Elastic Network Adapters (ENAs) fornecem recursos tradicionais de rede IP que são necessários para permitir as redes da VPC. Os EFAs fornecem todos os mesmos recursos de rede IP tradicionais que os ENAs e também oferecem suporte a recursos de desvio do sistema operacional. O desvio de sistema operacional permite que as aplicações de machine learning e de HPC ignorem o kernel do sistema operacional e se comuniquem diretamente com o dispositivo EFA.

Interfaces e bibliotecas compatíveis

Os EFAs oferecem suporte às seguintes interfaces e bibliotecas:

- Open MPI 5 e posterior
- Open MPI 4.0 ou mais recente é o preferencial para o Graviton
- Intel MPI 2019 Update 5 e posterior
- NVIDIA Collective Communications Library (NCCL) 2.4.2 e posterior

Tipos de instâncias compatíveis

Os tipos de instância a seguir são compatíveis com EFAs:

- Uso geral: `m5dn.24xlarge` | `m5dn.metal` | `m5n.24xlarge` | `m5n.metal` | `m5zn.12xlarge` | `m5zn.metal` | `m6a.48xlarge` | `m6a.metal` | `m6i.32xlarge` | `m6i.metal` | `m6id.32xlarge` | `m6id.metal` | `m6idn.32xlarge` | `m6idn.metal` | `m6in.32xlarge` | `m6in.metal` | `m7a.48xlarge` | `m7a.metal-48xl` | `m7g.16xlarge` | `m7g.metal` | `m7gd.16xlarge` | `m7gd.metal` | `m7i.48xlarge` | `m7i.metal-48xl`
- Otimizada para computação: `c5n.9xlarge` | `c5n.18xlarge` | `c5n.metal` | `c6a.48xlarge` | `c6a.metal` | `c6gn.16xlarge` | `c6i.32xlarge` | `c6i.metal` | `c6id.32xlarge` | `c6id.metal` | `c6in.32xlarge` | `c6in.metal` | `c7a.48xlarge` | `c7a.metal-48xl` | `c7g.16xlarge`

| c7g.metal | c7gd.16xlarge | c7gd.metal | c7gn.16xlarge | c7gn.metal | c7i.48xlarge | c7i.metal-48xl

- Otimizadas para memória: r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal | r6a.48xlarge | r6a.metal | r6i.32xlarge | r6i.metal | r6idn.32xlarge | r6idn.metal | r6in.32xlarge | r6in.metal | r6id.32xlarge | r6id.metal | r7a.48xlarge | r7a.metal-48xl | r7g.16xlarge | r7g.metal | r7gd.16xlarge | r7gd.metal | r7i.48xlarge | r7i.metal-48xl | r7iz.32xlarge | r7iz.metal-32xl | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge | x2iezn.metal
- Otimizadas para armazenamento: i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- Com computação acelerada: dl1.24xlarge | dl2q.24xlarge | g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge | g6.8xlarge | g6.12xlarge | g6.16xlarge | g6.24xlarge | g6.48xlarge | gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge | trn1.32xlarge | trn1n.32xlarge | vt1.24xlarge
- Computação de alta performance: hpc6a.48xlarge | hpc6id.32xlarge | hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge | hpc7g.8xlarge | hpc7g.16xlarge

Para ver os tipos de instância disponíveis com suporte a EFAs em uma região específica

Os tipos de instância disponíveis variam de acordo com a região. Para ver os tipos de instâncias disponíveis com suporte a EFAs em uma região, use o comando describe-instance-types com o parâmetro `--region`. Inclua o parâmetro `--filters` para definir o escopo dos resultados para os tipos de instância com suporte a EFA e o parâmetro `--query` para definir o escopo da saída para o valor de `InstanceType`.

```
aws ec2 describe-instance-types  --region us-east-1  --filters Name=network-info.efa-supported,Values=true  --query "InstanceTypes[*].[InstanceType]"  --output text | sort
```

Sistemas operacionais compatíveis

O suporte ao sistema operacional varia dependendo do tipo de processador. A tabela a seguir mostra os sistemas operacionais compatíveis.

Sistema operacional	Tipos de instância Intel/AMD (**`x86_64`**)	Tipos de instância AWS Graviton (**`arm64`**)
Amazon Linux 2023	✓	✓
Amazon Linux 2	✓	✓
CentOS 7	✓	
RHEL 7, 8 e 9	✓	✓
Debian 10 e 11	✓	✓
Rocky Linux 8 e 9	✓	✓
Ubuntu 20.04, 22.04 e 24.04	✓	✓
SUSE Linux Enterprise 15 SP2 e posterior	✓	✓
OpenSUSE Leap 15.5 e posterior	✓	

> **Note**
>
> O Ubuntu 20.04 é compatível com suporte direto ponto a ponto quando usado com instâncias `dl1.24xlarge`.

Limitações de EFA

Os EFAs têm as seguintes limitações:

- Todos os tipos de instância P4d e P5 são compatíveis com Remote Direct Memory Access (RDMA) de GPUDirect NVIDIA.
- Atualmente, o tráfego EFA entre instâncias P4d/P4de/DL1 e outros tipos de instância não é compatível.
- Os tipos de instância compatíveis com várias placas de rede podem ser configurados com um EFA por placa de rede. Todos os outros tipos de instância compatíveis oferecem suporte a apenas um EFA por instância.
- Instâncias dedicadas `c7g.16xlarge`, `m7g.16xlarge`, e `r7g.16xlarge`, e hosts dedicados não são compatíveis quando um EFA está anexado.
- EFA O tráfego de desvio do sistema operacional é limitado a uma única sub-rede. Em outras palavras, o tráfego de EFA não pode ser enviado de uma sub-rede para outra. O tráfego IP normal do EFA pode ser enviado de uma sub-rede para outra.
- EFA O tráfego de desvio do sistema operacional não é roteável. O tráfego IP normal do EFA permanece roteável.
- O EFA deve ser um membro de um grupo de segurança que permita todo o tráfego de entrada e saída de e para o próprio grupo de segurança.
- O EFA não é compatível com as instâncias do Windows.
- EFA não é compatível com o AWS Outposts

Preços do EFA

O EFA está disponível como um recurso de rede opcional do Amazon EC2 que pode ser habilitado em qualquer instância compatível sem nenhum custo adicional.

Começar a usar instâncias P5 e EFA

As instâncias P5 fornecem 3.200 Gbps de largura de banda de rede usando várias interfaces EFA. As instâncias P5 oferecem suporte a 32 placas de rede. Para obter mais informações sobre como começar a usar instâncias P5, consulte Como começar a usar instâncias P5 para o Linux.

Recomendamos que você defina uma única interface de rede EFA por placa de rede. Para configurar essas interfaces no lançamento, recomendamos as seguintes configurações:

- Para interface de rede `0`, especifique o índice de dispositivo `0`
- Para interface de rede 1 a 31, especifique o índice de dispositivo 1

Se você estiver usando o console do Amazon EC2, no Launch Instance Wizard, escolha Editar na seção Configurações de rede. Expanda Configuração avançada de rede e escolha Adicionar interface de rede para adicionar o número necessário de interfaces de rede. Para cada interface de rede, em EFA, selecione Habilitar. Para todas as interfaces de rede, exceto a interface de rede primária, em Índice de dispositivos, especifique 1. Defina as configurações restantes, conforme necessário.

Se você estiver usando a AWS CLI, use o comando run-instances, em `--network-interfaces`, especifique o número necessário de interfaces de rede. Para cada interface de rede, em `InterfaceType`, especifique `efa`. Para a interface de rede primária, em `NetworkCardIndex` e `DeviceIndex`, especifique `0`. Para as demais interfaces de rede, em `NetworkCardIndex`, especifique um valor exclusivo de 1 a 31, e em `DeviceIndex`, especifique 1.

O exemplo de snippet de comando a seguir mostra uma solicitação com 32 interfaces de rede EFA.

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
```

```
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
```

```
  "NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
  \
  "NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...
```

Se você estiver usando um modelo de execução, especifique o número necessário de interfaces de rede no modelo de execução. Para cada interface de rede, em `InterfaceType`, especifique `efa`. Para a interface de rede primária, em `NetworkCardIndex` e `DeviceIndex`, especifique `0`. Para

as demais interfaces de rede, em `NetworkCardIndex`, especifique um valor exclusivo de 1 a 31, e em `DeviceIndex`, especifique 1. O trecho a seguir mostra um exemplo com 3 interfaces de rede das 32 interfaces de rede possíveis.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Ao iniciar uma instância P5 com mais de uma interface de rede, não é possível atribuir endereços IP públicos automaticamente. No entanto, você pode anexar um endereço IP elástico à interface de rede primária (NetworkCardIndex = 0, DeviceIndex = 0) após a execução para ter conectividade com a Internet. Tanto o Ubuntu 20.04 e posteriores quanto o Amazon Linux 2 e posteriores estão

configurados para usar a interface de rede primária para o tráfego da Internet quando a instância é iniciada, conforme recomendado acima.

Conceitos básicos do EFA e MPI

Este tutorial ajuda a executar um cluster de instância habilitado para MPI e EFA para workloads de HPC. Neste tutorial, você seguirá as seguintes etapas:

Tópicos

- Etapa 1: Preparar um grupo de segurança habilitado para EFA
- Etapa 2: Iniciar uma instância temporária
- Etapa 3: Instalar o software EFA
- Etapa 4: (opcional) habilitar o Open MPI 5
- Etapa 5: (opcional) instalar o Intel MPI
- Etapa 6: desabilitar a proteção ptrace
- Etapa 7. Confirmar instalação
- Etapa 8: instalar a aplicação de HPC
- Etapa 9: criar uma AMI habilitada para EFA
- Etapa 10: executar instâncias habilitadas para EFA em um grupo de posicionamento de cluster
- Etapa 11: Encerrar a instância temporária
- Etapa 12: habilitar SSH sem senha

Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir cria um grupo de segurança que permite todo o tráfego de entrada e saída de e para si mesmo e que permite tráfego SSH de entrada de qualquer endereço IPv4 para conectividade SSH.

> **Important**
>
> Esse grupo de segurança deve ser usado apenas para fins de teste. Para seus ambientes de produção, recomendamos que você crie uma regra SSH de entrada que permita o tráfego somente do endereço IP do qual você está se conectando, como o endereço IP do seu computador ou uma variedade de endereços IP na sua rede local.

Para outros cenários, consulte Regras de grupo de segurança para diferentes casos de uso.

Para criar um grupo de segurança habilitado para EFA

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:
   a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como `EFA-enabled security group`.
   b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.
   c. Em VPC, selecione a VPC na qual você pretende executar suas instâncias habilitadas para EFA.
   d. Escolha Create security group (Criar grupo de segurança).
4. Selecione o grupo de segurança que você criou e, na guia Details (Detalhes), copie o Security group (Grupo de segurança).
5. Com o grupo de segurança ainda selecionado, escolha Actions (Ações), Edit inbound rules (Editar regras de entrada), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Source type (Tipo de origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
   d. Escolha Adicionar regra.
   e. Para Tipo, escolha SSH.
   f. Para Source type (Tipo de origem), escolha Anywhere-IPv4 (IPv4 em qualquer lugar).
   g. Escolha Salvar regras.
6. Na lista, selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.

d. Escolha Salvar regras.

Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que é possível usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual é possível executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=EFA-instance`).
4. Na seção Application and OS Images (Imagens de aplicação e sistema operacional), selecione uma AMI para um dos sistemas operacionais compatíveis.
5. Na seção Instance type (Tipo de instância), selecione um tipo de instância compatível.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:
   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.
   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolhaSelect existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.
   c. Expanda a seção Advanced network configuration (Configuração avançada de rede) e para Elastic Fabric Adapter (Adaptador de malha elástica), selecione Enable (Habilitar).
8. Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

Etapa 3: Instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric e pilha Open MPI que é necessário para oferecer compatibilidade com EFA em sua instância temporária.

As etapas diferem dependendo de como você planeja usar o EFA com Open MPI, com Intel MPI ou com Open MPI e Intel MPI.

Como instalar o software EFA

1. Conecte à instância que você iniciou. Para ter mais informações, consulte Conecte-se à sua instância do Linux.
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. esse processo pode demorar alguns minutos.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu e Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Reinicialize a instância e reconecte-se a ela.
4. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (`.tar.gz`). Para fazer download da última versão estável, use o seguinte comando:

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz
   ```

   Também é possível obter a versão mais recente substituindo o número da versão por `latest` no comando acima.
5. (Opcional) Verifique a autenticidade e a integridade do arquivo do EFA tarball (`.tar.gz`).

Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

> **Note**
>
> Como alternativa, se você preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte Verificar o instalador EFA usando uma soma de verificação.

a. Faça download da chave GPG pública e importe-a para seu pen-drive.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

```
$ gpg --fingerprint key_value
```

O comando deve retornar uma impressão digital idêntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.33.0.tar.gz.sig
```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
```

```
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir `Good signature` e a impressão digital corresponder à impressão digital retornada na etapa anterior, passe para a próxima etapa. Caso contrário, não execute o script de instalação do EFA e entre em contato com o AWS Support.

6. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ C:\> tar -xf aws-efa-installer-1.33.0.tar.gz && cd aws-efa-installer
```

7. Instale o software EFA. Dependendo de seu caso de uso, faça o seguinte.

> **Note**
>
> O EFA não oferece suporte ao NVIDIA GPUDirect com o SUSE Linux. Caso esteja usando SUSE Linux, você deverá especificar também a opção `--skip-kmod` para impedir a instalação do kmod. Por padrão, o SUSE Linux não permite módulos fora da árvore do kernel.

Open MPI and Intel MPI

Se planeja usar o EFA com Open MPI e Intel MPI, é necessário instalar o software EFA com Libfabric e Open MPI e concluir a Etapa 5: instalar o Intel MPI.

Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

> **Note**
>
> A partir do EFA 1.30.0, tanto o Open MPI 4 quanto o Open MPI 5 são instalados por padrão. Opcionalmente, você pode especificar a versão do Open MPI que deseja instalar. Para instalar somente o Open MPI 4, inclua `--mpi=openmpi4`. Para instalar somente o Open MPI 5, inclua `--mpi=openmpi5`. Para instalar os dois, omita a opção `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric está instalado em `/opt/amazon/efa`. O Open MPI 4 está instalado em `/opt/amazon/openmpi`. O Open MPI 5 está instalado em `/opt/amazon/openmpi5`.

Open MPI only

Se planeja usar o EFA somente com Open MPI, é necessário instalar o software EFA com Libfabric e Open MPI, podendo ignorar a Etapa 5: instalar o Intel MPI. Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

> **Note**
>
> A partir do EFA 1.30.0, tanto o Open MPI 4 quanto o Open MPI 5 são instalados por padrão. Opcionalmente, você pode especificar a versão do Open MPI que deseja instalar. Para instalar somente o Open MPI 4, inclua `--mpi=openmpi4`. Para instalar somente o Open MPI 5, inclua `--mpi=openmpi5`. Para instalar os dois, omita a opção `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric está instalado em `/opt/amazon/efa`. O Open MPI 4 está instalado em `/opt/amazon/openmpi`. O Open MPI 5 está instalado em `/opt/amazon/openmpi5`.

Intel MPI only

Se você pretende usar o EFA somente com Intel MPI, instale o software EFA sem Libfabric e Open MPI. Nesse caso, o Intel MPI usa o Libfabric incorporado. Se você optar por fazer isso, deverá concluir a Etapa 5: instalar o Intel MPI.

Para instalar o software EFA sem Libfabric e Open MPI, execute o comando a seguir.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.

Etapa 4: (opcional) habilitar o Open MPI 5

> **Note**
>
> Execute esta etapa somente se planeja usar o Open MPI 5.

A partir do EFA 1.30.0, tanto o Open MPI 4 quanto o Open MPI 5 são instalados por padrão. Como alternativa, você pode optar por instalar somente o Open MPI 4 ou o Open MPI 5.

Se você optou por instalar o Open MPI 5 na Etapa 3: instalar o software EFA e pretende usá-lo, execute as etapas a seguir para habilitá-lo.

Para habilitar o Open MPI 5

1. Adicione o Open MPI 5 à variável de ambiente PATH.

   ```
   $ module load openmpi5
   ```

2. Verifique se o Open MPI 5 está habilitado para uso.

   ```
   $ which mpicc
   ```

   O comando deve retornar o diretório de instalação do Open MPI 5: `/opt/amazon/openmpi5`.

3. (Opcional) Para garantir que o Open MPI 5 seja adicionado à variável de ambiente PATH sempre que a instância for iniciada, faça o seguinte:

   bash shell

   Adicione `module load openmpi5` a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

   csh and tcsh shells

   Adicione `module load openmpi5` a `/home/`*`username`*`/.cshrc`.

Se você precisar remover o Open MPI 5 da variável de ambiente PATH, execute o comando a seguir e remova o comando dos scripts de inicialização do shell.

```
$ module unload openmpi5
```

Etapa 5: (opcional) instalar o Intel MPI

> **Important**
>
> Execute esta etapa se planejar usar a Intel MPI. Se você planejar usa apenas Open MPI, ignore esta etapa.

A Intel MPI exige uma instalação adicional e a configuração de uma variável de ambiente.

Pré-requisito

Verifique se o usuário que executa as etapas a seguir tem permissões de sudo.

Para instalar a Intel MPI

1. Para baixar o script de instalação do Intel MPI, faça o seguinte
   a. Visite o site da Intel.
   b. Na seção da página da Web Intel MPI Library (Biblioteca Intel MPI), escolha o link para o instalador Intel MPI Library for Linux (Biblioteca MPI Intel para Linux) Offline.
2. Execute o script de instalação que você baixou na etapa anterior.

   ```
   $ sudo bash installation_script_name.sh
   ```
3. No instalador, escolha Accept & install (Aceitar e instalar).
4. Leia o Intel Improvement Program (Programa de melhoria da Intel), escolha a opção apropriada e, em seguida, escolha Begin Installation (Começar a instalação).
5. Quando a instalação terminar, escolha Close.
6. Por padrão, o Intel MPI usa o Libfabric integrado (interno). É possível configurar o Intel MPI para usar o Libfabric que acompanha o instalador do EFA. Normalmente, o instalador do EFA acompanha uma versão mais recente do Libfabric que o Intel MPI. Em alguns casos, o Libfabric que acompanha o instalador do EFA tem mais performance do que o Intel MPI. Para configurar o Intel MPI para usar o Libfabric que acompanha o instalador do EFA, siga um destes procedimentos, conforme o shell.

bash shells

Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_OFI_LIBRARY_INTERNAL=0
```

csh and tcsh shells

Adicione a instrução a seguir a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_LIBRARY_INTERNAL 0
```

7. Adicione o comando source a seguir ao script shell para obter o script `vars.sh` do diretório de instalação para configurar o ambiente do compilador sempre que a instância for iniciada. Dependendo de seu shell, faça o seguinte.

   bash shells

   Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

   csh and tcsh shells

   Adicione a instrução a seguir a /home/*username*/.cshrc.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.csh
   ```

8. Por padrão, se o EFA não estiver disponível devido a uma configuração incorreta, o Intel MPI assumirá como padrão a pilha de rede TCP/IP, podendo resultar em uma performance mais lenta da aplicação. Você pode evitar isso definindo `I_MPI_OFI_PROVIDER` como `efa`. Isso fará com que o Intel MPI apresente o seguinte erro, se o EFA não estiver disponível:

   ```
   Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
    error,
   MPIR_Init_thread (XXX).....:
   MPID_Init (XXXX)..............:
   ```

```
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX).............:
find_provider (XXXX)..........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Dependendo de seu shell, faça o seguinte.

bash shells

Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Adicione a instrução a seguir a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Por padrão, o Intel MPI não imprime informações de depuração. É possível especificar diferentes níveis de detalhamento para controlar as informações de depuração. Os valores possíveis (organizados em ordem pela quantidade de detalhes que fornecem) são: `0` (padrão), 1, 2, 3, 4, 5. O nível 1 e superiores imprimem `libfabric version` e `libfabric provider`. Use `libfabric version` para verificar se o Intel MPI está usando o Libfabric interno ou o Libfabric que acompanha o instalador do EFA. Se estiver usando o Libfabric interno, a versão terá o sufixo `impi`. Use `libfabric provider` para verificar se o Intel MPI está usando o EFA ou a rede TCP/IP. Se estiver usando o EFA, o valor será `efa`. Se estiver usando TCP/IP, o valor será `tcp;ofi_rxm`.

   Para habilitar as informações de depuração, siga um destes procedimentos, conforme seu shell.

   bash shells

   Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_DEBUG=value
   ```

csh and tcsh shells

Adicione a instrução a seguir a /home/*username*/.cshrc.

```
setenv I_MPI_DEBUG value
```

10. Por padrão, o Intel MPI usa a memória compartilhada do sistema operacional (shm) para comunicação intranós e usa Libfabric (ofi) somente para comunicação entre nós. Em geral, essa configuração fornece a melhor performance. Porém, em alguns casos, a malha Intel MPI shm pode fazer com que certas aplicações travem por tempo indeterminado.

    Para resolver esse problema, você pode forçar o Intel MPI a usar o Libfabric para comunicação intranós e entre nós. Para isso, faça o seguinte, de acordo com seu shell.

    bash shells

    Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

    ```
    export I_MPI_FABRICS=ofi
    ```

    csh and tcsh shells

    Adicione a instrução a seguir a /home/*username*/.cshrc.

    ```
    setenv I_MPI_FABRICS ofi
    ```

    > **Note**
    >
    > O provedor de Libfabric do EFA usa a memória compartilhada do sistema operacional para comunicação intranós. Isso significa que a configuração I_MPI_FABRICS em ofi fornece uma performance semelhante à configuração shm:ofi.

11. Saia da instância e faça login novamente.

Se você não usar mais a Intel MPI, remova as variáveis de ambiente dos scripts shell de startup.

Etapa 6: desabilitar a proteção ptrace

Para melhorar a performance da aplicação HPC, o Libfabric usa a memória local da instância para comunicações entre processos quando os processos estão sendo executados na mesma instância.

O recurso de memória compartilhada usa CMA (Cross Memory Attach), que não é compatível com a proteção ptrace. Se estiver usando uma distribuição Linux que tenha a proteção ptrace habilitada por padrão, como o Ubuntu, desabilite-a. Se a sua distribuição Linux não tiver a proteção ptrace habilitada por padrão, ignore esta etapa.

Como desabilitar a proteção ptrace

Execute um destes procedimentos:

- Para desabilitar temporariamente a proteção ptrace para fins de teste, execute o seguinte comando.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Para desabilitar permanentemente a proteção ptrace, adicione `kernel.yama.ptrace_scope = 0` a `/etc/sysctl.d/10-ptrace.conf` e reinicialize a instância.

Etapa 7. Confirmar instalação

Confirmar uma instalação bem-sucedida

1. Para confirmar se a Intel MPI foi instalada com êxito, execute o seguinte comando:

```
$ which mpicc
```

   - Para Open MPI, o caminho retornado deve incluir `/opt/amazon/`.
   - Para Intel MPI, o caminho retornado deve incluir `/opt/intel/`. Se o resultado esperado não for exibido, verifique se o script `vars.sh` da Intel MPI foi usado como origem.

2. Para confirmar se os componentes de software EFA e o Libfabric foram instalados com êxito, execute o comando a seguir.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
```

Etapa 8: instalar a aplicação de HPC

Instale a aplicação HPC na instância temporária. O procedimento de instalação varia dependendo da aplicação HPC específica. Para obter mais informações, consulte Manage software on your AL2 instance no Amazon Linux 2 User Guide.

> **Note**
>
> Pode ser necessário consultar a documentação da aplicação de HPC para obter instruções de instalação.

Etapa 9: criar uma AMI habilitada para EFA

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Image (Imagem), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
    a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
    b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.

c. Escolha Create Image (Criar imagem).

5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de `pending` para `available` antes de continuar para a próxima etapa.

Etapa 10: executar instâncias habilitadas para EFA em um grupo de posicionamento de cluster

Execute as instâncias habilitadas para EFA em um grupo de posicionamento de cluster usando a AMI habilitada para EFA criada na Etapa 7 e o grupo de segurança habilitado para EFA criado na Etapa 1.

> **Note**
>
> - Não é um requisito absoluto iniciar suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster. No entanto, recomendamos a execução de suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster ao executar as instâncias em um grupo de baixa latência em uma única zona de disponibilidade.
> - Para garantir que a capacidade esteja disponível à medida que escala as instâncias do cluster, é possível criar uma reserva de capacidade para o grupo de posicionamento de cluster. Para ter mais informações, consulte As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster.

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=EFA-instance`).
4. Na seção Application and OS Images (Imagens de aplicações e SO), selecione My AMIs (Minhas AMIs) e, em seguida, selecione a AMI que você criou na etapa anterior.
5. Na seção Instance type (Tipo de instância), selecione um tipo de instância compatível.

6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:
   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.
   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolhaSelect existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.
   c. Expanda a seção Advanced network configuration (Configuração avançada de rede) e para Elastic Fabric Adapter (Adaptador de malha elástica), selecione Enable (Habilitar).
8. (Opcional) Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. Na seção Advanced details (Detalhes avançados), para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento de cluster no qual iniciar as instâncias. Caso precise criar um novo grupo de posicionamento de cluster, escolha Create new placement group (Criar novo grupo de posicionamento).
10. No painel Summary (Resumo) à direita, em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA que você deseja iniciar e escolha Launch instance (Iniciar instância).

Etapa 11: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Etapa 12: habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, é necessário habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite `strictHostKeyChecking` e habilite `ForwardAgent` no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Gere um par de chaves RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   O par de chaves é criado no diretório do `$HOME/.ssh/`.
4. Altere as permissões da chave privada no nó líder.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:

   a. Conecte-se à instância.

   b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.
7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

   ```
   $ ssh member_node_private_ip
   ```

É necessário se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

Conceitos básicos do EFA e NCCL

A Nvidia Collective Communications Library (NCCL) é uma biblioteca de rotinas de comunicação coletiva padrão para várias GPUs em um único nó ou em vários nós. A NCCL pode ser usada com o EFA, o Libfabric e a MPI para oferecer suporte a várias workloads de machine learning. Para obter mais informações, consulte o site da NCCL.

As etapas a seguir ajudam você a começar a usar o EFA e o NCCL usando uma AMI base para um dos sistemas operacionais compatíveis.

> **Note**
>
> - Somente os tipos de instância `p3dn.24xlarge`, `p4d.24xlarge`, e `p5.48xlarge` são compatíveis.
> - Só há compatibilidade com AMIs básicas do Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9 e Ubuntu 20.04/22.04.
> - Somente a NCCL 2.4.2 e posterior são compatíveis com EFA.
> - Para obter mais informações sobre como executar workloads de machine learning com EFA e NCCL usando um AWS Deep Learning AMI, consulte Usando o EFA no DLAMI no Guia do desenvolvedor do AWS Deep Learning AMI.

Etapas

- Etapa 1: Preparar um grupo de segurança habilitado para EFA
- Etapa 2: Iniciar uma instância temporária
- Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN
- Etapa 4: instalar o GDRCopy
- Etapa 5: instalar o software EFA
- Etapa 6: instalar NCCL
- Etapa 7: instalar o plug-in aws-ofi-nccl

- Etapa 8: instalar os testes da NCCL
- Etapa 9: testar a configuração do EFA e da NCCL
- Etapa 10: instalar as aplicações de machine learning
- Etapa 11: criar um EFA e uma AMI habilitada para NCCL
- Etapa 12: encerrar a instância temporária
- Etapa 13: iniciar instâncias habilitadas para o EFA e para a NCCL em um grupo de posicionamento de cluster
- Etapa 14: habilitar SSH sem senha

Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir cria um grupo de segurança que permite todo o tráfego de entrada e saída de e para si mesmo e que permite tráfego SSH de entrada de qualquer endereço IPv4 para conectividade SSH.

> **Important**
>
> Esse grupo de segurança deve ser usado apenas para fins de teste. Para seus ambientes de produção, recomendamos que você crie uma regra SSH de entrada que permita o tráfego somente do endereço IP do qual você está se conectando, como o endereço IP do seu computador ou uma variedade de endereços IP na sua rede local.

Para outros cenários, consulte Regras de grupo de segurança para diferentes casos de uso.

Para criar um grupo de segurança habilitado para EFA

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:
   a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como `EFA-enabled security group`.
   b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.

c. Em VPC, selecione a VPC na qual você pretende executar suas instâncias habilitadas para EFA.

d. Escolha Create security group (Criar grupo de segurança).

4. Selecione o grupo de segurança que você criou e, na guia Details (Detalhes), copie o Security group (Grupo de segurança).

5. Com o grupo de segurança ainda selecionado, escolha Actions (Ações), Edit inbound rules (Editar regras de entrada), e faça o seguinte:

a. Escolha Adicionar regra.

b. Para Tipo, escolha Todo o tráfego.

c. Para Source type (Tipo de origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.

d. Escolha Adicionar regra.

e. Para Tipo, escolha SSH.

f. Para Source type (Tipo de origem), escolha Anywhere-IPv4 (IPv4 em qualquer lugar).

g. Escolha Salvar regras.

6. Na lista, selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída), e faça o seguinte:

a. Escolha Adicionar regra.

b. Para Tipo, escolha Todo o tráfego.

c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.

d. Escolha Salvar regras.

Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que é possível usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual é possível executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=`*`EFA-instance`*).
4. Na seção Application and OS Images (Imagens de aplicação e sistema operacional), selecione uma AMI para um dos sistemas operacionais compatíveis.
5. Na seção Tipo de instância, selecione `p3dn.24xlarge`, `p4d.24xlarge` ou `p5.48xlarge`.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:
   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.
   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolhaSelect existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.
   c. Expanda a seção Advanced network configuration (Configuração avançada de rede) e para Elastic Fabric Adapter (Adaptador de malha elástica), selecione Enable (Habilitar).
8. Na seção Storage (Armazenamento), configure os volumes conforme necessário.

   > **Note**
   >
   > É necessário provisionar um armazenamento adicional de 10 a 20 GiB para o Toolkit Nvidia CUDA. Se você não provisionar armazenamento suficiente, você receberá uma mensagem de erro `insufficient disk space` ao tentar instalar os drivers Nvidia e o Toolkit CUDA.

9. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

Amazon Linux 2

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Reconecte-se à sua instância depois de reinicializá-la.

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

   ```
   $ sudo yum groupinstall 'Development Tools' -y
   ```

3. Desabilite os drivers de código aberto `nouveau`.

   a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

      ```
      $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
      ```

   b. Adicione `nouveau` ao arquivo de lista de negação `/etc/modprobe.d/blacklist.conf` .

      ```
      $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
      blacklist vga16fb
      blacklist nouveau
      blacklist rivafb
      blacklist nvidiafb
      blacklist rivatv
      EOF
      ```

   c. Anexe `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` ao arquivo `grub` e recompile a configuração do Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicialize a instância e reconecte-se a ela.
5. Prepare os repositórios necessários

   a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

   ```
   $ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-7.noarch.rpm
   ```

   b. Instale a chave GPG pública do repositório CUDA.

   ```
   $ distribution='rhel7'
   ```

   c. Configure o repositório de rede CUDA e atualize o cache do repositório.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   d. (Somente kernel versão 5.10) Execute estas etapas somente se você estiver usando o Amazon Linux 2 com o kernel versão 5.10. Se você estiver usando o Amazon Linux 2 com o kernel versão 4.12, ignore estas etapas. Para verificar a versão do kernel, execute uname -r.

      i. Crie o arquivo de configuração do driver Nvidia chamado `/etc/dkms/nvidia.conf`.

      ```
      $ sudo mkdir -p /etc/dkms \
      && echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
       IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
       CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
      ```

      ii. (`p4d.24xlarge` e `p5.48xlarge` somente) Copie o arquivo de configuração do driver NVIDIA.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

   - `p3dn.24xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

   - `p4d.24xlarge` e `p5.48xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

7. Reinicialize a instância e reconecte-se a ela.
8. (`p4d.24xlarge` e `p5.48xlarge` somente) Inicie o serviço NVIDIA Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

   - Em shells bash, adicione as seguintes instruções a /home/*username*/`.bashrc` e /home/*username*/`.bash_profile`.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Em shells tcsh, adicione as seguintes instruções a /home/*username*/`.cshrc`.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

CentOS 7

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconecte-se à sua instância depois de reinicializá-la.

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y \
&& sudo yum install -y tar bzip2 make automake pciutils elfutils-libelf-devel
 libglvnd-devel iptables firewalld vim bind-utils
```

3. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto `nouveau`.

   a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
r)
```

   b. Adicione `nouveau` ao arquivo de lista de negação `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
```

```
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Abra o `/etc/default/grub` usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Recompile a configuração do Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicialize a instância e reconecte-se a ela.
5. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

b. Instale a chave GPG pública do repositório CUDA.

```
$ distribution='rhel7'
```

c. Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

6. Reinicialize a instância e reconecte-se a ela.

7. (`p4d.24xlarge` e `p5.48xlarge` somente) Inicie o serviço NVIDIA Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

8. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

   - Em shells bash, adicione as seguintes instruções a `/home/username/.bashrc` e `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

   - Em shells tcsh, adicione as seguintes instruções a `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

   O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

RHEL 7/8/9 and Rocky Linux 8/9

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconecte-se à sua instância depois de reinicializá-la.

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto `nouveau`.

   a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

   b. Adicione `nouveau` ao arquivo de lista de negação `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Abra o `/etc/default/grub` usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   d. Recompile a configuração do Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicialize a instância e reconecte-se a ela.
5. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

   a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

- RHEL 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

- RHEL 8 e Rocky Linux 8/9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

- RHEL 9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-9.noarch.rpm
```

b. Instale a chave GPG pública do repositório CUDA.

```
$ distribution=$(. /etc/os-release;echo $ID`rpm -E "%{?rhel}%{?fedora}"`)
```

c. Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

6. Reinicialize a instância e reconecte-se a ela.
7. (`p4d.24xlarge` e `p5.48xlarge` somente) Inicie o serviço NVIDIA Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

8. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

   - Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash_profile.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

9. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

   ```
   $ nvidia-smi -q | head
   ```

   O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

Ubuntu 20.04/22.04

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

   ```
   $ sudo apt-get update && sudo apt-get upgrade -y
   ```

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

   ```
   $ sudo apt-get update && sudo apt-get install build-essential -y
   ```

3. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto nouveau.

a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Adicione nouveau ao arquivo de lista de negação `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Abra o `/etc/default/grub` usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Recompile a configuração do Grub.

```
$ sudo update-grub
```

4. Reinicialize a instância e reconecte-se a ela.
5. Adicione o repositório CUDA e instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

   • `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
```

```
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- `p4d.24xlarge` e `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Reinicialize a instância e reconecte-se a ela.
7. (Somente `p4d.24xlarge` e `p5.48xlarge`) Instale o Nvidia Fabric Manager.

   a. É necessário instalar a versão do Nvidia Fabric Manager que corresponde à versão do módulo do kernel Nvidia que você instalou na etapa anterior.

      Execute o seguinte comando para determinar a versão do módulo do kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      A seguir está um exemplo de saída.

```
NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
 21:26:37 UTC 2021
```

No exemplo acima, a versão principal`450`do módulo do kernel foi instalado. Isso significa que você precisa instalar a versão do Nvidia Fabric Manager`450`.

b. Instale o Nvidia Fabric Manager. Execute o seguinte comando e especifique a versão principal identificada na etapa anterior.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Por exemplo, se a versão principal`450`do módulo do kernel foi instalado, use o seguinte comando para instalar a versão correspondente do Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Inicie o serviço e certifique-se de que ele seja iniciado automaticamente quando a instância for executada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

- Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
```

```
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

Etapa 4: instalar o GDRCopy

Instale o GDRCopy para melhorar a performance do Libfabric. Para obter mais informações sobre a GDRCopy, consulte o repositório do GDRCopy.

Amazon Linux 2, CentOS 7, RHEL 7/8/9, and Rocky Linux 8/9

Para instalar o GDRCopy

1. Instale as dependências necessárias.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Baixe e extraia o pacote do GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Crie o pacote RPM do GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Instale o pacote RPM do GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

Para instalar o GDRCopy

1. Instale as dependências necessárias.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Baixe e extraia o pacote do GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Crie o pacote RPM do GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Instale o pacote RPM do GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Etapa 5: instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric e pilha Open MPI que é necessário para oferecer compatibilidade com EFA em sua instância temporária.

Como instalar o software EFA

1. Conecte à instância que você iniciou. Para ter mais informações, consulte Conecte-se à sua instância do Linux.
2. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (`.tar.gz`). Para fazer download da última versão estável, use o seguinte comando:

```
$ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz
```

Também é possível obter a versão mais recente substituindo o número da versão por `latest` no comando acima.

3. (Opcional) Verifique a autenticidade e a integridade do arquivo do EFA tarball (`.tar.gz`).

   Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

   > **Note**
   >
   > Como alternativa, se você preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte Verificar o instalador EFA usando uma soma de verificação.

   a. Faça download da chave GPG pública e importe-a para seu pen-drive.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
   import aws-efa-installer.key
   ```

   O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

   b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

   ```
   $ gpg --fingerprint key_value
   ```

   O comando deve retornar uma impressão digital idêntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

   c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz.sig
    && gpg --verify ./aws-efa-installer-1.33.0.tar.gz.sig
   ```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir `Good signature` e a impressão digital corresponder à impressão digital retornada na etapa anterior, passe para a próxima etapa. Caso contrário, não execute o script de instalação do EFA e entre em contato com o AWS Support.

4. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ C:\> tar -xf aws-efa-installer-1.33.0.tar.gz && cd aws-efa-installer
```

5. Execute o script de instalação do software EFA.

> **Note**
>
> A partir do EFA 1.30.0, tanto o Open MPI 4 quanto o Open MPI 5 são instalados por padrão. A menos que você precise do Open MPI 5, recomendamos instalar somente o Open MPI 4. O comando a seguir instala somente o Open MPI 4. Se quiser instalar o Open MPI 4 e o Open MPI 5, remova `--mpi=openmpi4`.

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

O Libfabric é instalado no diretório `/opt/amazon/efa`, enquanto a Open MPI é instalada no diretório `/opt/amazon/openmpi`.

6. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.
7. Confirme se os componentes do software EFA foram instalados com sucesso.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

- `p3dn.24xlarge` com interface de rede única

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` e `p5.48xlarge` com várias interfaces de rede

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Etapa 6: instalar NCCL

Instale a NCCL. Para obter mais informações sobre a NCCL, consulte o Repositório da NCCL.

Como instalar a NCCL

1. Navegue até o diretório `/opt`.

```
$ cd /opt
```

2. Clone o repositório oficial da NCCL para a instância e navegue até o repositório local clonado.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Compile e instale a NCCL e especifique o diretório de instalação do CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Etapa 7: instalar o plug-in aws-ofi-nccl

O plugin aws-ofi-nccl mapeia as APIs de transporte orientadas para a conexão da NCCL para a interface de conexão menos confiável do Libfabric. Isso permite usar o Libfabric como um provedor de rede ao executar aplicações baseadas na NCCL. Para obter mais informações sobre o plugin aws-ofi-nccl, consulte o Repositório do aws-ofi-nccl.

Como instalar o plugin aws-ofi-nccl

1. Navegue até o diretório inicial.

```
$ cd $HOME
```

2. (Somente Amazon Linux 2 e Ubuntu) Instale os utilitários necessários.

   - Amazon Linux 2

```
$ sudo yum install hwloc-devel
```

   - Ubuntu 20.04

```
$ sudo apt-get install libhwloc-dev
```

3. Baixe os arquivos do plug-in aws-ofi-nccl. Os arquivos estão empacotados em um arquivo compactado tarball (`.tar.gz`).

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.9.2-aws/aws-ofi-nccl-1.9.2-aws.tar.gz
```

4. Extraia os arquivos do arquivo compactado .tar.gz e navegue para o diretório extraído.

```
$ tar -xf aws-ofi-nccl-1.9.2-aws.tar.gz && cd aws-ofi-nccl-1.9.2-aws
```

5. Para gerar os arquivos make, execute o script `configure` e especifique os diretórios de instalação da MPI, do Libfabric, da NCCL e do CUDA.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \
--with-libfabric=/opt/amazon/efa \
--with-cuda=/usr/local/cuda \
--enable-platform-aws
```

6. Adicione o diretório Open MPI à variável `PATH`.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Instale o plugin aws-ofi-nccl.

```
$ make && sudo make install
```

Etapa 8: instalar os testes da NCCL

Instale os testes da NCCL. Os testes da NCCL permitem confirmar se a NCCL está instalada adequadamente se ela está funcionando conforme esperado. Para obter mais informações sobre os testes da NCCL, consulte o Repositório nccl-tests.

Como instalar os testes da NCCL

1. Navegue até o diretório inicial.

```
$ cd $HOME
```

2. Clone o repositório oficial de nccl-tests para a instância e navegue até o repositório local clonado.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Adicione o diretório do Libfabric à variável `LD_LIBRARY_PATH`.

   - Amazon Linux, Amazon Linux 2, RHEL , Rocky Linux 8/9 e CentOS

     ```
     $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
     ```

   - Ubuntu

     ```
     $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
     ```

4. Instale os testes da NCCL e especifique os diretórios de instalação da MPI da NCCL e do CUDA.

   ```
   $ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
   local/cuda
   ```

Etapa 9: testar a configuração do EFA e da NCCL

Execute um teste para verificar se a instância temporária está configurada adequadamente para o EFA e para a NCCL.

Como testar a configuração do EFA e da NCCL

1. Crie um arquivo de host que especifique os hosts nos quais executar os testes. O comando a seguir cria um arquivo de host chamado `my-hosts` que inclui uma referência à própria instância.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
hosts
```

2. Execute o teste e especifique o arquivo de host (`--hostfile`) e o número de GPUs a serem usadas (`-n`). O comando a seguir executa o teste `all_reduce_perf` em 8 GPUs na própria instância e especifica as variáveis de ambiente a seguir.

   - `FI_EFA_USE_DEVICE_RDMA=1`: (somente `p4d.24xlarge`) usa a funcionalidade RDMA do dispositivo para transferência unilateral e bilateral.
   - `NCCL_DEBUG=INFO` habilita a saída de depuração detalhada. Também é possível especificar `VERSION` para imprimir somente a versão da NCCL no início do teste ou `WARN` para receber somente mensagens de erro.

   Para obter mais informações sobre os argumentos de teste da NCCL, consulte o README NCCL Tests no repositório oficial de nccl-tests.

   - `p3dn.24xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
   lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
   -x NCCL_DEBUG=INFO \
   --hostfile my-hosts -n 8 -N 8 \
   --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
    none \
   $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
   ```

   - `p4d.24xlarge` e `p5.48xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   -x FI_EFA_USE_DEVICE_RDMA=1 \
   -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
   lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
   -x NCCL_DEBUG=INFO \
   --hostfile my-hosts -n 8 -N 8 \
   --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
    none \
   ```

```
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. É possível confirmar se EFA está ativo como o provedor subjacente para NCCL quando o log `NCCL_DEBUG` é impresso.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

As seguintes informações adicionais são exibidas ao usar uma instância `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Etapa 10: instalar as aplicações de machine learning

Instale as aplicações de machine learning na instância temporária. O procedimento de instalação varia dependendo da aplicação de machine learning específica. Para obter mais informações sobre instalação de software em sua instância do Linux, consulte Manage software on your Amazon Linux 2 instance.

> **Note**
>
> Pode ser necessário consultar a documentação da aplicação de machine learning para obter instruções de instalação.

Etapa 11: criar um EFA e uma AMI habilitada para NCCL

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Image (Imagem), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:

a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
c. Escolha Create Image (Criar imagem).

5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de `pending` para `available` antes de continuar para a próxima etapa.

Etapa 12: encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Etapa 13: iniciar instâncias habilitadas para o EFA e para a NCCL em um grupo de posicionamento de cluster

Execute as instâncias habilitadas para EFA em um grupo de posicionamento de cluster usando a AMI habilitada para EFA criada e o grupo de segurança habilitado para EFA criado anteriormente.

> **Note**
>
> - Não é um requisito absoluto iniciar suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster. No entanto, recomendamos a execução de suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster ao executar as instâncias em um grupo de baixa latência em uma única zona de disponibilidade.
> - Para garantir que a capacidade esteja disponível à medida que escala as instâncias do cluster, é possível criar uma reserva de capacidade para o grupo de posicionamento de

cluster. Para ter mais informações, consulte As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster.

New console

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=EFA-instance`).
4. Na seção Application and OS Images (Imagens de aplicações e SO), selecione My AMIs (Minhas AMIs) e, em seguida, selecione a AMI que você criou na etapa anterior.
5. Na seção Instance type (Tipo de instância), selecione `p3dn.24xlarge` ou `p4d.24xlarge`.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:
   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.
   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolhaSelect existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.
   c. Expanda a seção Advanced network configuration (Configuração avançada de rede) e para Elastic Fabric Adapter (Adaptador de malha elástica), selecione Enable (Habilitar).
8. (Opcional) Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. Na seção Advanced details (Detalhes avançados), para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento de cluster no qual iniciar a instância. Caso precise criar um novo grupo de posicionamento de cluster, escolha Create new placement group (Criar novo grupo de posicionamento).
10. No painel Summary (Resumo) à direita, em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA que você deseja iniciar e escolha Launch instance (Iniciar instância).

Old console

Para executar as instâncias habilitadas para EFA e NCCL em um grupo de posicionamento de cluster.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Launch Instance (Executar instância).
3. Na página Choose an AMI (Escolher uma AMI), selecione My AMIs (Minhas AMIs), localize a AMI criada anteriormente e escolha Select (Selecionar).
4. Na página Choose an Instance Type (Escolher um tipo de instância), escolha p3dn.24xlarge e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
   a. Em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA e NCCL que você deseja executar.
   b. Em Network (Rede) e Subnet (Sub-rede), selecione a VPC e a sub-rede na qual executar as instâncias.
   c. Em Placement group, selecione Add instance to placement group (Adicionar instância ao placement group).
   d. Em Placement group name (Nome do grupo de posicionamento), selecione Add to a new placement group (Adicionar a um novo grupo de posicionamento) e, em seguida, insira um nome descritivo para o grupo de posicionamento. Em seguida, em Placement group strategy (Estratégia do grupo de posicionamento), selecione cluster.
   e. Para EFA, escolha Enable (Habilitar).
   f. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede). Como opção, é possível especificar um endereço IPv4 principal e um ou mais endereços IPv4 secundários. Se estiver executando a instância em uma sub-rede que tenha um bloco CIDR IPv6 associado, será possível especificar opcionalmente um endereço IPv6 principal e um ou mais endereços IPv6 secundários.
   g. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).

7. Na página Add Tags (Adicionar tags), especifique tags para as instâncias, como nome amigável, e selecione Next: Configure Security Group (Próximo: Configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou anteriormente.
9. Escolha Review and Launch.
10. Na página Revisar execução da instância, reveja as configurações, e escolha Executar para escolher um par de chaves e executar a instâncias.

Etapa 14: habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, é necessário habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite `strictHostKeyChecking` e habilite `ForwardAgent` no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:
   a. Conecte-se à instância.
   b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.
7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

   ```
   $ ssh member_node_private_ip
   ```

   É necessário se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

Trabalhar com EFA

É possível criar, usar e gerenciar um EFA como qualquer outra interface de rede elástica no Amazon EC2. No entanto, ao contrário das interfaces de rede elástica, os EFAs não podem ser anexados ou desanexados de uma instância em um estado em execução.

Requisitos do EFA

Para usar um EFA, é necessário fazer o seguinte:

- Escolha um dos tipos de instância compatíveis.
- Use uma AMI para um dos sistemas operacionais compatíveis.
- Instale os componentes de software de EFA. Para ter mais informações, consulte Etapa 3: Instalar o software EFA e Etapa 5: (opcional) instalar o Intel MPI.
- Use um grupo de segurança que permite todo o tráfego de entrada e saída de e para o próprio grupo de segurança. Para obter mais informações, consulte Etapa 1: Preparar um grupo de segurança habilitado para EFA.

Tópicos

- Criar um EFA.
- Associar um EFA a uma instância interrompida

- Associar um EFA ao executar uma instância
- Adicionar um EFA a um modelo de execução
- Gerenciar endereços IP para um EFA
- Alterar o grupo de segurança para um EFA
- Desanexar um EFA
- Visualizar EFAs
- Excluir um EFA

Criar um EFA.

É possível criar um EFA em uma sub-rede de uma VPC. Você não pode mover o EFA para outra sub-rede depois que ela é criada e só pode anexá-la a instâncias interrompidas na mesma zona de disponibilidade.

Para criar um novo EFA usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Escolha Criar interface de rede.
4. Em Description (Descrição), insira um nome descritivo para o EFA.
5. Para Subnet (Sub-rede), selecione a sub-rede na qual criar o EFA.
6. Para Private IP (IP privado), insira o endereço IPv4 privado principal. Se você não especificar um endereço IPv4,selecionaremos um endereço IPv4 privado disponível da sub-rede selecionada.
7. (Somente IPv6) Se você tiver selecionado uma sub-rede com um bloco CIDR IPv6 associado, é possível especificar um endereço IPv6 no campo IP IPv6.
8. Para Security groups, selecione um ou mais security groups.
9. Para EFA, selecione Enabled (Habilitado).
10. Escolha Yes, Create.

Para criar um novo EFA usando a AWS CLI

Use o comando create-network-interface e, para `interface-type`, especifique `efa`, conforme mostrado no exemplo a seguir.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --
description example_efa --interface-type efa
```

Associar um EFA a uma instância interrompida

É possível anexar um EFA a qualquer instância compatível que esteja no estado `stopped`. É possível anexar um EFA a uma instância que esteja no estado `running`. Para obter mais informações sobre os tipos de instâncias compatíveis, consulte Tipos de instâncias compatíveis.

Anexe um EFA a uma instância da mesma forma como você anexa uma interface de rede a uma instância. Para obter mais informações, consulte Anexar uma interface de rede a uma instância..

Associar um EFA ao executar uma instância

Para anexar um EFA existente ao iniciar uma instância (AWS CLI)

Use o comando run-instances e, para NetworkInterfaceId, especifique o ID do EFA, conforme mostrado no exemplo a seguir.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Para anexar um novo EFA ao iniciar uma instância (AWS CLI)

Use o comando run-instances e, para InterfaceType, especifique o ID do `efa`, conforme mostrado no exemplo a seguir.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Adicionar um EFA a um modelo de execução

É possível criar um modelo de execução que contenha informações de configuração necessárias para executar instâncias habilitadas para EFA. Para criar um modelo de execução habilitado para EFA, crie um novo modelo de execução e especifique um tipo de instância compatível, sua AMI habilitada para EFA e um grupo de segurança habilitado para EFA. Para ter mais informações, consulte Conceitos básicos do EFA e MPI.

É possível aproveitar modelos de inicialização para executar instâncias habilitadas para EFA com outros produtos da AWS, como AWS Batch ou AWS ParallelCluster.

Para obter mais informações sobre como criar modelos do execução, consulte Criar um modelo de inicialização.

Gerenciar endereços IP para um EFA

É possível alterar os endereços IP associados a um EFA. Se tiver um endereço IP elástico, será possível associá-lo a um EFA. Se seu EFA estiver provisionado em uma sub-rede que tenha um bloco CIDR IPv6 associado, será possível atribuir um ou mais endereços IPv6 ao EFA.

Você atribui um endereço IP elástico (IPv4) e IPv6 a um EFA da mesma forma como atribui um endereço IP a uma interface de rede elástica. Para obter mais informações, consulte Gerenciar endereços IP.

Alterar o grupo de segurança para um EFA

É possível alterar o grupo de segurança associado a um EFA. Para habilitar a funcionalidade de desvio do sistema operacional, o EFA deve ser um membro de um grupo de segurança que permita todo o tráfego de entrada e saída de e para o próprio grupo de segurança.

É possível alterar o grupo de segurança associado a um EFA da mesma forma como altera o grupo de segurança associado a uma interface de rede elástica. Para obter mais informações, consulte Alterar o grupo de segurança.

Desanexar um EFA

Para desanexar um EFA de uma instância, primeiro é necessário parar a instância. Você não pode desanexar um EFA de uma instância que está em estado de execução.

Você desanexa um EFA de uma instância da mesma maneira como desanexa uma interface de rede elástica de uma instância. Para obter mais informações, consulte Desanexar uma interface de rede de uma instância.

Visualizar EFAs

É possível ver todos os EFAs da sua conta.

Você visualiza EFAs da mesma maneira como visualiza interfaces de rede elástica. Para obter mais informações, consulte Visualizar detalhes sobre uma interface de rede.

Excluir um EFA

Para excluir um EFA, é necessário primeiro separá-lo da instância. Você não pode excluir um EFA enquanto está anexado a uma instância.

Você exclui EFAs da mesma maneira como visualiza interfaces de rede elástica. Para ter mais informações, consulte Excluir uma interface de rede.

Monitorar um EFA

É possível usar os seguintes recursos para monitorar a performance dos seus Elastic Fabric Adapters.

Logs de fluxo do Amazon VPC

É possível criar um log de fluxo da Amazon VPC para capturar informações sobre o tráfego de entrada e saída de um EFA. Os dados de log de fluxo podem ser publicados no Amazon CloudWatch Logs e no Amazon S3. Após criar um log de fluxo, será possível recuperar e visualizar seus dados no destino selecionado. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Você cria um log de fluxo para um EFA da mesma forma como cria um log de fluxo para uma interface de rede elástica. Para mais informações, consulte Criar um log de fluxo no Guia do usuário da Amazon VPC.

Nas entradas do log de fluxo, o tráfego do EFA é identificado por `srcAddress` e `destAddress`, ambos formatados como endereços MAC, conforme mostrado no exemplo a seguir.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

O Amazon CloudWatch fornece métricas que permitem monitorar os EFAs em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Para ter mais informações, consulte Monitorar instâncias usando o CloudWatch.

Verificar o instalador EFA usando uma soma de verificação

Como opção, é possível verificar o tarball EFA (arquivo .tar.gz) usando uma soma de verificação MD5 ou SHA256. Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada.

Como verificar o tarball

Use o utilitário md5sum para a soma de verificação MD5 ou o utilitário sha256sum para a soma de verificação SHA256 e especifique o nome do arquivo tarball. Execute o comando a partir do diretório no qual salvou o arquivo tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Os comandos devem retornar um valor de soma de verificação no formato a seguir.

```
checksum_value tarball_filename.tar.gz
```

Compare o valor de soma de verificação retornado pelo comando com o valor de soma de verificação fornecido na tabela abaixo. Se as somas de verificação corresponderem, então é seguro executar o script de instalação. Se as somas de verificação não corresponderem, não execute o script de instalação e entre em contato com o AWS Support.

Por exemplo, o comando a seguir verifica o tarball EFA 1.9.4 usando a soma de verificação SHA256.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Resultado do exemplo:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

A tabela a seguir lista as somas de verificação para versões recentes do EFA.

Versão	Faça download do URL	Somas de verificação
EFA 1.33.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz	MD5: `e2f61fccbcaa11e2ccfddd3660522276` SHA256: `0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce`
EFA 1.32.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz	MD5: `db8d65cc028d8d08b5a9f2d88881c1b1` SHA256: `5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66`
EFA 1.31.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.31.0.tar.gz	MD5: `856352f12bef2ccbadcd75e35aa52aaf` SHA256: `943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf`
EFA 1.30.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.30.0.tar.gz	MD5: `31f48e1a47fe93ede8ebd273fb747358` SHA256: `876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a`
EFA 1.29.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.1.tar.gz	MD5: `e1872ca815d752c1d7c2b5c175e52a16` SHA256: `178b263b8c25845b63dc93b25bcdff5870df`

Versão	Faça download do URL	Somas de verificação
		5204ec509af26f43e8 d283488744
EFA 1.29.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.0.tar.gz	MD5: 39d06a002154d94cd9 82ed348133f385 SHA256: 836655f87015547e73 3e7d9f7c760e4e2469 7f8bbc261bb5f3560a bd4206bc36
EFA 1.28.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.28.0.tar.gz	MD5: 9dc13b744666582260 5e66febe074035 SHA256: 2e625d2d6d3e073b51 78e8e861891273d896 b66d03cb1a32244fd5 6789f1c435
EFA 1.27.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.27.0.tar.gz	MD5: 98bfb515ea3e8d93f5 54020f3837fa15 SHA256: 1d49a97b0bf8d964d9 1652a79ac851f2550e 33a5bf9d0cf86ec935 7ff6579aa3
EFA 1.26.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.1.tar.gz	MD5: 884e74671fdef47255 01f7cd2d451d0c SHA256: c616994c924f54ebfa bfab32b7fe8ac56947 fae00a0ff453d975e2 98d174fc96

Versão	Faça download do URL	Somas de verificação
EFA 1.26.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.0.tar.gz	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.1.tar.gz	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.0.tar.gz	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.1.tar.gz	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62

Versão	Faça download do URL	Somas de verificação
EFA 1.24.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.0.tar.gz	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA 1.23.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.1.tar.gz	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.0.tar.gz	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.1.tar.gz	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665

Versão	Faça download do URL	Somas de verificação
EFA 1.22.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.0.tar.gz	MD5: `8f100c93dc8ab519c2aeb5dab89e98f8` SHA256: `f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a`
EFA 1.21.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.21.0.tar.gz	MD5: `959ccc3a4347461909ec02ed3ba7c372` SHA256: `c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050`
EFA 1.20.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.20.0.tar.gz	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`
EFA 1.19.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.19.0.tar.gz	MD5: `2fd45324953347ec5518da7e3fefa0ec` SHA256: `99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709`

Versão	Faça download do URL	Somas de verificação
EFA 1.18.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.18.0.tar.gz	MD5: `fc2571a72f5d3c7b7b576ce2de38d91e` SHA256: `acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6`
EFA 1.17.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.3.tar.gz	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.2.tar.gz	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`
EFA 1.17.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.1.tar.gz	MD5: `733ae2cfc9d14b52017eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f`

Versão	Faça download do URL	Somas de verificação
EFA 1.17.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.0.tar.gz	MD5: d430fc841563c11c3805c5f82a4746b1 SHA256: 75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d
EFA 1.16.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.16.0.tar.gz	MD5: 399548d3b0d2e812d74dd67937b696b4 SHA256: cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b
EFA 1.15.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.2.tar.gz	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49
EFA 1.15.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.1.tar.gz	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7

Versão	Faça download do URL	Somas de verificação
EFA 1.15.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.0.tar.gz	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA 1.14.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.1.tar.gz	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.0.tar.gz	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA 1.13.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1

Versão	Faça download do URL	Somas de verificação
EFA 1.12.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172
EFA 1.12.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59

Versão	Faça download do URL	Somas de verificação
EFA 1.11.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz	MD5: `2376cf18d1353a4551e35c33d269c404` SHA256: `a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371`
EFA 1.11.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`
EFA 1.11.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz	MD5: `7d9058e010ad65bf2e14259214a36949` SHA256: `7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa`
EFA 1.10.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz	MD5: `78521d3d668be22976f46c6fecc7b730` SHA256: `61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4`

Versão	Faça download do URL	Somas de verificação
EFA 1.10.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz	MD5: `46f73f5a7afe41b4bb918c81888fefa9` SHA256: `136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282`
EFA 1.9.5	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz	MD5: `95edb8a209c18ba8d250409846eb6ef4` SHA256: `a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25`
EFA 1.9.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz	MD5: `f26dd5c350422c1a985e35947fa5aa28` SHA256: `1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14`
EFA 1.9.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`

Versão	Faça download do URL	Somas de verificação
EFA 1.8.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Topologia da instância do Amazon EC2

A descrição da topologia de instâncias fornece uma visão hierárquica da proximidade relativa entre as instâncias. É possível usar essas informações para gerenciar as infraestruturas de computação de alta performance (HPC) e de machine learning (ML) em escala e, ao mesmo tempo, otimizar o posicionamento dos trabalhos. Os trabalhos de HPC e ML são sensíveis a latência e throughput. É possível usar a topologia de instâncias para detectar a localização das instâncias e depois usar essas informações para otimizar os trabalhos de HPC e ML executando-os em instâncias fisicamente mais próximas umas das outras.

A topologia de instâncias pode ser usada para detectar a localização das instâncias existentes, mas não para decidir se uma nova instância fisicamente próxima a uma instância existente será iniciada. Para influenciar o posicionamento da instância, é possível usar o As reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster.

Definição de preço

Não há custo adicional para descrever sua topologia de instâncias.

Conteúdo

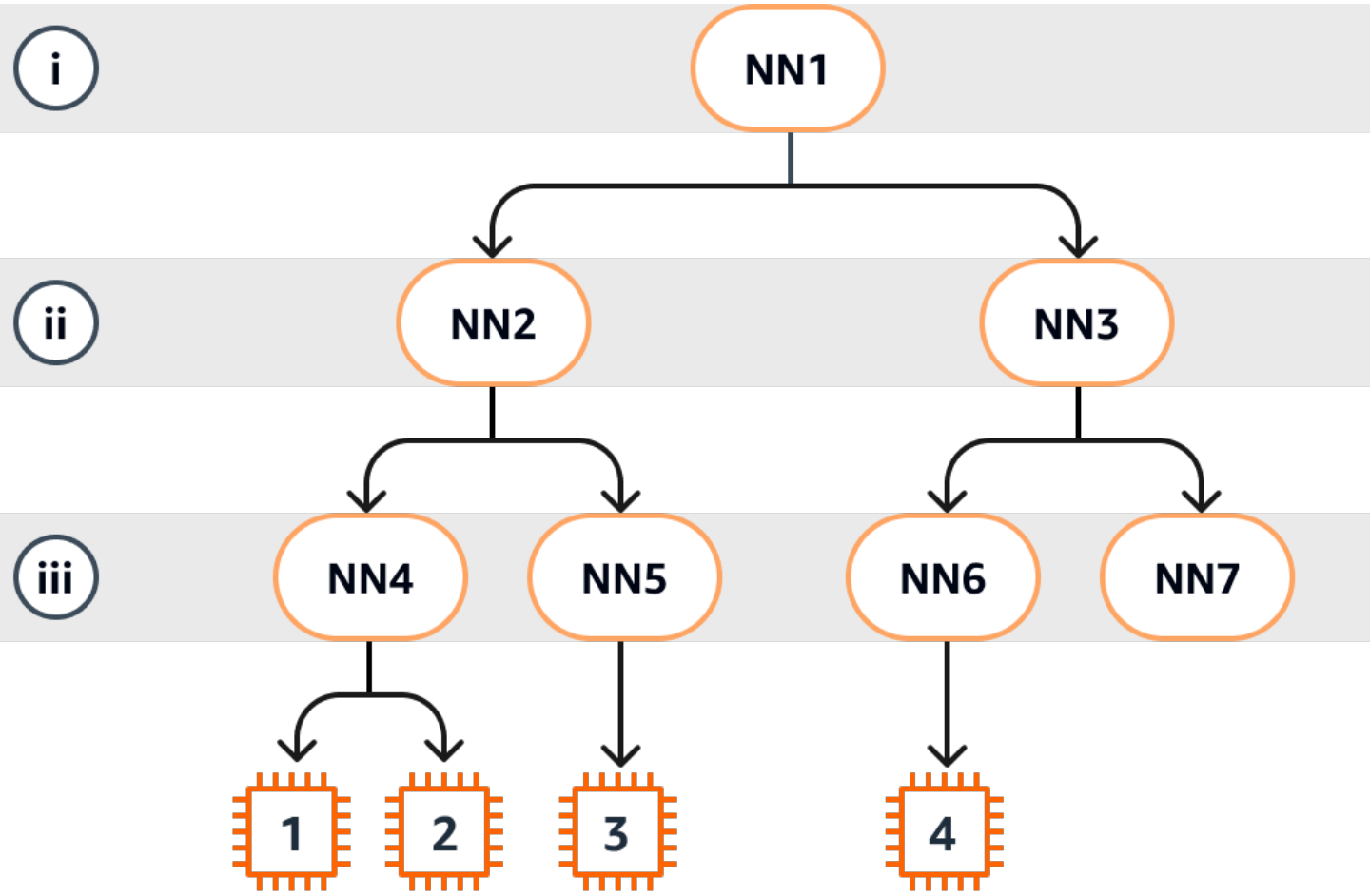
- Como a topologia de instâncias funciona
- Pré-requisitos da topologia de instâncias
- Exemplos de topologia de instâncias do Amazon EC2

Como a topologia de instâncias funciona

Cada instância do EC2 se conecta a um conjunto de nós. Um conjunto de nós compreende três nós de rede, com cada nó representando uma camada diferente na rede da AWS. As camadas da rede são organizadas em uma hierarquia de três ou mais camadas. O conjunto de nós fornece a visão de cima para baixo dessa hierarquia, sendo a camada inferior a que está conectada mais perto de uma instância.

As informações sobre o conjunto de nós são chamadas de topologia de instâncias e são retornadas pela API.

O diagrama a seguir fornece uma representação visual que você pode usar para entender a topologia de instâncias. Os nós da rede são identificados como NN1 – NN7. Os números i, ii e iii identificam as camadas de rede. Os números 1, 2, 3 e 4 identificam as instâncias do EC2. As instâncias se conectam a um nó na camada inferior, identificado por iii. Mais de uma instância podem se conectar ao mesmo nó.



Neste exemplo:

- A instância 1 se conecta ao nó de rede 4 (NN4) na camada iii. O NN4 se conecta ao nó de rede 2 (NN2) na camada ii e o NN2 se conecta ao nó de rede 1 (NN1) na camada i, que é o topo da hierarquia da rede neste exemplo. O conjunto de nós de rede compreende NN1, NN2 e NN4, expressos hierarquicamente das camadas superiores até a camada mais inferior.
- A instância 2 também se conecta ao nó de rede 4 (NN4). A instância 1 e a instância 2 compartilham o mesmo conjunto de nós de rede: NN1, NN2 e NN4.
- A instância 3 se conecta ao nó de rede 5 (NN5). O nó NN5 se conecta ao nó NN2, e o nó NN2 se conecta ao nó NN1. O conjunto de nós de rede para a instância 3 é NN1, NN2 e NN5.
- A instância 4 se conecta ao nó de rede 6 (NN6). Seu conjunto de nós de rede é NN1, NN3 e NN6.

Ao considerar a proximidade das instâncias 1, 2 e 3, as instâncias 1 e 2 estão mais próximas uma da outra porque se conectam ao mesmo nó de rede (NN4), enquanto a instância 3 está mais distante porque se conecta a um nó de rede diferente (NN5).

Ao considerar a proximidade de todas as instâncias neste diagrama, as instâncias 1, 2 e 3 estão mais próximas umas das outras do que da instância 4 porque compartilham NN2 em seu conjunto de nós de rede.

Como regra geral, se o nó de rede conectado a quaisquer duas instâncias for o mesmo, essas instâncias estarão fisicamente próximas uma da outra, como é o caso das instâncias 1 e 2. Além disso, quanto menor o número de saltos entre os nós de rede, mais próximas umas das outras as instâncias estão. Por exemplo, as instâncias 1 e 3 têm menos saltos para um nó de rede comum (NN2) do que para o nó de rede (NN1) que têm em comum com a instância 4 e, portanto, estão mais próximas umas das outras do que da instância 4.

Não há instâncias sendo executadas no nó de rede 7 (NN7) neste exemplo e, portanto, a saída da API não incluirá NN7.

Como interpretar a saída

Você obtém as informações da topologia de instâncias usando a API DescribeInstanceTopology. A saída fornece uma visão hierárquica da topologia de rede subjacente de uma instância.

O exemplo de saída a seguir corresponde às informações de topologia de rede das quatro instâncias no diagrama anterior. Os comentários são incluídos na saída do exemplo para os propósitos deste exemplo.

É importante observar as seguintes informações na saída:

- `NetworkNodes` descreve o conjunto de nós de rede de uma instância.
- Em cada conjunto de nós de rede, os nós de rede são listados em ordem hierárquica de cima para baixo.
- O nó de rede conectado à instância é o último nó de rede na lista (a camada inferior).
- Para descobrir quais instâncias estão próximas umas das outras, primeiro encontre os nós de rede comuns na camada inferior. Se não houver nós de rede comuns na camada inferior, encontre nós de rede comuns nas camadas superiores.

Na saída de exemplo a seguir, `i-1111111111example` e `i-2222222222example` estão localizadas mais próximas uma da outra em comparação com as outras instâncias neste exemplo porque elas têm o nó de rede `nn-4444444444example` em comum na camada inferior.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
```

```
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Limitações

As limitações a seguir se aplicam a:

- As instâncias devem estar no estado `running`.
- Cada visualização da topologia da instância é exclusiva por conta.
- O AWS Management Console não oferece suporte à a visualização da topologia de instâncias.

Pré-requisitos da topologia de instâncias

Antes de descrever a topologia de instâncias para suas instâncias, certifique-se de que elas atendam aos seguintes requisitos.

Requisitos para descrever a topologia das suas instâncias

- Regiões da AWS
- Tipos de instância
- Estado da instância
- Permissão do IAM

Regiões da AWS

Regiões da AWS compatíveis:

- Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon)
- Ásia-Pacífico (Seul), Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Europa (Frankfurt), Europa (Irlanda), Europa (Estocolmo)

Tipos de instância

Tipos de instâncias compatíveis:

- `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
- `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge`
- `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge`

Para ver os tipos de instância disponíveis em uma região específica

Os tipos de instância disponíveis variam de acordo com a região. Para ver se um tipo de instância está disponível em uma região, use o comando describe-instance-types-offerings com o parâmetro `--region`. Use o parâmetro `--filters` para incluir no escopo dos resultados a família da instância ou o tipo de instância em que você está interessado e o parâmetro `--query` para incluir no escopo da saída o valor de `InstanceType`.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2 \
    --filters 'Name=instance-type, Values=trn1*' \
```

```
    --query 'InstanceTypeOfferings[].InstanceType'
```

Saída esperada

```
[
    "trn1.2xlarge",
    "trn1.32xlarge",
    "trn1n.32xlarge"
]
```

Estado da instância

As instâncias devem estar no estado `running`. Não é possível obter informações sobre a topologia da instância para instâncias em outro estado.

Permissão do IAM

Sua identidade do IAM (usuário, grupo de usuários ou perfil) exige a seguinte permissão do IAM:

- `ec2:DescribeInstanceTopology`

Exemplos de topologia de instâncias do Amazon EC2

É possível usar o comando describe-instance-topology da CLI para descrever a topologia de instâncias para suas instâncias do EC2.

Quando você usa o comando `describe-instance-topology` sem parâmetros ou filtros, a resposta inclui todas as instâncias que correspondem aos tipos de instância compatíveis com esse comando na região especificada. Você pode especificar a região incluindo o parâmetro `--region` ou definindo uma região padrão. Para obter mais informações sobre a definição de uma região padrão, consulte Especificar a região para um recurso.

Você pode incluir parâmetros para retornar instâncias que correspondam aos IDs de instância ou aos nomes de grupos de posicionamento especificados. Você também pode incluir filtros para retornar instâncias que correspondam a um determinado tipo ou família de instâncias, ou a instâncias em uma zona de disponibilidade ou zona local específica. Você pode incluir um único parâmetro ou filtro, ou uma combinação de parâmetros e filtros.

A saída é paginada, com até 20 instâncias por página por padrão. Você pode especificar até 100 instâncias por página usando o parâmetro `--max-results`.

Para obter mais informações, consulte describe-instance-topology na Referência de comandos da AWS CLI.

Permissões obrigatórias

A permissão a seguir é necessária para descrever a topologia de instâncias:

- `ec2:DescribeInstanceTopology`

Exemplos

- Exemplo 1: sem parâmetros ou filtros
- Exemplo 2: filtro de tipo de instância
  - Exemplo 2a: filtro de correspondência exata para um tipo de instância especificado
  - Exemplo 2b: filtro com curinga para uma família de instâncias
  - Exemplo 2c: filtros combinados de família de instâncias e correspondência exata
- Exemplo 3: filtro de zone-id
  - Exemplo 3a: filtro de zona de disponibilidade
  - Exemplo 3b: filtro de zona local
  - Exemplo 3c: filtros combinados de zona de disponibilidade e zona local
- Exemplo 4: filtros combinados de instance-type e zone-id
- Exemplo 5: parâmetro do nome do grupo de posicionamento
- Exemplo 6: IDs de instância

Exemplo 1: sem parâmetros ou filtros

Para descrever a topologia da instância de todas as suas instâncias

Use o comando describe-instance-topology da CLI sem especificar nenhum parâmetro ou filtro.

```
aws ec2 describe-instance-topology --region us-west-2
```

A resposta retorna apenas as instâncias que correspondem aos tipos de instância compatíveis com essa API. As instâncias podem estar em diferentes zonas de disponibilidade, zonas locais (`ZoneId`) e grupos de posicionamento (`GroupName`). Se a instância não estiver em um grupo de posicionamento, o campo `GroupName` estará vazio. Na saída do exemplo a seguir, apenas uma instância está em um grupo de posicionamento.

Exemplo de saída


```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
```

```
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 2: filtro de tipo de instância

Você pode filtrar por um tipo de instância especificado (correspondência exata) ou filtrar por uma família de instâncias (usando um caractere curinga). Você também pode combinar um filtro um tipo de instância e um filtro de família de instâncias.

Exemplo 2a: filtro de correspondência exata para um tipo de instância especificado

Para descrever a topologia da instância de todas as suas instâncias que correspondem a um tipo de instância especificado

Use o comando describe-instance-topology da CLI com o filtro de `instance-type`. Neste exemplo, a saída é filtrada para instâncias `trn1n.32xlarge`. A resposta retornará apenas as instâncias que corresponderem ao tipo de instância especificado.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 2b: filtro com curinga para uma família de instâncias

Para descrever a topologia da instância de todas as suas instâncias que correspondem a uma família de instâncias

Use o comando describe-instance-topology da CLI com o filtro de `instance-type`. Neste exemplo, a saída é filtrada para instâncias `trn1*`. A resposta retornará apenas as instâncias que corresponderem à família de instâncias especificada.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
```

```
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 2c: filtros combinados de família de instâncias e correspondência exata

Para descrever a topologia da instância de todas as suas instâncias que correspondem a uma família de instâncias ou a um tipo de instância especificado

Use o comando describe-instance-topology da CLI com o filtro de `instance-type`. Neste exemplo, a saída é filtrada para as instâncias `pd4d*` ou `trn1n.32xlarge`. A resposta retornará as instâncias que corresponderem a qualquer dos filtros especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
```

```
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 3: filtro de zone-id

Você pode usar o filtro `zone-id` para filtrar por uma zona de disponibilidade ou zona local. Você também pode combinar um filtro de zona de disponibilidade e um filtro de zona local.

Exemplo 3a: filtro de zona de disponibilidade

Para descrever a topologia da instância de todas as suas instâncias que correspondem a uma zona de disponibilidade especificada

Use o comando describe-instance-topology da CLI com o filtro de `zone-id`. Neste exemplo, a saída é filtrada usando o ID da zona de disponibilidade `use1-az1`. A resposta retornará apenas as instâncias que corresponderem à zona de disponibilidade especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Exemplo de saída

```
{
    "Instances": [
        {
```

```
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 3b: filtro de zona local

Para descrever a topologia da instância de todas as suas instâncias que correspondem a uma zona local especificada

Use o comando describe-instance-topology da CLI com o filtro de `zone-id`. Neste exemplo, a saída é filtrada usando o ID da zonal local `use1-atl2-az1`. A resposta retornará apenas as instâncias que corresponderem à zona local especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
```

```
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 3c: filtros combinados de zona de disponibilidade e zona local

Para descrever a topologia da instância de todas as suas instâncias que correspondem a uma zona de disponibilidade ou zona local especificada

Use o comando describe-instance-topology da CLI com o filtro de `zone-id`. Neste exemplo, a saída é filtrada usando o ID da zona de disponibilidade `use1-az1` e da zona local `use1-atl2-az1`. A resposta retornará as instâncias que corresponderem a qualquer dos filtros especificados.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
```

```
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 4: filtros combinados de instance-type e zone-id

Você pode combinar todos os filtros em um único comando.

Para descrever a topologia da instância de todas as instâncias que correspondem a um tipo de instância, família de instâncias, zona de disponibilidade ou zona local especificada

Use o comando describe-instance-topology da CLI com os filtros de `instance-type` e `zone-id`. Neste exemplo, a saída é filtrada para a família de instâncias `p4d*`, o tipo de instância `trn1n.32xlarge`, o ID da zona de disponibilidade `use1-az1` e o ID da zona local `use1-atl2-az1`. A resposta retornará as instâncias que corresponderem a instâncias `p4d*` ou `trn1n.32xlarge` nas zonas `us-east-1a` ou `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-
id,Values=use1-az1,use1-atl2-az1"
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
```

```
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 5: parâmetro do nome do grupo de posicionamento

Para descrever a topologia da instância de todas as suas instâncias em um grupo de posicionamento especificado

Use o comando describe-instance-topology da CLI com o parâmetro `group-names`. No exemplo a seguir, as instâncias podem estar no grupo de posicionamento `ML-group` ou `HPC-group`. A resposta retornará as instâncias que estiverem em um dos grupos de posicionamento.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemplo 6: IDs de instância

Para descrever a topologia da instância das instâncias especificadas

Use o comando describe-instance-topology da CLI com o parâmetro `--instance-ids`. A resposta retornará as instâncias que corresponderem aos IDs de instância especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Exemplo de saída

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
```

```
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Grupos de posicionamento

Para atender às necessidades de sua workload, você pode iniciar um grupo de instâncias do EC2 interdependentes em um grupo de posicionamento para influenciar seu posicionamento.

Dependendo do tipo de workload, é possível criar um grupo de posicionamento com uma das seguintes estratégias de posicionamento:

- Cluster: agrupa as instâncias em uma zona de disponibilidade. Essa estratégia permite que as workloads atinjam a performance de rede de baixa latência necessária para a comunicação de nó a nó totalmente acoplada que é típica das aplicações de computação de alta performance (HPC).
- Partição: distribui as instâncias entre partições lógicas, de tal modo que as instâncias em uma partição não compartilhem o hardware subjacente com os grupos de instâncias em outras partições. Essa estratégia é normalmente usada por grandes workloads distribuídas e replicadas, como Hadoop, Cassandra e Kafka.
- Distribuir: posiciona estritamente um pequeno grupo de instâncias no hardware subjacente distinto a fim de reduzir as falhas correlacionadas.

Os grupos de posicionamento são opcionais. Se você não iniciar suas instâncias em um grupo de posicionamento, o EC2 tentará posicionar as instâncias de tal forma que todas elas sejam distribuídas pelo hardware subjacente para minimizar as falhas correlacionadas.

Não há custo para a criação de um grupo de posicionamento.

Estratégias de posicionamento

É possível criar um grupo de posicionamento usando uma das estratégias de posicionamento a seguir.

Estratégias de posicionamento:

- Grupos de posicionamento de cluster
- Placement groups de partição
- Grupos de posicionamento de distribuição

Grupos de posicionamento de cluster

Um grupo de posicionamento de cluster é um agrupamento lógico de instâncias dentro de uma única zona de disponibilidade. As instâncias não estão isoladas em um rack único. Um grupo de posicionamento de cluster pode abranger redes privadas virtuais (VPCs) emparelhadas na mesma região. As instâncias no mesmo grupo de posicionamento de cluster dispõem de um limite de throughput por fluxo superior para tráfego TCP/IP e são colocadas no mesmo segmento de largura de banda de bisseção alta da rede.

A imagem a seguir mostra instâncias colocadas em um grupo de posicionamento de cluster.

Os grupos de posicionamento de cluster são recomendados para aplicações que se beneficiam de baixa latência de rede, alta throughput de rede ou ambos. Eles também são recomendados quando a maioria do tráfego de rede está entre as instâncias no grupo. Para fornecer a menor latência possível e a melhor performance de rede de pacote por segundo para seu grupo de posicionamento, escolha

um tipo de instância que comporte rede avançada. Para obter mais informações, consulte Redes aprimoradas.

Recomendamos executar suas instâncias da seguinte maneira:

- Use uma única solicitação de execução para executar o número de instâncias necessárias no placement group.
- Use o mesmo tipo de instância para todas as instâncias no placement group.

Se você tentar adicionar mais instâncias ao grupo de posicionamento depois ou se tentar executar mais de um tipo de instância no grupo de posicionamento, aumentará as possibilidades de ocorrer um erro de capacidade insuficiente.

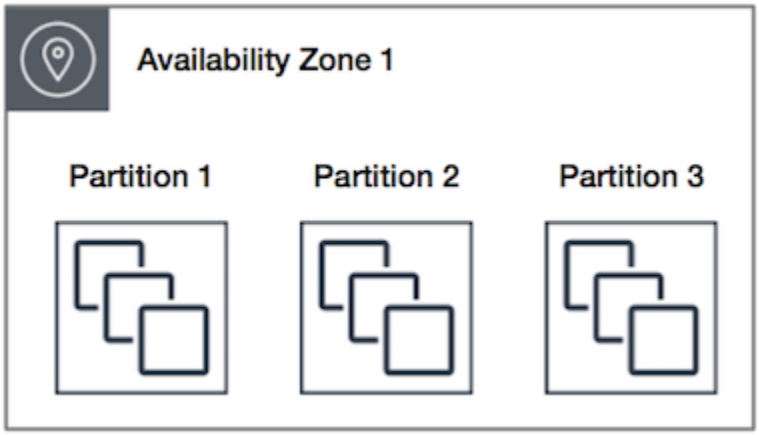
Se você interrompe uma instância em um placement group e depois a inicia novamente, ela ainda é executada no placement group. Contudo, ocorrerá uma falha no início se não houver capacidade suficiente para a instância.

Se você receber um erro de capacidade ao executar uma instância em um placement group que já tenha instâncias em execução, interrompa e inicie todas as instâncias no placement group e tente executá-lo novamente. Iniciar as instâncias pode migrá-las para o hardware com capacidade para todas as instâncias solicitadas.

Placement groups de partição

Os grupos de posicionamento de partição ajudam a reduzir a probabilidade de falhas de hardware correlacionadas da aplicação. Ao usar grupos de posicionamento de partição, o Amazon EC2 divide cada grupo em segmentos lógicos chamados de partições. O Amazon EC2 garante que cada partição em um grupo de posicionamento tenha seu próprio conjunto de racks. Cada rack tem sua própria rede e fonte de energia. Não há duas partições em um grupo de posicionamento que compartilhem os mesmos racks, permitindo que você isole o impacto da falha de hardware na aplicação.

A imagem a seguir é uma representação visual simples de um grupo de posicionamento de partição em uma única zona de disponibilidade. Ela mostra instâncias que são colocadas em um placement grupo de posicionamento de partição com três partições — Partition 1 (Partição 1), Partition 2 (Partição 2) e Partition 3 (Partição 3). Cada partição é composta por várias instâncias. As instâncias em cada partição não compartilham racks com as instâncias nas outras partições, contendo o impacto de uma única falha de hardware apenas na partição associada.



Grupos de posicionamento de partição podem ser usados para implantar grandes workloads distribuídas e replicadas, como HDFS, HBase e Cassandra, em racks distintos. Ao executar instâncias em um grupo de posicionamento de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente pelo número de partições especificado por você. Também é possível executar instâncias em uma partição específica para ter mais controle sobre onde as instâncias são colocadas.

Um grupo de posicionamento de partição pode ter partições em várias zonas de disponibilidade na mesma região. Um grupo de posicionamento de partição pode ter, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um grupo de posicionamento de partição é limitado somente pelos limites da sua conta.

Além disso, grupos de posicionamento de partição oferecem visibilidade nas partições — é possível ver quais instâncias estão em quais partições. É possível compartilhar essas informações com aplicações que reconhecem a topologia, como HDFS, HBase e Cassandra. Essas aplicações usam essas informações para tomar decisões inteligentes de replicação de dados para aumentar a disponibilidade e a durabilidade dos dados.

Se você iniciar ou executar uma instância em um grupo de posicionamento de partição e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde.

Grupos de posicionamento de distribuição

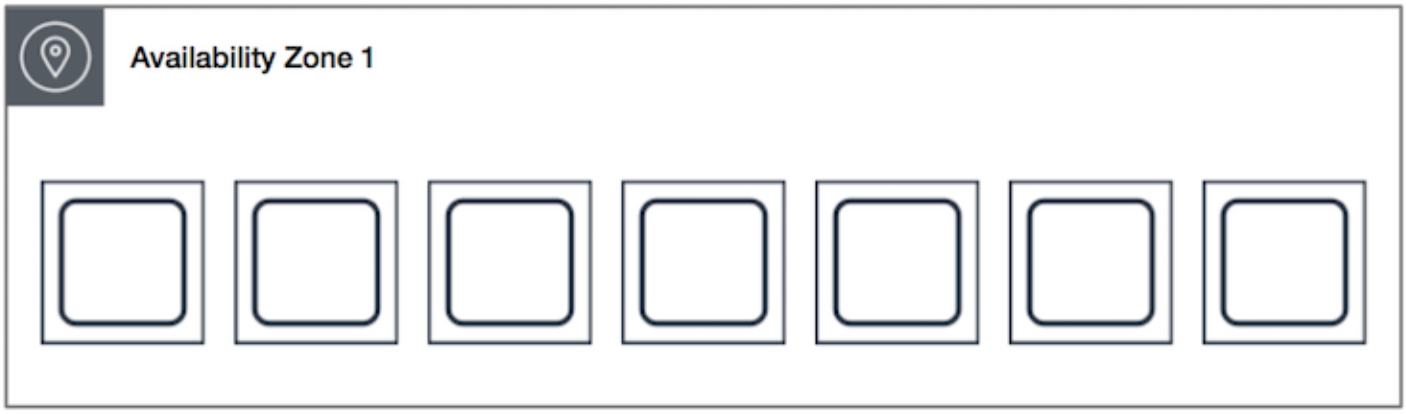
Um grupo de posicionamento de distribuição é um grupo de instâncias que são colocadas cada uma em hardware distinto.

Os grupos de posicionamento de distribuição são recomendados para aplicações com uma pequena quantidade de instâncias críticas que devem ser mantidas separadas umas das outras. Executar instâncias em um grupo de posicionamento de nível de distribuição reduz o risco de falhas simultâneas que podem ocorrer quando as instâncias compartilham os mesmos equipamentos. Os grupos de posicionamento em nível de distribuição concedem acesso a equipamentos distintos e, portanto, são adequados para combinar tipos de instâncias ou executar instâncias ao longo do tempo.

Se você iniciar ou executar uma instância em um grupo de posicionamento disseminado e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde. Grupos de posicionamento podem distribuir instâncias em racks ou hosts. É possível usar grupos com posicionamento distribuído em nível de rack em regiões da AWS e AWS Outposts. Você pode usar grupos com posicionamento distribuído em nível de host somente com AWS Outposts.

Grupos com posicionamento distribuído em nível de rack

A imagem a seguir mostra sete instâncias em uma única zona de disponibilidade que são colocadas em um grupo de posicionamento de distribuição. As sete instâncias são colocadas em sete racks diferentes, cada um com sua própria rede e fonte de energia.



Um grupo com posicionamento distribuído em nível de rack pode abranger várias zonas de disponibilidade na mesma região. Em uma região, um grupo com posicionamento distribuído em nível de rack pode ter no máximo sete instâncias em execução por zona de disponibilidade por grupo. Com o Outposts, seu grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.

Grupos de posicionamento de distribuição em host

Os grupos com posicionamento distribuído em host estão disponíveis apenas com AWS Outposts. Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost. Para ter mais informações, consulte the section called “Grupos de posicionamento no AWS Outposts”.

Regras e limitações do grupo de posicionamento

Tópicos

- Regras e limitações gerais
- Regras e limitações do grupo de posicionamento de cluster
- Regras e limitações do grupo de posicionamento de partição
- Regras e limitações do grupo de posicionamento de distribuição

Regras e limitações gerais

Antes de usar os grupos de posicionamento, esteja ciente das seguintes regras:

- É possível criar até 500 grupos de posicionamento por conta em cada região.
- O nome especificado para um grupo de posicionamento deve ser exclusivo na conta da AWS para a região em questão.
- Não é possível mesclar grupos de posicionamento.
- Uma instância pode ser executada em um grupo de posicionamento por vez; ela não pode abranger vários grupos de posicionamento.
- O recurso Reservas de capacidade sob demanda e as Instâncias reservadas de zona permitem que você reserve capacidade para instâncias do EC2 em zonas de disponibilidade. Quando você executa uma instância, se os atributos da instância corresponderem aos especificados por uma reserva de capacidade sob demanda ou por uma instância reservada por zona, a capacidade reservada será usada automaticamente pela instância. Isso também é verdade se você executar a instância em um grupo de posicionamento.

  Se você planeja executar instâncias em um grupo de posicionamento de clusters, recomendamos que você reserve a capacidade explicitamente no grupo de posicionamento de clusters. Você pode fazer isso criando uma reserva de capacidade sob demanda em um grupo de posicionamento de cluster especificado. Observe que, embora possa reservar capacidade dessa forma usando

reservas de capacidade sob demanda, não é possível fazer isso com instâncias reservadas por zona, pois elas não podem reservar capacidade explicitamente em um grupo de posicionamento.

- Não é possível iniciar os hosts dedicados em grupos de posicionamento.
- Você não pode iniciar uma instância spot que esteja configurada para parar ou hibernar em caso de interrupção em um grupo de posicionamento.

Regras e limitações do grupo de posicionamento de cluster

As seguintes regras se aplicam aos grupos de posicionamento de cluster:

- Somente os seguintes tipos de instância são compatíveis:
  - Instâncias da geração atual, exceto as instâncias de desempenho expansíveis (por exemplo, T2), as instâncias Mac1 e as instâncias M7i-flex.
  - As seguintes instâncias da geração anterior: A1, C3, C4, I2, M4, R3 e R4.
- Um grupo de posicionamento de cluster não pode abranger várias zonas de disponibilidade.
- A velocidade máxima de throughput de rede do tráfego entre duas instâncias em um grupo de posicionamento de cluster é limitada pela instância mais lenta. Para aplicações com requisitos de throughput alta, escolha um tipo de instância com conectividade de rede que atenda a suas necessidades.
- Para instâncias ativadas para a rede avançada, as seguintes regras se aplicam:
  - As instâncias dentro de um grupo de posicionamento de cluster podem usar até 10 Gbps para tráfego de fluxo único. As instâncias que não estiverem dentro de um grupo de posicionamento de cluster poderão usar até 5 Gbps para tráfego de fluxo único.
  - O tráfego para e de buckets do Amazon S3 na mesma região pelo espaço de endereço IP público ou por um VPC endpoint pode usar toda a largura de banda agregada da instância disponível.
- É possível executar vários tipos de instâncias em um grupo de posicionamento de cluster. No entanto, isso reduz a probabilidade de a capacidade necessária estar disponível para que a execução seja realizada com sucesso. Recomendamos usar o mesmo tipo de instância para todas as instâncias em um grupo de posicionamento de cluster.
- O tráfego de rede para a Internet e por meio de uma conexão do AWS Direct Connect com recursos on-premises é limitado a 5 Gbps para grupos com posicionamento em cluster.

Regras e limitações do grupo de posicionamento de partição

As seguintes regras se aplicam aos grupos de posicionamento de partição:

- Um grupo de posicionamento de partição oferece suporte a, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um grupo de posicionamento de partição é limitado somente pelos limites da sua conta.
- Quando as instâncias são executadas em um grupo de posicionamento de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente em todas as partições. O Amazon EC2 não garante uma distribuição uniforme de instâncias em todas as partições.
- Um grupo de posicionamento de partição com Instâncias dedicadas pode ter, no máximo, duas partições.
- Reservas de capacidade não reservam capacidade em um grupo de posicionamento de partição.

Regras e limitações do grupo de posicionamento de distribuição

As seguintes regras se aplicam aos grupos de posicionamento de distribuição:

- Um grupo de posicionamento de distribuição em rack suporta, no máximo, sete instâncias em execução por zona de disponibilidade. Por exemplo, em uma região com três zonas de disponibilidade, é possível executar um total de 21 instâncias no grupo, com sete instâncias em cada zona de disponibilidade. Se você tentar iniciar uma oitava instância na mesma zona de disponibilidade e no mesmo grupo de posicionamento de distribuição, ela não será executada. Se você precisar de mais de sete instâncias em uma zona de disponibilidade, recomendamos usar vários grupos de posicionamento de distribuição. O uso de vários grupos de posicionamento de dispersão não fornece garantias sobre a disseminação de instâncias entre grupos, mas ajuda a garantir a dispersão para cada grupo, limitando assim o impacto de certas classes de falhas.
- Os grupos de posicionamento de distribuição não são compatíveis com o Instâncias dedicadas.
- Grupos de posicionamento de distribuição em host apenas são compatíveis com grupos de posicionamento AWS Outposts. Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost.
- Em uma região, um grupo com posicionamento distribuído em nível de rack pode ter no máximo sete instâncias em execução por zona de disponibilidade por grupo. Com o AWS Outposts, seu grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.

- Reservas de capacidade não reservam capacidade em um grupo de posicionamento de espalhamento.

Trabalho com grupos de posicionamento

Conteúdo

- Criar um grupo de posicionamento.
- Visualizar informações sobre um grupo de posicionamento
- Marcar um grupo de posicionamento
- Executar instâncias em um grupo de posicionamento
- Descrever instâncias em um grupo de posicionamento
- Alterar o placement group de uma instância
- Remova uma instância de um grupo de posicionamento
- Excluir um grupo de posicionamento.

Criar um grupo de posicionamento.

É possível criar um grupo de posicionamento usando um dos métodos a seguir.

Console

Para criar um grupo de posicionamento usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups.
3. Escolha Criar grupo de posicionamento.
4. Especifique um nome para o grupo.
5. Escolha a estratégia de posicionamento para o grupo.
   - Se escolher Spread, escolha o nível de spread.
     - Rack: sem restrições
     - Host: somente para Outposts
   - Se você escolher Partition (Partição), selecione o número de partições no grupo.

6. Para marcar o grupo de posicionamento, escolha Add tag (Adicionar etiqueta) e, em seguida, insira uma chave e um valor. Escolha Add tag (Adicionar etiqueta) para cada etiqueta que você deseja adicionar.
7. Escolha Criar grupo.

AWS CLI

Como criar um placement group usando a AWS CLI

Use o comando create-placement-group. O exemplo a seguir cria um grupo de posicionamento chamado `my-cluster` que usa a estratégia de posicionamento do `cluster` e aplica uma tag com uma chave de `purpose` e um valor de `production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Como criar um grupo de posicionamento de partição usando a AWS CLI

Use o comando create-placement-group. Especifique o parâmetro `--strategy` com o valor `partition` e especifique o parâmetro `--partition-count` com o número desejado de partições. Neste exemplo, o grupo de posicionamento de partição é chamado de `HDFS-Group-A` e criado com cinco partições.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Como criar um placement group usando a AWS Tools for Windows PowerShell

Use o comando New-EC2PlacementGroup.

Visualizar informações sobre um grupo de posicionamento

Você pode visualizar todos os seus grupos de posicionamento e suas respectivas informações aplicando um dos seguintes métodos.

Console

Para visualizar informações detalhadas sobre um ou mais grupos de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Rede e segurança, escolha Grupos de segurança.
3. Na tabela Grupos de posicionamento, para cada grupo de posicionamento, é possível visualizar as seguintes informações:
   - Nome do grupo: o nome que você deu ao grupo de posicionamento.
   - ID do grupo: o ID do grupo de posicionamento.
   - Estratégia: a estratégia de posicionamento para o grupo de posicionamento.
   - Estado: o estado do grupo de posicionamento.
   - Partição: o número de partições. Válido somente se a estratégia for partição.
   - ARN do grupo: o nome do recurso da Amazon (ARN) do grupo de posicionamento.

AWS CLI

Para descrever todos os seus grupos de posicionamento

Use o comando describe-placement-group AWS CLI.

```
aws ec2 describe-placement-groups
```

Exemplo de resposta

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
```

```
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        },
            ...
    ]
}
```

Para descrever um grupo de posicionamento específico

Use o comando describe-placement-group AWS CLI. Você pode especificar o parâmetro `--group-id` ou `--group-name`.

Especifique o ID do grupo de posicionamento:

```
aws ec2 describe-placement-groups --group-id pg-0123456789example
```

Especifique o nome do grupo de posicionamento:

```
aws ec2 describe-placement-groups --group-name my-cluster-pg
```

Exemplo de resposta

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        }
    ]
}
```

Marcar um grupo de posicionamento

Para categorizar e gerenciar grupos de posicionamento existentes, é possível marcá-los com metadados personalizados. Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Quando você marca um grupo de posicionamento, as instâncias executadas no grupo de posicionamento não são marcadas automaticamente. É necessário marcar explicitamente as instâncias que são executadas no grupo de posicionamento. Para ter mais informações, consulte Adicionar uma tag ao executar uma instância.

É possível visualizar, adicionar e excluir etiquetas usando um dos seguintes métodos.

Console

Como visualizar, adicionar ou excluir uma tag para um grupo de posicionamento existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups.
3. Selecione um grupo de posicionamento e escolha Actions (Ações), Manage tags (Gerenciar tags).
4. A tela Gerenciar tags exibe todas as tags atribuídas ao grupo de posicionamento.
   - Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. É possível adicionar até 50 tags por grupo de posicionamento. Para ter mais informações, consulte Restrições de tags.
   - Para excluir uma tag, escolha Remove (Remover) ao lado da tag que você deseja excluir.
5. Escolha Salvar.

AWS CLI

Como visualizar tags de placement group

Use o comando describe-tags para visualizar as tags para o recurso especificado. No exemplo a seguir, descreva as tags para todos os grupos de posicionamento.

```
aws ec2 describe-tags \
    --filters Name=resource-type,Values=placement-group
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
```

```
            "Value": "Production"
        },
        {
            "Key": "Environment",
            "ResourceId": "pg-9876543210EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

Também é possível usar o comando describe-tags para visualizar as tags de um grupo de posicionamento especificando seu ID. No exemplo a seguir, descreva as tags para pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \

    --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

Também é possível visualizar as tags de um grupo de posicionamento descrevendo o placement group.

Use o comando describe-placement-groups para visualizar a configuração do grupo de posicionamento especificado, que inclui todas as tags especificadas para o grupo de posicionamento.

```
aws ec2 describe-placement-groups \
    --group-name my-cluster
```

```
{
```

```
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Como marcar um grupo de posicionamento existente usando o comando da AWS CLI

É possível usar o comando create-tags para marcar os recursos existentes. No exemplo a seguir, o grupo de posicionamento existente está marcado com `Key=Cost-Center` e `Value=CC-123`.

```
aws ec2 create-tags \
    --resources pg-0123456789EXAMPLE \
    --tags Key=Cost-Center,Value=CC-123
```

Como excluir a tag de um grupo de posicionamento usando o comando da AWS CLI

É possível usar o comando delete-tags para excluir tags de recursos existentes. Para obter exemplos, consulte Exemplos na Referência de Comandos da AWS CLI.

PowerShell

Como visualizar tags de placement group

Use o comando Get-EC2Tag.

Como descrever as tags de um grupo de posicionamento específico

Use o comando Get-EC2PlacementGroup.

Como marcar um grupo de posicionamento existente

Use o comando New-EC2Tag.

Como excluir a tag de um grupo de posicionamento

Use o comando Remove-EC2Tag.

Executar instâncias em um grupo de posicionamento

É possível executar uma instância em um grupo de posicionamento se as regras e limitações do placement group forem atendidas usando um dos métodos a seguir.

Console

Para executar instâncias em um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do console do EC2, na caixa Iniciar instância, escolha Iniciar instância. Preencha o formulário conforme direcionado, tendo o cuidado de fazer o seguinte:
   - Em Instance type (Tipo de instância), selecione um tipo de instância que possa ser executado em um grupo de posicionamento.
   - Na caixa Summary (Resumo), em Number of instances (Número de instâncias), insira o número total de instâncias que serão necessárias nesse grupo de posicionamento, pois talvez você não possa adicionar instâncias ao grupo de posicionamento posteriormente.
   - Em Advanced details (Detalhes avançados), para Placement group name (Nome do placement group), é possível optar por adicionar instâncias a um grupo de posicionamento novo ou existente. Se você escolher um grupo de posicionamento com uma estratégia de partição, para Target partition (Partição de destino), selecione a partição na qual executar as instâncias.

AWS CLI

Para executar instâncias em um grupo de posicionamento

Use o comando run-instances e especifique o nome do grupo de posicionamento usando o parâmetro `--placement "GroupName = my-cluster"`. Neste exemplo, o grupo de posicionamento é chamado de `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Como executar instâncias em uma partição específica de um grupo de posicionamento de partição usando a AWS CLI

Use o comando run-instances e especifique a partição e o nome do grupo de posicionamento usando o parâmetro `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"`. Neste exemplo, o grupo de posicionamento de partição é chamado de `HDFS-Group-A` e o número de partição é `3`.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

Como executar instâncias em um grupo de posicionamento usando o AWS Tools for Windows PowerShell

Use o comando New-EC2Instance e especifique o nome do grupo de posicionamento usando o parâmetro `-Placement_GroupName`.

Descrever instâncias em um grupo de posicionamento

É possível visualizar as informações de posicionamento de suas instâncias usando um dos métodos a seguir. Também é possível filtrar grupos de posicionamento de partição pelo número de partição usando a AWS CLI.

Console

Para visualizar o grupo de posicionamento e o número de partição de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Description (Descrição), em Host and placement group (Host e grupo de posicionamento), localize Placement group (Grupo de posicionamento). Se a instância não estiver em um placement group, o campo estará vazio. Caso contrário, ela conterá o nome do placement group. Se o grupo de posicionamento for um grupo de posicionamento de partição, o Partition number (Número de partição) conterá o número de partição da instância.

AWS CLI

Para visualizar o número de partição de uma instância em um grupo com posicionamento em partições

Use o comando describe-instances e especifique o parâmetro `--instance-id`.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

A resposta contém as informações de posicionamento, o que inclui o nome do grupo de posicionamento e o número da partição da instância.

```
"Placement": {
     "AvailabilityZone": "us-east-1c",
     "GroupName": "HDFS-Group-A",
     "PartitionNumber": 3,
     "Tenancy": "default"
}
```

Para filtrar instâncias de um grupo com posicionamento em partições e número de partição específicos

Use o comando describe-instances e especifique o parâmetro `--filters` com os filtros `placement-group-name` e `placement-partition-number`. Neste exemplo, o grupo de posicionamento de partição é chamado de `HDFS-Group-A` e o número de partição é `7`.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-
Group-A" "Name = placement-partition-number, Values = 7"
```

A resposta lista todas as instâncias que estão na partição especificada dentro do grupo de posicionamento especificado. A seguir está um exemplo de saída mostrando somente o ID da instância, o tipo de instância e informações de posicionamento das instâncias retornadas.

```
"Instances": [
                {
                    "InstanceId": "i-0a1bc23d4567e8f90",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
                    }
```

```
            {
                "InstanceId": "i-0a9b876cd5d4ef321",
                "InstanceType": "r4.large",
                },

                "Placement": {
                    "AvailabilityZone": "us-east-1c",
                    "GroupName": "HDFS-Group-A",
                    "PartitionNumber": 7,
                    "Tenancy": "default"
                }
        ],
```

Alterar o placement group de uma instância

É possível alterar o grupo de posicionamento de uma instância da seguinte maneira:

- Mova uma instância existente para um grupo de posicionamento
- Mova uma instância de um grupo de posicionamento para outro

Antes de mover a instância, ela deve estar no estado `stopped`.

Console

Para mover uma instância para um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Estado da instância e Interromper instância.
4. Com a instância selecionada, escolha Ações, Configurações de instância, Modificar posicionamento de instância).
5. Em Grupo de posicionamento, escolha o grupo de posicionamento para o qual mover a instância.
6. Escolha Salvar.

AWS CLI

Para mover uma instância para um grupo de posicionamento

1. Interrompa a instância usando o comando stop-instances.
2. Use o comando modify-instance-placement e especifique o nome do grupo de posicionamento para o qual mover a instância.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

3. Inicie a instância usando o comando start-instances.

PowerShell

Como mover uma instância para um placement group usando o AWS Tools for Windows PowerShell

1. Interrompa a instância usando o comando Stop-EC2Instance.
2. Use o comando Edit-EC2InstancePlacement e especifique o nome do grupo de posicionamento para o qual mover a instância.
3. Inicie a instância usando o comando Start-EC2Instance.

Remova uma instância de um grupo de posicionamento

É possível remover uma instância de um grupo de posicionamento usando um dos métodos a seguir.

Antes de remover uma instância de um grupo de posicionamento, ela deve estar no estado `stopped`.

Console

Para remover uma instância de um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Estado da instância e Interromper instância.

4. Com a instância selecionada, escolha Ações, Configurações de instância, Modificar posicionamento de instância).
5. Em Grupo de posicionamento, escolha Nenhum.
6. Escolha Salvar.

AWS CLI

Para remover uma instância de um grupo de posicionamento

1. Interrompa a instância usando o comando stop-instances.
2. Use o comando modify-instance-placement e especifique uma string vazia para o nome do grupo de posicionamento.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

3. Inicie a instância usando o comando start-instances.

PowerShell

Como remover uma instância de um placement group usando o AWS Tools for Windows PowerShell

1. Interrompa a instância usando o comando Stop-EC2Instance.
2. Use o comando Edit-EC2InstancePlacement e especifique uma string vazia para o nome do grupo de posicionamento.
3. Inicie a instância usando o comando Start-EC2Instance.

Excluir um grupo de posicionamento.

Se precisar substituir um grupo de posicionamento ou se não precisar mais dele, será possível excluí-lo. É possível excluir um grupo de posicionamento usando um dos métodos a seguir.

Pré-requisito

Para excluir um grupo de posicionamento, ele não deve conter instâncias. É possível encerrar todas as instâncias executadas no grupo de posicionamento, movê-las para outro grupo de posicionamento ou removê-las do grupo de posicionamento.

Console

Para excluir um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups.
3. Selecione o grupo de posicionamento e escolha Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, insira **`Delete`** e escolha Delete (Excluir).

AWS CLI

Para excluir um grupo de posicionamento

Use o comando delete-placement-group e especifique o nome do grupo de posicionamento para excluí-lo. Neste exemplo, o nome do grupo de posicionamento é `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Como excluir um placement group usando o AWS Tools for Windows PowerShell

Use o comando Remove-EC2PlacementGroup para excluir o grupo de posicionamento.

Compartilhar um grupo de posicionamento

O compartilhamento de grupos de posicionamento permite que você influencie o posicionamento de instâncias interdependentes que pertencem a contas distintas da AWS. É possível compartilhar um grupo com posicionamento em várias contas da AWS ou dentro de suas organizações. Você pode iniciar instâncias em um grupo de posicionamento compartilhado.

O proprietário de um grupo de posicionamento pode compartilhar um grupo de posicionamento com:

- Contas específicas da AWS que são internas ou externas à organização
- Uma unidade organizacional dentro de sua organização da

- Toda a sua organização da

> **Note**
>
> A conta da AWS da qual você deseja compartilhar um grupo de posicionamento deve ter as seguintes permissões na política do IAM.
>
> - `ec2:PutResourcePolicy`
> - `ec2:DeleteResourcePolicy`

Tópicos

- Regras e limitações
- Compartilhamento entre zonas de disponibilidade
- Compartilhar um grupo de posicionamento
- Identificar um grupo de posicionamento compartilhado
- Iniciar uma instância em um grupo de posicionamento compartilhado
- Cancelar o compartilhamento de um grupo de posicionamento compartilhado

Regras e limitações

As regras e limitações a seguir se aplicam quando você compartilha um grupo de posicionamento ou quando um grupo de posicionamento é compartilhado com você.

- Para compartilhar um grupo de posicionamento, é necessário que você seja o proprietário dele na sua conta da AWS. Não é possível compartilhar um grupo de posicionamento que tenha sido compartilhado com você.
- Quando você compartilha um grupo com posicionamento em partições ou um grupo com posicionamento distribuído, os limites do grupo de posicionamento não mudam. Um grupo com posicionamento em partições compartilhado é compatível com, no máximo, sete partições por zona de disponibilidade e um grupo com posicionamento distribuído compartilhado é compatível com, no máximo sete instâncias em execução por zona de disponibilidade.
- Para compartilhar um grupo com posicionamento com a organização ou com uma unidade organizacional em sua organização, você deve habilitar o compartilhamento com o AWS Organizations. Para mais informações, consulte Compartilhar seus recursos da AWS.

- Você é responsável por gerenciar as instâncias de que é proprietário em um grupo de posicionamento compartilhado.
- Você não pode visualizar nem modificar instâncias e reservas de capacidade associadas a um grupo de posicionamento compartilhado do qual não é proprietário.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de seus Hosts dedicados relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da zona de disponibilidade é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de zona de disponibilidade da região `us-east-1` e é o mesmo local em cada conta da AWS.

Como visualizar os IDs de zona de disponibilidade para as zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram.
2. Os IDs de zona de disponibilidade da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no painel direito.

Compartilhar um grupo de posicionamento

Para compartilhar um grupo de posicionamento, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na sua organização, os consumidores da organização terão acesso ao grupo de posicionamento compartilhado.

Se o grupo de posicionamento for compartilhado com uma conta da AWS fora da sua organização, o proprietário da conta da AWS receberá um convite para participar do compartilhamento de recursos. Ele poderá acessar o grupo de posicionamento compartilhado depois que aceitar o convite.

Você pode compartilhar um grupo de posicionamento entre contas da AWS usando https://console.aws.amazon.com/ram ou a AWS CLI.

AWS RAM console

Para compartilhar um grupo de posicionamento do qual você é o proprietário usando https://console.aws.amazon.com/ram, consulte Creating a resource share (Criar um compartilhamento de recursos).

AWS CLI

Para compartilhar um grupo de posicionamento de sua propriedade, use o comando create-resource-share.

Identificar um grupo de posicionamento compartilhado

O nome do recurso da Amazon (ARN) de um grupo com posicionamento contém o ID da conta de 12 dígitos da conta proprietária do grupo com posicionamento. É possível usar o ID da conta para identificar o proprietário de um grupo com posicionamento que é compartilhado com você.

Você pode encontrar o ARN do grupo com posicionamento ao usar um dos métodos apresentados a seguir. Para ter mais informações, consulte Visualizar informações sobre um grupo de posicionamento.

Amazon EC2 console

Como identificar um grupo com posicionamento compartilhado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Rede e segurança, escolha Grupos de segurança.
3. A tabela Grupos com posicionamento lista todos os grupos com posicionamento que pertencem a você e são compartilhados com você. A coluna ARN do grupo exibe o ARN do grupo com posicionamento.

   Se a coluna ARN do grupo não estiver visível, escolha configurações () no canto superior direito, ative ARN do grupo e selecione Confirmar.

AWS CLI

Como identificar um grupo com posicionamento compartilhado

Use o comando `describe-placement-groups` para listar todos os grupos com posicionamento que pertencem a você e são compartilhados com você. Na resposta, o parâmetro `GroupId` exibirá o ARN de um grupo com posicionamento.

Iniciar uma instância em um grupo de posicionamento compartilhado

> **Important**
>
> Ao usar a AWS CLI para iniciar uma instância em um grupo com posicionamento compartilhado, você deve especificar o ID do grupo com posicionamento ao usar o parâmetro `GroupId`.

Você poderá usar o nome do grupo com posicionamento somente se for o proprietário do grupo com o posicionamento que está sendo compartilhado. Recomendamos usar o ID do grupo com posicionamento para evitar possíveis conflitos de nomes de grupos com posicionamento entre contas da AWS.

É possível encontrar o ID de um grupo com posicionamento no console do Amazon EC2, na tela Grupos com posicionamento ou ao usar o comando `describe-placement-groups` da AWS CLI. Para ter mais informações, consulte Visualizar informações sobre um grupo de posicionamento.

Console

Como iniciar instâncias em um grupo com posicionamento compartilhado

1. Siga o procedimento para iniciar uma instância, mas não inicie a instância até concluir as etapas apresentadas a seguir para especificar as configurações para o grupo com posicionamento.
2. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para ter mais informações, consulte Regras e limitações do grupo de posicionamento.
3. Expanda Detalhes avançados e defina as configurações do grupo com posicionamento da seguinte maneira:

a. Em Grupo com posicionamento, selecione o grupo com posicionamento que foi compartilhado com você.

> **Note**
>
> Se houver grupos com posicionamento com nomes semelhantes, verifique o ID do grupo com posicionamento para ter certeza de ter selecionado o grupo com posicionamento correto.

b. Se você escolher um grupo com posicionamento com uma estratégia de partição, em Partição de destino, escolha a partição na qual deseja iniciar a instância.

4. No painel Resumo, faça o seguinte:

a. Em Number of instances (Número de instâncias), insira o número total de instâncias que serão necessárias nesse grupo de posicionamento, pois talvez você não possa adicionar instâncias ao grupo de posicionamento posteriormente.

b. Analise a configuração da instância e, em seguida, escolha Iniciar instância.

Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

AWS CLI

Para iniciar uma instância em um grupo de posicionamento compartilhado

Use o comando `run-instances` e especifique o ID do grupo com posicionamento do grupo com posicionamento compartilhado.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example"
```

Para iniciar instâncias em uma partição específica de um grupo com posicionamento em partições

Use o comando `run-instances` e especifique o ID do grupo com posicionamento e o número da partição do grupo com posicionamento compartilhado.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example, PartitionNumber
 = 3"
```

> **Tip**
>
> Use o emparelhamento de VPC para conectar instâncias pertencentes a contas distintas da AWS e obter todos os benefícios de latência oferecidos pelos grupo com posicionamento em cluster compartilhados. Para obter mais informações, consulte O que é emparelhamento de VPC?

Cancelar o compartilhamento de um grupo de posicionamento compartilhado

O proprietário do grupo de posicionamento pode cancelar o compartilhamento de um grupo de posicionamento compartilhado a qualquer momento.

Quando você cancela o compartilhamento de um grupo de posicionamento compartilhado, as seguintes alterações ocorrem.

- As contas da AWS com as quais um grupo de posicionamento foi compartilhado não podem mais iniciar instâncias nem reservar capacidade.
- Se suas instâncias estiverem sendo executadas em um grupo de posicionamento compartilhado, elas serão desassociadas do grupo de posicionamento, mas continuarão sendo executadas normalmente em sua conta da AWS.
- Se você tiver reservas de capacidade em um grupo de posicionamento compartilhado, elas serão desassociadas do grupo de colocação, mas você continuará tendo acesso a elas em suaAWS conta.

É possível cancelar o compartilhamento de um grupo de posicionamento usando um dos métodos a seguir.

AWS RAM console

Para cancelar o compartilhamento um grupo de posicionamento usando https://console.aws.amazon.com/ram, consulte Deleting a resource share (Excluir um compartilhamento de recursos).

AWS CLI

Para cancelar o compartilhamento de um grupo de posicionamento compartilhado usando a AWS Command Line Interface, use o comando disassociate-resource-share.

Grupos de posicionamento no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

É possível criar grupos de posicionamento em Outposts que você criou na sua conta. Isso permite que você distribua instâncias no hardware de base em um Outpost no local. Você cria e utiliza grupos de posicionamento em Outposts da mesma forma que cria e utiliza grupos de posicionamento em zonas de disponibilidade regulares. Ao criar um grupo de posicionamento com uma estratégia de distribuição em um Outpost, você pode optar por fazer com que o grupo de posicionamento distribua instâncias entre hosts ou racks. A distribuição de instâncias entre hosts permite usar uma estratégia de distribuição com um único rack do Outpost.

Considerações

- Um grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.
- Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost.

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Para utilizar um grupo de posicionamento em um Outpost

1. Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.
2. Crie um grupo de posicionamento na região associada do Outpost. Se você criar um grupo de posicionamento com uma estratégia de distribuição, poderá escolher o nível de distribuição

em nível host ou de rack para determinar como o grupo distribuirá instâncias pelo hardware de base no Outpost. Para ter mais informações, consulte the section called “Criar um grupo de posicionamento.”.

3. Inicie uma instância no grupo de posicionamento. Para Subnet (Sub-rede), escolha a sub-rede criada na Etapa 1 e para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento criado na Etapa 2. Para obter mais informações, consulte Executar uma instância no Outpost no Manual do usuário do AWS Outposts.

Unidade de transmissão máxima (MTU) de rede para a instância do EC2

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Os quadros de Ethernet consistem no pacote, ou nos dados em si que você envia, e nas informações de overhead de rede que o cercam.

Os quadros de ethernet podem vir em diferentes formatos, sendo o mais comum o Ethernet v2 padrão. Ele é compatível com 1.500 MTU, que é o maior tamanho de pacote de Ethernet compatível na maior parte da Internet. A MTU máxima compatível com uma instância depende do tipo de instância.

As regras seguintes se aplicam às instâncias que estão em zonas de Wavelength:

- O tráfego que vai de uma instância para outra dentro de uma VPC na mesma zona do Wavelength tem um MTU de 1300.
- O tráfego que vai de uma instância a outra que usa o IP do portador dentro de uma zona de Wavelength tem um MTU de 1500.
- O tráfego que vai de uma instância a outra entre uma zona de Wavelength e a região que usa um endereço IP público tem um MTU de 1500.
- O tráfego que vai de uma instância a outra entre uma zona de Wavelength e a região que usa um endereço IP privado tem um MTU de 1300.

As regras a seguir se aplicam às instâncias que estão no Outposts.

- O tráfego que vai de uma instância do Outposts para uma instância da região tem um MTU de 1300.

Conteúdo

- Frames jumbo (9001 MTU)
- Path MTU Discovery
- Verificar o MTU do caminho entre dois hosts
- Verificação da MTU para a instância
- Definição da MTU para a instância
- Solução de problemas

Frames jumbo (9001 MTU)

Os frames jumbo permitem mais de 1500 bytes de dados ao aumentar o tamanho da carga útil por pacote, aumentando assim a porcentagem do pacotes que não configura sobrecarga. São necessários menos pacotes para enviar a mesma quantidade de dados usáveis. No entanto, o tráfego é limitado a um MTU máximo de 1500 nos seguintes casos:

- Tráfego em um gateway de Internet
- Tráfego em uma conexão de emparelhamento de VPC entre regiões
- Tráfego através de ligações VPN
- Tráfego externo a uma determinada região da AWS

Se os pacotes tiverem mais de 1500 bytes, eles são fragmentados ou caem se o marcador `Don't Fragment` for definido no cabeçalho IP.

Os frames Jumbo devem ser usados com cuidado para o tráfego voltado para Internet ou qualquer tráfego que saia de uma VPC. Os pacotes são fragmentados por sistemas intermediários, que retarda o tráfego. Para usar frames jumbo dentro de uma VPC e não diminuir o tráfego vinculado para fora da VPC, é possível configurar o tamanho de MTU por rota ou usar interfaces de rede elásticas com diferentes tipos de MTU e rotas diferentes.

Para instâncias posicionadas em um grupo de posicionamento de cluster, os frames jumbo ajudam a alcançar a máxima throughput de rede possível e são recomendados neste caso. Para ter mais informações, consulte Grupos de posicionamento.

É possível usar quadros jumbo para tráfego entre suas VPCs e suas redes on-premises por meio do AWS Direct Connect. Para obter mais informações e saber como verificar a capacidade de frames

jumbo, consulte Setting Network MTU (Configuração de MTU de rede) no Manual do usuário do AWS Direct Connect.

Todos os tipos de instância do Amazon EC2 são compatíveis com 1.500 MTU, e todos os tipos de instância da geração atual são compatíveis frames jumbo. Os seguintes tipos de instância da geração anterior são compatíveis com frames jumbo: A1, C3, I2, M3 e R3.

Para obter mais informações sobre os tamanhos de MTU compatíveis:

- Para gateways NAT, consulte NAT gateway basics no Manual do usuário da Amazon VPC.
- Para gateways de trânsito, consulte MTU no Amazon VPC Transit Gateways User Guide.
- Para zonas locais, consulte Considerations no AWS Local Zones User Guide.

Path MTU Discovery

A Path MTU Discovery (PMTUD) é usada para determinar a MTU do caminho entre dois dispositivos. A MTU do caminho é o tamanho de pacote máximo com suporte no caminho entre o host de origem e o host de recepção. Quando há alguma diferença no tamanho da MTU da rede entre dois hosts, a PMTUD permite que o host de recepção responda ao host de origem com uma mensagem de ICMP. Essa mensagem instrui o host de origem a usar o menor tamanho de MTU no caminho de rede para enviar novamente a solicitação. Sem essa negociação, a perda de pacotes pode ocorrer porque a solicitação é muito grande para o host aceitar.

Para o IPv4, quando um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou o dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

O protocolo IPv6 não é compatível com a fragmentação na rede. Se um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

As conexões feitas por meio de alguns componentes, como gateways NAT e balanceadores de carga, são rastreadas automaticamente. Isso significa que o rastreamento de grupos de segurança é habilitado automaticamente para suas tentativas de conexão de saída. Se as conexões forem

rastreadas automaticamente ou se as regras do seu grupo de segurança permitirem tráfego ICMP de entrada, você poderá receber respostas do PMTUD.

Observe que o tráfego ICMP pode ser bloqueado mesmo se o tráfego for permitido no nível do grupo de segurança, como se você tiver uma entrada na lista de controle de acesso à rede que negue o tráfego ICMP para a sub-rede.

> **Important**
>
> O Path MTU Discovery não garante que os quadros Jumbo não sejam descartados por alguns roteadores. Um gateway da Internet na VPC encaminhará somente pacotes de até 1.500 bytes. São recomendados pacotes de 1.500 MTU para o tráfico de Internet.

Verificar o MTU do caminho entre dois hosts

É possível verificar a MTU do caminho entre a instância EC2 e outro host. É possível especificar um nome DNS ou um endereço IP como o destino. Se o destino for outra instância do EC2, verifique se o grupo de segurança permite tráfego UDP de entrada.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Execute o comando tracepath na instância para verificar a MTU do caminho entre a instância EC2 e o destino especificado. Esse comando faz parte do pacote `iputils`, que está disponível, por padrão, em muitas distribuições do Linux.

Este exemplo verifica a MTU do caminho entre a instância do EC2 e o arquivo `amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

Neste exemplo de saída, a MTU do caminho é 1500.

```
1?: [LOCALHOST]      pmtu 9001
1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
1:  no reply
2:  no reply
3:  no reply
4:  100.64.16.241 (100.64.16.241)                             0.574ms
```

```
 5:  72.21.222.221 (72.21.222.221)                        84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                      79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                        96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                        79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                      91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Instâncias do Windows

Para verificar a MTU do caminho usando mturoute

1. Faça o download de mturoute.exe para a instância do EC2 em http://www.elifulkerson.com/projects/mturoute.php.
2. Abra uma janela do prompt de comando e altere para o diretório para onde você fez o download de mturoute.exe.
3. Use o comando apresentado a seguir para verificar a MTU do caminho entre a instância do EC2 e o destino especificado. Este exemplo verifica a MTU do caminho entre a instância do EC2 e o arquivo `www.elifulkerson.com`.

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   Neste exemplo de saída, a MTU do caminho é 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Verificação da MTU para a instância

É possível verificar o valor da MTU para a instância. Algumas instâncias são configuradas para usar frames jumbo, e outras são configuradas para usar tamanhos de quadro padrão.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Para verificar a configuração de MTU em uma instância do Linux

Execute o comando ip apresentado a seguir na instância do EC2. Se a interface de rede primária não for `eth0`, substitua `eth0` pela sua interface de rede.

```
[ec2-user ~]$ ip link show eth0
```

Neste exemplo de saída, *`mtu 9001`* indica que a instância usa frames jumbo.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Instâncias do Windows

O procedimento usado dependerá do driver da instância.

ENA driver

Versão 2.1.0 e versões posteriores

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Use o caractere curinga (asterisco) para obter todos os nomes Ethernet. Verifique a saída para o nome da interface `*JumboPacket`. Um valor de 9015 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versão 1.5 e versões anteriores

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Verifique a saída para o nome da interface `MTU`. Um valor de 9001 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Verifique entrada do nome da interface `*JumboPacket`. Um valor

de 9014 indica que os frames jumbo estão ativados. (Observe que o tamanho do MTU inclui o cabeçalho e a carga.) Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Para obter o valor da MTU, use o comando apresentado a seguir na instância do EC2. O nome da interface pode variar. Na saída, procure uma entrada intitulada "Ethernet", "Ethernet 2" ou "Conexão Local". Você precisará do nome da interface para ativar ou desativar os frames jumbo. Um valor de 9001 indica que os frames jumbo estão ativados.

```
netsh interface ipv4 show subinterface
```

Definição da MTU para a instância

Você pode querer usar frames jumbo para o tráfego de rede na VPC e frames padrão para o tráfego para a Internet. Seja qual for o seu caso de uso, recomendamos verificar se a instância se comporta conforme o esperado.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Para definir o valor de MTU em uma instância do Linux

1. Execute o comando ip apresentado a seguir na instância. O comando define o valor da MTU desejado para 1500, mas é possível usar 9001.

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (Opcional) Para persistir a configuração de MTU de rede após a reinicialização, modifique os arquivos de configuração a seguir com base no tipo de sistema operacional.

   - No Amazon Linux 2, adicione a linha a seguir ao arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0`:

     ```
     MTU=1500
     ```

Adicione a linha a seguir ao arquivo `/etc/dhcp/dhclient.conf`:

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name,
 domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
servers;
```

- Para o Amazon Linux AMI, adicione as seguintes linhas ao seu `/etc/dhcp/dhclient-eth0.conf` arquivo.

```
interface "eth0" {
supersede interface-mtu 1500;
}
```

- Para outras distribuições de Linux, consulte a documentação específica.

3. (Opcional) Reinicialize sua instância e verifique se a configuração de MTU está correta.

Instâncias do Windows

O procedimento usado dependerá do driver da instância.

ENA driver

É possível alterar a MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty na instância.

Versão 2.1.0 e versões posteriores

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versão 1.5 e versões anteriores

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

É possível alterar a MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty na instância.

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

É possível alterar a MTU usando o comando netsh na instância. Não é possível alterar a MTU usando o Gerenciador de Dispositivos.

Use o comando apresentado a seguir para habilitar frames jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Solução de problemas

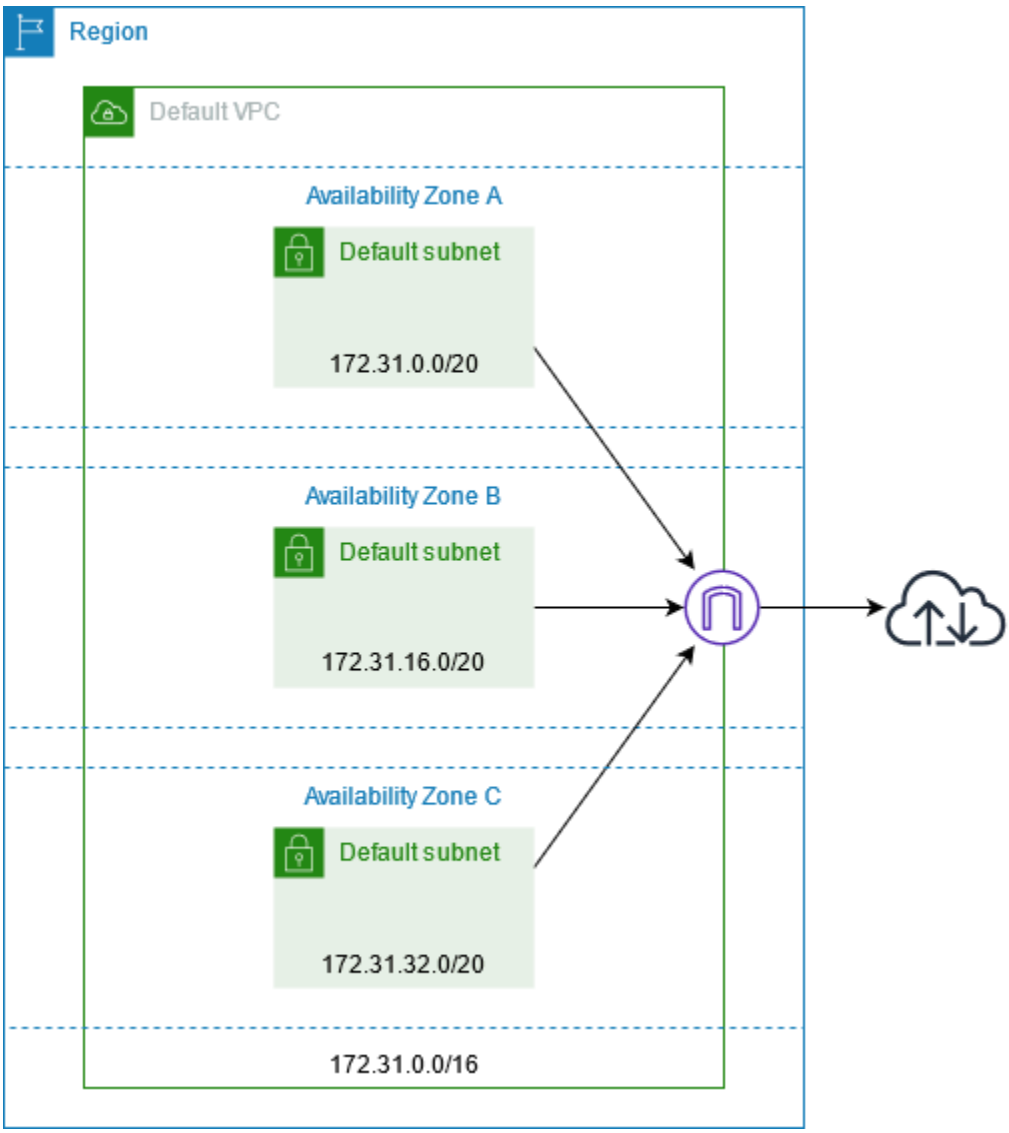
Se você tiver problemas de conectividade entre a instância do EC2 e um cluster do Amazon Redshift ao usar jumbo frames, consulte As consultas parecem travar no Guia de gerenciamento do Amazon Redshift.

Nuvens privadas virtuais para as instâncias do EC2

O Amazon Virtual Private Cloud (Amazon VPC) permite que você defina uma rede virtual em sua própria área logicamente isolada na nuvem AWS, conhecida como uma nuvem privada virtual ou VPC. É possível criar recursos da AWS, como instâncias do Amazon EC2, nas sub-redes da sua VPC. Sua VPC assemelha-se a uma rede tradicional que é possívelria operar no seu próprio data center, com os benefícios de usar a infraestrutura escalável da AWS. É possível configurar seu VPC, selecionar o intervalo de endereços IP dele, criar sub-redes e definir tabelas de rotas, gateways de rede e configurações de segurança. É possível conectar instâncias na VPC à Internet ou ao seu próprio data center.

Suas VPCs padrão

Quando você cria sua conta da AWS, nós criamos uma VPC padrão em cada região. Uma VPC padrão é uma VPC que já está configurada e pronta para uso. Por exemplo, há uma sub-rede padrão para cada zona de disponibilidade em cada VPC padrão, um gateway da Internet vinculado à VPC, e há uma rota na tabela de rotas principal que envia todo o tráfego (0.0.0.0/0) para o gateway da Internet. Como alternativa, você pode criar sua própria VPC padrão e configurá-la de acordo com suas necessidades.



Criar VPCs adicionais

Siga o procedimento abaixo para criar uma VPC com as sub-redes, gateways e a configuração de roteamento de que você precisa.

Para criar uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha Criar VPC.
3. Em Recursos a serem criados, escolha VPC e mais.
4. Em Name tag auto-generation (Geração automática de tags de nome), insira um nome para a VPC.

5. Em IPv4 CIDR block (Bloco CIDR IPv4), mantenha a sugestão padrão ou insira o bloco CIDR exigido por seu aplicativo ou rede.
6. Em Number of Availability Zones (Número de zonas de disponibilidade), escolha 2, para que você possa iniciar instâncias em várias zonas de disponibilidade para garantir alta disponibilidade.
7. Se for necessário tornar suas instâncias acessíveis pela Internet, faça o seguinte:
   - Se for possível manter suas instâncias em uma sub-rede pública, selecione um valor diferente de zero para Number of public subnets (Número de sub-redes públicas). Mantenha as duas opções em DNS options (Opções de DNS) selecionadas. Opcionalmente, você pode adicionar sub-redes privadas agora ou mais tarde.
   - Se for necessário manter suas instâncias em uma sub-rede privada, selecione 0 para Number of public subnets (Número de sub-redes públicas). Em Number of private subnets (Número de sub-redes privadas), selecione um número de acordo com o que você precisar (os valores possíveis correspondem a 1 ou 2 sub-redes privadas por zona de disponibilidade). Em NAT gateways (Gateways NAT), se suas instâncias em ambas as zonas de disponibilidade enviarem ou receberem um volume significativo de tráfego nas zonas de disponibilidade, selecione 1 per AZ (1 por AZ). Caso contrário, selecione In 1 AZ (Em 1 AZ) e execute instâncias que enviam ou recebem tráfego entre zonas na mesma zona de disponibilidade do gateway NAT.
8. Expanda Customize subnet CIDR blocks (Personalizar blocos CIDR de sub-rede). Mantenha as sugestões padrão ou insira um bloco CIDR para cada sub-rede. Para obter mais informações, consulte Blocos CIDR de sub-redes no Guia do usuário da Amazon VPC.
9. Examine o painel Preview (Visualização), que mostra os recursos da VPC que serão criados com base em suas seleções.
10. Escolha Criar VPC.

Acessar a Internet diretamente de suas instâncias

As instâncias iniciadas para uma sub-rede padrão em uma VPC padrão têm acesso à Internet, pois as VPCs padrão estão configuradas para atribuir endereços IP públicos e nomes de host do DNS, e a tabela de rotas principal está configurada com uma rota para um gateway da Internet conectado à VPC.

Para instâncias iniciadas em sub-redes e VPCs não padrão, você pode usar uma das seguintes opções para garantir que as instâncias iniciadas nessas sub-redes tenham acesso à Internet:

- Configurar um gateway da Internet. Para obter mais informações, consulte Estabelecer conexão com a Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.
- Configure um gateway NAT público. Para mais informações, consulte Acessar a Internet de uma sub-rede privada no Guia do usuário da Amazon VPC.

Sub-redes compartilhadas

Ao iniciar instâncias do EC2 em sub-redes de VPC compartilhadas, observe o seguinte:

- Os participantes podem executar instâncias em uma sub-rede especificando o ID da sub-rede compartilhada. Os participantes devem ser os proprietários de qualquer grupo de segurança ou interface de rede que especificarem.
- Os participantes podem iniciar, interromper, encerrar e descrever as instâncias que eles criaram em uma sub-rede compartilhada. Os participantes não podem iniciar, interromper, encerrar nem descrever as instâncias criadas pelo proprietário da VPC em uma sub-rede compartilhada.
- Os proprietários da VPC não podem iniciar, interromper, encerrar nem descrever as instâncias criadas pelos participantes em uma sub-rede compartilhada.
- Os participantes podem se conectar a uma instância em uma sub-rede compartilhada usando o endpoint de conexão de instância do EC2. O participante deve criar um endpoint de conexão de instância do EC2 na sub-rede compartilhada. Os participantes não podem usar o endpoint de conexão de instância do EC2 que o proprietário da VCP criou na sub-rede compartilhada.

Para obter mais informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Sub-redes somente IPv6

Uma instância do EC2 iniciada em uma sub-rede exclusivamente IPv6 recebe um endereço IPv6, mas não um endereço IPv4. As instâncias que são iniciadas em uma sub-rede somente IPv6 devem ser instâncias desenvolvidas no AWS Nitro System.

Segurança no Amazon EC2

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um data center e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem –- a AWS é responsável pela proteção da infraestrutura que executa serviços AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de compatibilidade que se aplicam ao Amazon EC2, consulte Serviços da AWS em escopo por programa de compatibilidade.
- Segurança na nuvem: sua responsabilidade inclui as seguintes áreas:
  - Controlar o acesso à rede para as instâncias, por exemplo, por meio da configuração da VPC e dos grupos de segurança. Para obter mais informações, consulte Controlar o tráfego de rede.
  - Gerenciar as credenciais usadas para a conexão às instâncias.
  - Gerenciar o sistema operacional convidado e o software implantado no sistema operacional convidado, incluindo atualizações e patches de segurança. Para obter mais informações, consulte Gerenciamento de atualizações para instâncias do Windows do Amazon EC2.
  - Configurar as funções do IAM anexadas à instância e as permissões associadas a estas funções. Para obter mais informações, consulte Funções do IAM para Amazon EC2.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon EC2. Ela mostra como configurar o Amazon EC2 para atender aos objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon EC2.

Conteúdo

- Proteção de dados no Amazon EC2
- Segurança da infraestrutura no Amazon EC2
- Resiliência no Amazon EC2

- Validação de conformidade do Amazon EC2
- Identity and Access Management para o Amazon EC2
- Acessar o Amazon EC2 usando um endpoint da VPC de interface
- Gerenciamento de atualizações para instâncias do Windows do Amazon EC2
- Práticas recomendadas de segurança para instâncias do Windows
- Pares de chaves do Amazon EC2 e instâncias do Amazon EC2
- Grupos de segurança do Amazon EC2 para as instâncias do EC2
- NitroTPM
- Credential Guard para instâncias do Windows

Proteção de dados no Amazon EC2

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Amazon Elastic Compute Cloud. Conforme descrito nesse modelo, AWS é responsável por proteger a infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e atividade do usuário logando com AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.

- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso também vale para o uso do Amazon EC2 ou de outros Serviços da AWS com o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Conteúdo

- Segurança de dados do Amazon EBS
- Criptografia em repouso
- Criptografia em trânsito

Segurança de dados do Amazon EBS

Os volumes do Amazon EBS são apresentados a você como dispositivos de bloco brutos e não formatados. Eles são dispositivos lógicos criados na infraestrutura do EBS, e o serviço Amazon EBS garante que os dispositivos estejam logicamente vazios (ou seja, os blocos brutos são zerados ou contêm dados pseudorrandomizados criptograficamente) antes de qualquer uso ou reutilização por um cliente.

Se você tiver procedimentos que exigem que todos os dados sejam apagados usando um método específico, após ou antes do uso (ou ambos), como aqueles detalhados em DoD 5220,22-M (Manual Operacional do Programa Nacional de Segurança Industrial) ou em NIST 800-88 (Diretrizes para higienização de mídia), será possível fazer isso no Amazon EBS. Essa atividade em nível de bloco será refletida na mídia de armazenamento subjacente dentro do serviço do Amazon EBS.

Criptografia em repouso

Volumes do EBS

A criptografia do Amazon EBS é uma solução de criptografia para snapshots e volumes do EBS. Ele usa a AWS KMS keys. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

[Instâncias do Windows] Você também pode usar permissões do Microsoft EFS e do NTFS para criptografia em nível de pastas e de arquivos.

Volumes de armazenamento de instâncias

Os dados nos volumes de armazenamento de instâncias de NVMe são criptografados usando uma criptografia XTS-AES-256 implementada em um módulo de hardware na instância. As chaves usadas para criptografar dados gravados em dispositivos de armazenamento NVMe conectados localmente são por cliente e por volume. As chaves são geradas e residem apenas dentro do módulo de hardware, que é inacessível para o pessoal da AWS. As chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode desativar essa criptografia e não pode fornecer sua própria chave de criptografia.

Os dados em volumes de armazenamento de instância HDD em instâncias H1, D3 e D3en são criptografados usando XTS-AES-256 e chaves de uso único.

Quando você interrompe, hiberna ou termina uma instância, cada bloco de armazenamento no volume do armazenamento de instância é redefinido. Portanto, seus dados não podem ser acessados por meio do armazenamento de instâncias de outra instância.

Memória

A criptografia de memória está habilitada nas seguintes instâncias:

- Instâncias com processadores AWS Graviton. AWS O Graviton2, o AWS Graviton3 e o AWS Graviton3E são compatíveis com criptografia de memória sempre ativa. As chaves de criptografia são geradas com segurança dentro do sistema host, não saem do sistema host e são destruídas quando o host é reinicializado ou desligado. Para obter mais informações, consulte Processadores AWS Graviton.
- Instâncias com processadores Intel Xeon Scalable de 3ª geração (Ice Lake), como instâncias M6i, e processadores Intel Xeon Scalable de 4ª geração (Sapphire Rapids), como instâncias M7i. Esses processadores são compatíveis com criptografia de memória sempre ativa usando a Intel Total Memory Encryption (TME).
- Instâncias com processadores AMD EPYC de 3ª geração (Milan), como instâncias M6a, e processadores AMD EPYC de 4ª geração (Genoa), como instâncias M7a. Esses processadores são compatíveis com criptografia de memória always-on usando Secure Memory Encryption

(SME) da AMD. Instâncias com processadores AMD EPYC de 3ª geração (Milan) também são compatíveis com Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) da AMD.

Criptografia em trânsito

Criptografia na camada física

Todos os dados fluindo pelas regiões da AWS por meio da rede global da AWS é automaticamente criptografada na camada física antes de sair das instalações seguras da AWS. Todo o tráfego entre AZs é criptografado. Camadas adicionais de criptografia, inclusive as listadas nesta seção, podem fornecer mais proteções.

Criptografia fornecida pelo emparelhamento da Amazon VPC e do Transit Gateway entre regiões

Todo o tráfego entre regiões que usa o emparelhamento da Amazon VPC e do Transit Gateway é automaticamente criptografado em massa ao sair de uma região. Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego antes que ele saia das instalações seguras da AWS, conforme observado anteriormente nesta seção.

Criptografia entre instâncias

A AWS fornece conectividade privada e segura entre instâncias do EC2 de todos os tipos. Além disso, alguns tipos de instância usam os recursos de descarregamento do hardware subjacente Nitro System para criptografar automaticamente o tráfego em trânsito entre instâncias. Essa criptografia usa algoritmos de criptografia autenticada com dados associados (AEAD) com criptografia de 256 bits. Não há impacto na performance da rede. Para oferecer suporte a essa criptografia adicional de tráfego em trânsito entre instâncias, os seguintes requisitos devem ser atendidos:

- As instâncias utilizam os seguintes tipos de instância:
  - Uso geral: M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i e M7i-flex
  - Otimizada para computação: C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i e C7i-flex
  - Otimizada para memória: R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iz, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, X2idn, X2iedn e X2iezn
  - Otimizada para armazenamento: D3, D3en, I3en, I4g, I4i, Im4gn e Is4gen
  - Com computação acelerada: DL1, DL2q, G4ad, G4dn, G5, G6, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, Trn1n e VT1

  - Computação de alta performance: Hpc6a, Hpc6id, Hpc7a, Hpc7g
- As instâncias estão na mesma região.
- As instâncias estão na mesma VPC ou VPCs emparelhadas, e o tráfego não passa por um dispositivo ou serviço de rede virtual, como um balanceador de carga ou um gateway de trânsito.

Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego antes que ele saia das instalações seguras da AWS, conforme observado anteriormente nesta seção.

Para visualizar os tipos de instância que criptografam o tráfego em trânsito entre instâncias usando o AWS CLI

Use o comando describe-instance-types a seguir.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Criptografia de e para o AWS Outposts

Um Outpost cria conexões de rede especiais chamadas links de serviço à região da AWS inicial e, opcionalmente, conectividade privada com uma sub-rede da VPC especificada. Todo o tráfego que passa por essas conexões é totalmente criptografado. Para obter mais informações, consulte Conectividade por meio de links de serviço e Criptografia em trânsito no Manual do usuário do AWS Outposts.

Criptografia de acesso remoto

Os protocolos SSH e RDP fornecem canais de comunicação seguros para acesso remoto às instâncias, seja diretamente, seja por meio do EC2 Instance Connect. O acesso remoto às instâncias usando o Gerenciador de Sessões ou o Run Command do AWS Systems Manager é criptografado usando TLS 1.2, e as solicitações para criar uma conexão são assinadas usando SigV4 e autenticadas e autorizadas pelo AWS Identity and Access Management.

É de sua responsabilidade usar um protocolo de criptografia, como o Transport Layer Security (TLS), para criptografar dados sigilosos em trânsito entre clientes e suas instâncias do Amazon EC2.

(Instâncias do Windows) Certifique-se de permitir somente conexões criptografadas entre as instâncias do EC2 e os endpoints da API da AWS ou outros serviços de rede remota confidenciais.

Isso pode ser imposto por meio do uso de grupo de segurança de saída ou regras de Firewall do Windows.

Segurança da infraestrutura no Amazon EC2

Como um serviço gerenciado, o Amazon Elastic Compute Cloud é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Well-Architected Framework.

Você usa chamadas à API publicadas pela AWS para acessar o Amazon EC2 por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Para obter mais informações, consulte Proteção de infraestrutura no Pilar de Segurança: AWS Well-Architected Framework.

Isolamento de rede

Uma nuvem virtual privada (VPC) é uma rede virtual na área isolada logicamente na Nuvem AWS. Use VPCs separadas para isolar a infraestrutura por workload ou entidade organizacional.

Uma sub-rede é um intervalo de endereços IP em uma VPC. Quando executa uma instância, você a executa em uma sub-rede em sua VPC. Use sub-redes para isolar as camadas de sua aplicação (por exemplo, Web, aplicação e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet.

Para chamar a API do Amazon EC2 da sua VPC usando endereços IP privados, use o AWS PrivateLink. Para ter mais informações, consulte Acessar o Amazon EC2 usando um endpoint da VPC de interface.

Isolamento em hosts físicos

Diferentes instâncias do EC2 no mesmo host físico são isoladas umas das outras como se estivessem em hosts físicos separados. O hipervisor isola a CPU e a memória, e as instâncias recebem discos virtualizados em vez de acesso aos dispositivos de disco bruto.

Quando você interrompe ou encerra uma instância, a memória alocada para ela é apagada (definida como zero) pelo hipervisor antes que ela seja alocada para uma nova instância, e cada bloco de armazenamento é redefinido. Isso garante que seus dados não sejam expostos acidentalmente para outra instância.

Os endereços MAC de rede são atribuídos dinamicamente às instâncias pela infraestrutura da rede da AWS. Os endereços IP são atribuídos dinamicamente a instâncias pela infraestrutura de rede da AWS ou atribuídos por um administrador do EC2 por meio de solicitações autenticadas da API. A rede da AWS permite que as instâncias enviem tráfego somente de endereços MAC e IP atribuídos a elas. Caso contrário, o tráfego será descartado.

Por padrão, uma instância não pode receber tráfego que não seja endereçado especificamente a ela. Se for necessário executar a conversão de endereço de rede (NAT), o roteamento ou os serviços de firewall em sua instância, será possível desabilitar a verificação de origem/destino da interface de rede.

Controlar o tráfego de rede

Considere as seguintes opções de controle de tráfego de rede para suas instâncias do EC2:

- Restrinja o acesso a suas instâncias usando grupos de segurança. Configure regras que permitam o tráfego de rede mínimo necessário. Por exemplo, é possível permitir o tráfego somente dos intervalos de endereços da rede corporativa ou apenas para protocolos específicos, como HTTPS. Para instâncias do Windows, permita o tráfego de gerenciamento do Windows e as conexões de saída mínimas.
- Use os grupos de segurança como o mecanismo primário a fim de controlar o acesso à rede para instâncias do Amazon EC2. Quando necessário, use as ACLs de rede para fornecer controle de rede sem estado e de alta granularidade. Os grupos de segurança são mais versáteis que as ACLs de rede devido à capacidade de realizar a filtragem de pacotes com estado e criar regras que

fazem referência a outros grupos de segurança. No entanto, as ACLs de rede podem ser eficientes como um controle secundário para negar um subconjunto ou tráfego específico ou fornecer grades de proteção de sub-rede de alto nível. Além disso, como as ACLs de rede se aplicam a toda uma sub-rede, elas podem ser usadas como defesa em profundidade caso uma instância seja iniciada de forma não intencional sem um grupo de segurança correto.

- [Instâncias do Windows] Gerencie as configurações do Firewall do Windows, de maneira centralizada, com os Objetos de Política de Grupo (GPO) para aprimorar ainda mais os controles de rede. Os clientes costumam usar o Firewall do Windows para obter maior visibilidade do tráfego de rede e para complementar os filtros de grupo de segurança, criando regras avançadas para impedir que aplicações específicas acessem a rede ou filtrem o tráfego de endereços IP de um subconjunto. Por exemplo, o Firewall do Windows pode limitar o acesso ao endereço IP do serviço de metadados do EC2 para usuários ou aplicações específicas. Como alternativa, um serviço voltado para o público pode usar grupos de segurança para restringir o tráfego a portas específicas e o Firewall do Windows a manter uma lista negra de endereços IP explicitamente bloqueados.
- Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet. Use um bastion host ou gateway NAT para acesso à Internet em uma instância em uma sub-rede privada.
- [Instâncias do Windows] Use protocolos de administração seguros, como o encapsulamento de RDP sobre SSL e TLS. O Quick Start para Gateway de Desktop Remoto fornece as melhores práticas para implantar um gateway de desktop remoto remota, incluindo a configuração de RDP para usar SSL/TLS.
- [Instâncias do Windows] Use o Active Directory ou o AWS Directory Service para controlar e monitorar, de forma rígida e centralizada, o acesso interativo de usuários e de grupos às instâncias do Windows e evitar permissões de usuários locais. Evite também usar Administradores de domínio e, em vez disso, crie contas baseadas em função mais granulares e específicas para a aplicação. A Administração Suficiente (JEA) permite que as alterações nas instâncias do Windows sejam gerenciadas sem acesso interativo ou de administrador. Além disso, a JEA permite que as organizações bloqueiem o acesso administrativo ao subconjunto dos comandos do Windows PowerShell necessários para a administração da instância. Para obter informações adicionais, consulte a seção "Gerenciamento de acesso a nível de SO para o Amazon EC2" no whitepaper Práticas recomendadas de segurança da AWS.
- [Instâncias do Windows] Os administradores de sistema devem usar contas do Windows com acesso limitado para realizar atividades diárias e elevar o acesso somente quando necessário para realizar alterações específicas na configuração. Além disso, somente acesse as instâncias do Windows diretamente quando absolutamente necessário. Em vez disso, use os sistemas

de gerenciamento de configuração central, como o Run Command do EC2, o Systems Center Configuration Manager (SCCM), o Windows PowerShell DSC ou o Amazon EC2 Systems Manager (SSM), para enviar as alterações aos servidores Windows.

- Configure as tabelas de rotas de sub-rede da Amazon VPC com as rotas de rede mínimas necessárias. Por exemplo, estabeleça somente instâncias do Amazon EC2 que requerem acesso direto à Internet em sub-redes com rotas para um gateway da Internet, e estabeleça somente instâncias do Amazon EC2 que precisam de acesso direto a redes internas em sub-redes com rotas para um gateway privado virtual.
- Considere usar grupos de segurança adicionais ou interfaces de rede para controlar e auditar o tráfego de gerenciamento de instâncias do Amazon EC2 separadamente do tráfego de aplicação regular. Esta abordagem permite que os clientes implementem políticas do IAM especiais para o controle de alterações, facilitando a auditoria de alterações às regras de grupo de segurança ou scripts automáticos de verificação de regras. O uso de diversas interfaces de rede também oferece opções adicionais para controlar o tráfego de rede, incluindo a capacidade de criar políticas de roteamento baseadas em host ou aproveitar diferentes regras de roteamento de sub-rede da VPC com base na sub-rede atribuída da interface de rede.
- Use o AWS Virtual Private Network ou o AWS Direct Connect para estabelecer conexões privadas de suas redes remotas com suas VPCs. Para obter mais informações, consulte Opções de conectividade entre a rede e a Amazon VPC.
- Use Logs de fluxo da VPC para monitorar o tráfego recebido nas instâncias.
- Use a proteção contra malware do GuardDuty para identificar comportamentos suspeitos indicativos de softwares mal-intencionados em suas instâncias que podem comprometer a workload, redirecionar recursos para o uso mal-intencionado e obter acesso não autorizado aos dados.
- Use o monitoramento do runtime do GuardDuty para identificar e responder a possíveis ameaças às instâncias. Para obter mais informações, consulte How Runtime Monitoring works with Amazon EC2 instances.
- Use o AWS Security Hub, o Reachability Analyzer ou o Analisador de Acesso à Rede para verificar se há acessibilidade não intencional à rede em suas instâncias.
- Use o EC2 Instance Connect para se conectar a suas instâncias usando Secure Shell (SSH) sem a necessidade de compartilhar e gerenciar chaves SSH.
- Use o Gerenciador de Sessões do AWS Systems Manager para acessar as instâncias remotamente em vez de abrir portas SSH ou RDP de entrada e gerenciar pares de chaves.

- Use o Run Command do AWS Systems Manager para automatizar as tarefas administrativas comuns em vez de realizar conexão com as instâncias.
- [Instâncias do Windows] Muitos dos perfis do sistema operacional do Windows e das aplicações de negócios da Microsoft também fornecem funcionalidades aprimoradas, como restrições de intervalo de endereços IP no IIS, políticas de filtragem de TCP/IP no Microsoft SQL Server e políticas de filtragem de conexão no Microsoft Exchange. A funcionalidade de restrição de rede na camada de aplicação pode fornecer camadas adicionais de defesa para servidores de aplicação de negócios críticos.

A Amazon VPC oferece suporte a controles adicionais de segurança de rede, como gateways, servidores proxy e opções de monitoramento de rede. Para obter mais informações, consulte Control network traffic no Guia do usuário da Amazon VPC.

Resiliência no Amazon EC2

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Se você precisar replicar seus dados ou aplicações para distâncias geográficas maiores, use as zonas locais da AWS. Uma zona local da AWS é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As zonas locais têm suas próprias conexões com a Internet e suporte no AWS Direct Connect. Como todas as regiões da AWS, as zonas locais da AWS são completamente isoladas de outras zonas da AWS.

Se você precisar replicar seus dados ou aplicações em uma zona local da AWS, a AWS recomenda que você use uma das seguintes zonas como zona de failover:

- Outra zona local
- Uma zona de disponibilidade na região que não é a zona principal. É possível usar o comando describe-availability-zones para visualizar a zona principal.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, o Amazon EC2 oferece os seguintes recursos para oferecer suporte à resiliência de seus dados:

- Copiar AMIs entre regiões
- Copiar snapshots do EBS entre regiões
- Automatizando AMIs compatíveis com EBS usando o Amazon Data Lifecycle Manager
- Automatizar snapshots do EBS usando o Amazon Data Lifecycle Manager
- Manter a integridade e a disponibilidade da frota usando o Amazon EC2 Auto Scaling
- Distribuir o tráfego de entrada entre instâncias em uma única zona de disponibilidade ou em várias zonas de disponibilidade usando o Elastic Load Balancing.

Validação de conformidade do Amazon EC2

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido de segurança e conformidade: estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services: esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

> **Note**
>
> Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- Recursos de Conformidade da AWS: essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config: o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty: este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados ao monitorar o ambiente em busca de atividades suspeitas e maliciosas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Identity and Access Management para o Amazon EC2

As credenciais de segurança identificam você para os serviços na AWS e concedem uso ilimitado dos recursos da AWS, como os recursos do Amazon EC2. É possível usar recursos do Amazon EC2 e do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e

aplicações usem seus recursos do Amazon EC2 sem compartilhar suas credenciais de segurança. É possível usar o IAM para controlar como outros usuários usam recursos em sua conta da AWS, e usar os grupos de segurança para controlar o acesso às instâncias do Amazon EC2. É possível escolher permitir uso completo ou limitado dos recursos do Amazon EC2.

Para práticas recomendadas de proteção dos seus recursos do AWS usando o IAM, consulte Práticas recomendadas de segurança no IAM.

Conteúdo

- Acesso à rede para a instância
- Atributos de permissões do Amazon EC2
- IAM e Amazon EC2
- Políticas do IAM no Amazon EC2
- Políticas gerenciadas pela AWS para o Amazon EC2
- Funções do IAM para Amazon EC2

Acesso à rede para a instância

Um grupo de segurança atua como um firewall que controla o tráfego permitido para acessar uma ou mais instâncias. Quando executa uma instância, você atribui um ou mais grupos de segurança a ela. Para cada grupo de segurança, você adiciona regras que controlam o tráfego para a instância. É possível modificar as regras de um grupo de segurança a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

Para ter mais informações, consulte Regras de grupos de segurança.

Atributos de permissões do Amazon EC2

Sua organização pode ter várias contas da AWS. O Amazon EC2 permite que você especifique contas adicionais da AWS que podem usar as Imagens de máquinas da Amazon (AMIs) e snapshots do Amazon EBS. Essas permissões funcionam somente em nível de conta da AWS. Você não pode restringir as permissões a usuários específicos na conta da AWS especificada. Todos os usuários na conta da AWS que você especifica podem usar a AMI ou o snapshot.

Cada AMI tem um atributo `LaunchPermission` que controla quais contas da AWS podem acessar a AMI. Para obter mais informações, consulte Tornar um AMI pública.

Cada snapshot do Amazon EBS tem um atributo `createVolumePermission` que controla quais contas da AWS podem usar o snapshot. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS.

IAM e Amazon EC2

O IAM permite que você:

- Crie usuários e grupos na sua Conta da AWS
- Atribua credenciais de segurança exclusivas a cada usuário em sua Conta da AWS
- Controle as permissões de cada usuário para executar tarefas usando recursos da AWS
- Permita que os usuários em outra Conta da AWS compartilhem seus recursos da AWS
- Crie perfis para sua Conta da AWS e defina os usuários ou os serviços que podem assumi-las
- Use identidades existentes em sua empresa a fim de conceder permissões para executar tarefas usando recursos da AWS

Ao usar o IAM com o Amazon EC2, é possível controlar se os usuários de sua organização podem executar uma tarefa usando ações específicas da API do Amazon EC2 e se podem usar recursos específicos da AWS.

Este tópico ajuda a responder as seguintes questões:

- Como criar grupos e usuários no IAM?
- Como criar uma política?
- Quais políticas do IAM são necessárias para realizar tarefas no Amazon EC2?
- Como conceder permissões para executar ações no Amazon EC2?
- Como conceder permissões para executar ações em recursos específicos do Amazon EC2?

Crie usuários, grupos e perfis

Você pode criar usuários e grupos para sua Conta da AWS e, em seguida, atribuir a eles as permissões necessárias. Como prática recomendada, os usuários devem adquirir as permissões assumindo perfis do IAM.

Um perfil do IAM é uma identidade do IAM que você pode criar em sua conta que tem permissões específicas. Um perfil do IAM é semelhante a um usuário do IAM porque é uma identidade da AWS

com políticas de permissão que determinam o que ela pode e não pode fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Além disso, um perfil não tem credenciais de longo prazo padrão associadas a ele, como senha ou chaves de acesso. Em vez disso, quando você assumir um perfil, ele fornecerá credenciais de segurança temporárias para sua sessão de perfil. Para obter mais informações sobre como criar perfis do IAM e conceder permissões a eles, consulte the section called “Funções do IAM”.

Tópicos relacionados da

Para mais informações sobre IAM, consulte o seguinte:

- Políticas do IAM no Amazon EC2
- Funções do IAM para Amazon EC2
- AWS Identity and Access Management (IAM)
- Guia do usuário do IAM

Políticas do IAM no Amazon EC2

Por padrão, os usuários não têm permissão para criar ou modificar recursos do Amazon EC2 ou para executar tarefas usando a API do Amazon EC2, o colsole do Amazon EC2 ou a CLI. Para permitir que os usuários criem ou modifiquem recursos e realizem tarefas, você precisa criar políticas do IAM que concedam aos usuários do permissão para usar os recursos específicos e as ações de API de que precisam e, então, anexar essas políticas aos usuários ou grupos, ou perfis do IAM que exijam essas permissões.

Quando você anexa uma política a um usuário, um grupo de usuários ou um perfil, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos recursos especificados. Para obter mais informações gerais sobre as políticas do IAM, consulte Permissões e políticas no IAM no Guia do usuário do IAM. Para obter mais informações sobre como gerenciar e criar políticas personalizadas do IAM, consulte Gerenciamento de políticas do IAM.

Conceitos Básicos

Uma política do IAM deve conceder ou negar permissões para usar uma ou mais ações do Amazon EC2. Ela também deve especificar os recursos que podem ser usados com a ação, que podem ser todos os recursos ou, em alguns casos, recursos específicos. A política também pode incluir condições que você aplica ao recurso.

O Amazon EC2 oferece suporte parcial a permissões em nível de recurso. Isso significa que, para algumas operações de API do EC2, não é possível especificar com qual recurso um usuário tem permissão para trabalhar para essa ação. Em vez disso, você precisa permitir que os usuários trabalhem com todos os recursos dessa ação.

Tarefa	Tópico
Compreender a estrutura básica de uma política	Sintaxe da política
Definir ações em sua política	Ações do Amazon EC2
Definir recursos específicos em sua política	Nomes de recurso da Amazon (ARNs) para o Amazon EC2
Aplicar condições ao uso dos recursos	Chaves de condição do Amazon EC2
Trabalhar com permissões disponíveis em nível de recurso para o Amazon EC2	Ações, recursos e chaves de condição para o Amazon EC2
Testar a política	Verificar se os usuários têm as permissões necessárias
Gerar uma política do IAM	Gerar políticas com base na atividade de acesso
Políticas de exemplo para uma CLI ou SDK	Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK
Políticas de exemplo para o console do Amazon EC2	Políticas de exemplo para trabalhar no console do Amazon EC2

Conceder permissões a usuários, grupos e perfis

A seguir estão exemplos de algumas políticas gerenciadas da AWS que estão disponíveis para utilização se atenderem às suas necessidades:

- `PowerUserAccess`
- `ReadOnlyAccess`

- `AmazonEC2FullAccess`
- `AmazonEC2ReadOnlyAccess`

Para ter mais informações, consulte the section called “Políticas gerenciadas pela AWS”.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Estrutura da política

Os tópicos a seguir explicam a estrutura de uma política do IAM.

Tópicos

- Sintaxe da política
- Ações do Amazon EC2
- Permissões no nível do recurso com suporte para ações de API do Amazon EC2
- Nomes de recurso da Amazon (ARNs) para o Amazon EC2
- Chaves de condição do Amazon EC2
- Verificar se os usuários têm as permissões necessárias

Sintaxe da política

A política do IAM é um documento JSON que consiste em uma ou mais declarações. Cada instrução é estruturada da maneira a seguir.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Existem vários elementos que compõem uma instrução:

- Efeito: o efeito pode ser `Allow` ou `Deny`. Por padrão, os usuários não têm permissão para usar recursos e ações da API. Por isso, todas as solicitações são negadas. Um permitir explícito substitui o padrão. Uma negação explícita substitui todas as permissões.
- Action: a ação é a ação de API específica para a qual você está concedendo ou negando permissão. Para conhecer como especificar ação, consulte Ações do Amazon EC2.
- Resource: o recurso afetado pela ação. Algumas ações de API do Amazon EC2 permitem incluir recursos específicos na política que podem ser criados ou modificados pela ação. Você especifica um recurso usando um nome de recurso da Amazon (ARN) ou usando o caractere curinga (*) para indicar que a instrução se aplica a todos os recursos. Para obter mais informações, consulte Permissões no nível do recurso com suporte para ações de API do Amazon EC2.
- Condition: condições são opcionais. Elas podem ser usadas para controlar quando a política está em vigor. Para obter mais informações sobre como especificar condições para o Amazon EC2, consulte Chaves de condição do Amazon EC2.

Para obter mais informações sobre requisitos de políticas, consulte a Referência de política JSON do IAM no Guia do usuário do IAM. Para obter um exemplo de declarações de políticas do IAM para o Amazon EC2, consulte Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK.

Ações do Amazon EC2

Em uma declaração de política do IAM, é possível especificar qualquer ação de API de qualquer serviço que dê suporte ao IAM. Para o Amazon EC2, use o seguinte prefixo com o nome da ação da API: `ec2:`. Por exemplo: `ec2:RunInstances` e `ec2:CreateImage`.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme o seguinte:

```
"Action": ["ec2:action1", "ec2:action2"]
```

Também é possível especificar várias ações usando caracteres curinga. Por exemplo, é possível especificar todas as ações cujo nome começa com a palavra "Describe" da seguinte forma:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> No momento, as ações de API do Amazon EC2 não são compatíveis com permissões em nível de recurso. Para obter mais informações sobre permissões no nível do recurso para o Amazon EC2, consulte Políticas do IAM no Amazon EC2.

Para especificar todas as ações de API do Amazon EC2, use o curinga "*" da seguinte maneira:

```
"Action": "ec2:*"
```

Para obter uma lista de ações de Amazon EC2, consulte Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

Permissões no nível do recurso com suporte para ações de API do Amazon EC2

Permissões no nível do recurso se referem à capacidade de especificar em quais recursos os usuários têm permissão para realizar ações. O Amazon EC2 tem suporte parcial para permissões no nível do recurso. Isso significa que, para determinadas ações do Amazon EC2, é possível controlar quando os usuários têm permissão para usar essas ações com base em condições que precisam ser concluídas, ou em recursos específicos que os usuários têm permissão para usar. Por exemplo, é possível conceder aos usuários permissões para ativar instâncias, mas apenas de um tipo específico, e usando uma AMI específica.

Para especificar um recurso em uma declaração de política do IAM, use o respectivo nome de recurso da Amazon (ARN). Para obter mais informações sobre como especificar o valor do ARN, consulte Nomes de recurso da Amazon (ARNs) para o Amazon EC2. Se uma ação de API não oferecer suporte a ARNs individuais, você deverá usar um curinga (*) para especificar que todos os recursos podem ser afetados pela ação.

Para visualizar tabelas que identificam quais ações de API do Amazon EC2 oferecem suporte a permissões no nível do recurso e os ARNs e chaves de condição que é possível usar em uma política, consulte Ações, recursos e chaves de condição do Amazon EC2 .

Lembre-se de que é possível aplicar permissões em nível de recurso baseadas em tags às políticas do IAM que você usa para a maioria das ações da API do Amazon EC2. Isso oferece a você mais controle sobre quais recursos o usuário pode criar, modificar ou usar. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

Nomes de recurso da Amazon (ARNs) para o Amazon EC2

Cada declaração de política do IAM se aplica aos recursos que você especifica usando os ARNs.

Um ARN tem a seguinte sintaxe geral:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

serviço

O serviço (por exemplo, `ec2`).

região

A região do recurso (por exemplo, `us-east-1`).

account-id

O ID da conta da AWS, sem hifens (por exemplo, `123456789012`).

resourceType

O tipo de recurso (por exemplo, `instance`).

resourcePath

Um caminho que identifica o recurso. É possível usar o curinga * nos caminhos.

Por exemplo, é possível indicar uma instância específica (`i-1234567890abcdef0`) na declaração usando o ARN da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

É possível especificar todas as instâncias pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Também é possível especificar todos os recursos do Amazon EC2 pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Para especificar todos os recursos ou caso uma ação de API específica não dê suporte a ARNs, use o curinga * no elemento `Resource` da maneira a seguir.

```
"Resource": "*"
```

Muitas ações da API do Amazon EC2 envolvem vários recursos. Por exemplo, `AttachVolume` anexa um volume do Amazon EBS a uma instância, portanto, um usuário precisa ter permissões para usar o volume e a instância. Para especificar vários recursos em uma única instrução, separe seus ARNs com vírgulas, como se segue.

```
"Resource": ["arn1", "arn2"]
```

Para obter uma lista de ARNs para recursos do Amazon EC2, consulte Tipos de recursos definidos pelo Amazon EC2.

Chaves de condição do Amazon EC2

Ema uma instrução de política, também é possível especificar condições que controlam quando ela entrará em vigor. Cada condição contém um ou mais pares de chave-valor. As chaves de condição não diferenciam maiúsculas de minúsculas. Definimos chaves de condição global da AWS, além de chaves de condição específicas do serviço adicionais.

Para obter uma lista de chaves de condição específicas do serviço para o Amazon EC2, consulte Condition keys for Amazon EC2 (Chaves de condição para o Amazon EC2). O Amazon EC2

também implementa as chaves de condição globais da AWS. Para obter mais informações, consulte Informações disponíveis em todas as solicitações no Guia do usuário do IAM.

Para usar uma chave de condição em sua política do IAM, use a instrução `Condition`. Por exemplo, a política a seguir concede aos usuários permissão para adicionar e remover regras de entrada e saída para qualquer grupo de segurança. Ela usa a chave de condição `ec2:Vpc` para especificar que essas ações só podem ser executadas em grupos de segurança em uma VPC específica.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
    }
  ]
}
```

Caso você especifique várias condições ou várias chaves em uma única condição, avaliamos essas condições usando uma operação AND lógica. Caso você especifique uma única condição com vários valores para uma chave, avaliamos a condição usando uma operação OR lógica. Para que as permissões sejam concedidas, todas as condições devem ser atendidas.

Também é possível usar espaços reservados quando especifica as condições. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

> **Important**
>
> Muitas chaves de condição são específicas a um recurso, e algumas ações da API usam vários recursos. Se você gravar uma política com uma chave de condição, use o elemento `Resource` da declaração para especificar o recurso ao qual a chave de condição se aplica.

Caso contrário, as políticas podem impedir que os usuários executem a ação, porque a verificação da condição falha para os recursos aos quais a chave de condição não se aplica. Se você não quiser especificar um recurso, ou se escreveu o elemento `Action` da política para incluir várias ações da API, será necessário usar o tipo de condição `...IfExists` para garantir que a chave de condição seja ignorada pelos recursos que não a usam. Para obter mais informações, consulte Condições ...IfExists no Guia do usuário do IAM.

Todas as ações do Amazon EC2 oferecem suporte às chaves de condição `aws:RequestedRegion` e `ec2:Region`. Para ter mais informações, consulte Exemplo: restringir acesso a uma região específica.

Chave da condição ec2:Attribute

A chave de condição `ec2:Attribute` pode ser usada para condições que filtram o acesso por um atributo de um recurso. A chave de condição oferece suporte somente a propriedades que sejam de um tipo de dados primitivo (como uma string ou um inteiro) ou objetos complexos AttributeValue que tenham apenas uma propriedade Value (como os objetos Description ou ImdsSupport da ação de API ModifyImageAttribute).

Important

A chave de condição não pode ser usada com objetos complexos que tenham várias propriedades, como o objeto LaunchPermission da ação da API ModifyImageAttribute.

Por exemplo, a política a seguir usa a chave de condição `ec2:Attribute/Description` para filtrar o acesso pelo objeto complexo Descrição da ação da API ModifyImageAttribute. A chave de condição permite somente solicitações que modifiquem a descrição de uma imagem para `Production` ou `Development`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
```

```
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

A política a seguir usa a chave de condição `ec2:Attribute` para filtrar o acesso pela propriedade primitiva Atributo da ação da API ModifyImageAttribute. A chave de condição recusa todas as solicitações que tentam modificar a descrição de uma imagem.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

Chaves de condição do ec2:ResourceID

Quando as chaves de condição `ec2:`*`Resource`*`ID` a seguir forem usadas com as ações de API especificadas, o valor da chave de condição será usado para especificar o recurso resultante criado pela ação da API. As chaves de condição `ec2:`*`Resource`*`ID` não podem ser usadas para especificar um recurso de origem especificado na solicitação da API. Se você usar uma das chaves de condição `ec2:`*`Resource`*`ID` a seguir com uma API especificada, será necessário especificar sempre o curinga (*). Se você especificar um valor diferente, a condição sempre será resolvida para * em runtime. Por exemplo, para usar a chave de condição `ec2:ImageId` com a API CopyImage, será necessário especificar a chave de condição da seguinte forma:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Recomendamos evitar usar estas chaves de condição com estas ações de API:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID` – `CopyImage`, `CreateImage`, `ImportImage` e `RegisterImage`
- `ec2:InstanceID`: `RunInstances` e `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID` – `CopySnapshot`, `CreateSnapshot`, `CreateSnapshots` e `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID`: `CreateVolume` e `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Para filtrar o acesso com base em IDs de recursos específicos, recomendamos usar o elemento de política `Resource` conforme descrito a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Chave da condição ec2:SourceInstanceARN

Use `ec2:SourceInstanceARN` para especificar o ARN da instância a partir da qual uma solicitação é feita. Essa é uma chave de condição global da AWS, o que significa que é possíve usá-la com outros serviços além do Amazon EC2. Para ver um exemplo de política, consulte Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS.

Verificar se os usuários têm as permissões necessárias

Depois que você tiver criado uma política do IAM, recomendaremos verificar se ela concede aos usuários as permissões para usar as ações de API e os recursos específicos de que eles precisam antes de colocar a política em produção.

Primeiro, crie um usuário para fins de teste e anexe a política do IAM que você criou ao usuário de teste. Em seguia, faça uma solicitação como o usuário de teste.

Se a ação do Amazon EC2 que você estiver testando criar ou modificar um recurso, será necessário fazer a solicitação usando o parâmetro `DryRun` (ou executar o comando da AWS CLI com a opção `--dry-run`). Nesse caso, a chamada conclui a verificação da autorização, mas não conclui a operação. Por exemplo, é possível verificar se o usuário pode encerrar uma determinada instância sem efetivamente encerrá-la. Caso o usuário de teste tenha as permissões obrigatórias, a solicitação retorna `DryRunOperation`. Do contrário, ela retorna `UnauthorizedOperation`.

Caso a política não conceda ao usuário as permissões que você esperava ou caso ela seja muito permissiva, é possível ajustar a política conforme necessário e testá-la novamente até obter os resultados desejados.

> **Important**
>
> Pode levar alguns minutos para que as alterações de política sejam propagadas até entrarem em vigor. Por isso, recomendamos que você aguarde cinco minutos antes de testar as atualizações da política.

Caso uma verificação de autorização falhe, a solicitação retorna uma mensagem codificada com informações de diagnóstico. É possível decodificar a mensagem usando a ação `DecodeAuthorizationMessage`. Para obter mais informações, consulte DecodeAuthorizationMessage na Referência de API do AWS Security Token Service e decode-authorization-message na Referência de comandos da AWS CLI.

Conceder permissão para marcar recursos durante a criação

Algumas ações de resource-creating da API do Amazon EC2 permitem especificar tags quando você cria o recurso. É possível usar tags de recursos para implementar o controle baseado em atributo (ABAC). Para ter mais informações, consulte Marcar com tag os recursos do e Controlar o acesso aos recursos do EC2 usando tags de recursos.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso, como `ec2:RunInstances` ou `ec2:CreateVolume`. Se as tags forem especificadas na ação resource-creating, a Amazon executará autorização adicional na ação `ec2:CreateTags` para verificar se os usuários têm permissões para criar tags. Portanto, os usuários também precisam ter permissões para usar a ação `ec2:CreateTags`.

Na definição de política do IAM para a ação `ec2:CreateTags`, use o elemento `Condition` com a chave de condição `ec2:CreateAction` para conceder permissões de marcação à ação que cria o recurso.

O exemplo a seguir demonstra uma política que permite que os usuários executem instâncias e apliquem tags a instâncias e volumes durante a execução. Os usuários não têm permissão para marcar recursos existentes (não podem chamar a ação `ec2:CreateTags` diretamente).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:RunInstances"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:region:account:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
            }
        }
    }
  ]
}
```

Da mesma forma, a política a seguir permite que os usuários criem volumes e apliquem qualquer tag aos volumes durante a criação do volume. Os usuários não têm permissão para marcar recursos existentes (não podem chamar a ação `ec2:CreateTags` diretamente).

```
{
  "Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateVolume"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:region:account:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "CreateVolume"
            }
        }
```

```
    }
  ]
}
```

A ação `ec2:CreateTags` será avaliada somente se as tags forem aplicadas durante a ação resource-creating. Portanto, um usuário que tiver permissões para criar um recurso (pressupondo-se que não existam condições de marcação) não precisa de permissão para usar a ação `ec2:CreateTags` se nenhuma tag for especificada na solicitação. Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `ec2:CreateTags`.

A ação `ec2:CreateTags` também é avaliada se as tags forem fornecidas em um modelo de execução. Para visualizar um exemplo de política, consulte Tags em um modelo de execução.

Controlar o acesso a tags específicas

É possível usar condições adicionais no elemento `Condition` de suas políticas do IAM para controlar as chaves de tag e os valores que podem ser aplicados aos recursos.

As chaves de condição a seguir podem ser usadas com os exemplos na seção anterior:

- `aws:RequestTag`: para indicar que uma chave de tag ou uma chave e um valor de tag específicos devem estar presentes em uma solicitação. Outras tags também podem ser especificadas na solicitação.
  - Use com o operador de condição `StringEquals` para impor uma combinação de chave e valor de tag específica, por exemplo, para impor a tag `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Use com o operador de condição `StringLike` para impor uma chave de tag específica, por exemplo, para impor a chave de tag `purpose`:

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- `aws:TagKeys`: para aplicar as chaves de tags usadas na solicitação.
  - Use com o modificador `ForAllValues` para impor chaves de tags específicas se forem fornecidas na solicitação (se as tags forem especificadas na solicitação, somente chaves de tags específicas são permitidas; nenhuma outra tag é permitida). Por exemplo, as chaves de tags `environment` ou `cost-center` são permitidas:

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

- Use com o modificador `ForAnyValue` para impor a presença de pelo menos uma das chaves de tags especificadas na solicitação. Por exemplo, pelo menos uma das chaves de tags `environment` ou `webserver` deve estar presente na solicitação:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Essas chaves de condição podem ser aplicadas às ações resource-creating que são compatíveis com a marcação bem como as ações `ec2:CreateTags` e `ec2:DeleteTags`. Para saber se uma ação de API do Amazon EC2 é compatível com marcação, consulte Ações, recursos e chaves de condição para Amazon EC2.

Para forçar os usuários a especificarem tags quando criam um recurso, use a chave de condição `aws:RequestTag` ou a chave de condição `aws:TagKeys` com o modificador `ForAnyValue` na ação resource-creating. A ação `ec2:CreateTags` não será avaliada se um usuário não especificar tags para a ação resource-creating.

Para condições, a chave de condição não diferencia maiúsculas de minúsculas, e o valor da condição diferencia maiúsculas de minúsculas. Portanto, para aplicar a diferenciação de maiúsculas de minúsculas de uma tag, use a chave de condição `aws:TagKeys`, onde a chave da tag é especificada como um valor na condição.

Para obter exemplos de políticas do IAM, consulte Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK. Para obter mais informações sobre as condições de vários valores, consulte Como criar uma condição que testa vários valores de chaves no Guia do usuário do IAM.

Controlar o acesso aos recursos do EC2 usando tags de recursos

Ao criar uma política do IAM que conceda permissão aos usuários para usar recursos do EC2, é possível incluir informações de tag no elemento `Condition` da política para controlar o acesso com base em tags. Isso é conhecido como controle de acesso baseado em atributo (ABAC). O ABAC oferece um controle melhor sobre quais recursos um usuário pode modificar, usar ou excluir. Para obter mais informações, consulte O que é ABAC para a AWS?

Por exemplo, é possível criar uma política que permite que os usuários encerrem uma instância, mas nega a ação se a instância tiver a tag `environment=production`. Para fazer isso, use a

chave de condição `aws:ResourceTag` para permitir ou negar acesso ao recurso com base nas tags anexadas ao recurso.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Para saber se uma ação de API do Amazon EC2 oferece suporte ao controle de acesso usando a chave de condição `aws:ResourceTag`, consulte Ações, recursos e chaves de condição para Amazon EC2 . Como as ações de `Describe` não oferecem suporte a permissões em nível de recurso, especifique-as em uma declaração separada sem condições.

Para obter exemplos de políticas do IAM, consulte Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK.

Se você permitir ou negar aos usuários o acesso a recursos com base em tags, considere negar explicitamente aos usuários a capacidade de adicionar essas tags ou removê-las dos mesmos recursos. Caso contrário, é possível que um usuário contorne suas restrições e obtenha acesso a um recurso modificando as tags.

Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK

Você deve conceder aos usuários as permissões necessárias para o Amazon EC2 usando as políticas do IAM. Os exemplos a seguir mostram declarações de políticas possíveis de serem usadas para controlar as permissões que os usuários têm para o Amazon EC2. Essas políticas são projetadas para solicitações feitas com a AWS CLI ou com o AWS SDK. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM. Para obter exemplos de políticas para trabalhar no console do Amazon EC2, consulte Políticas de exemplo para trabalhar no console do Amazon EC2. Para obter exemplos de políticas do IAM específicas da Amazon VPC, consulte Identity and Access Management para a Amazon VPC.

Nos exemplos a seguir, substitua cada *espaço reservado* por suas próprias informações.

Exemplos

- Exemplo: acesso somente leitura
- Exemplo: restringir acesso a uma região específica
- Trabalhar com instâncias
- Executar instâncias (RunInstances)
- Trabalhar com Instâncias spot

- Exemplo: trabalhar com Instâncias reservadas
- Exemplo: marcar recursos
- Exemplo: trabalhar com funções do IAM
- Exemplo: trabalhar com tabelas de rotas
- Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS
- Exemplo: trabalhar com modelos de execução
- Trabalhar com metadados de instância
- Trabalhar com volumes e snapshots do Amazon EBS

Exemplo: acesso somente leitura

A política a seguir concede aos usuários permissões para utilizar todas as ações da API do Amazon EC2 cujos nomes começam com `Describe`. O elemento `Resource` usa um caractere curinga para indicar que os usuários podem especificar todos os recursos com essas ações da API. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso. Para obter mais informações sobre quais ARNs é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Os usuários não têm permissão para executar nenhuma ação nos recursos (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API é negada para os usuários.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Exemplo: restringir acesso a uma região específica

A política a seguir nega permissão aos usuários para uso de todas as ações da API do Amazon EC2 a menos que a região seja a Europa (Frankfurt). Ela usa a chave de condição global `aws:RequestedRegion`, que é compatível com todas as ações da API do Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

Como alternativa, é possível usar a chave de condição `ec2:Region`, que é específica ao Amazon EC2 e é compatível com todas as ações da API do Amazon EC2.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Trabalhar com instâncias

Exemplos

- Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias
- Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas

Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias

A política a seguir concede aos usuários permissões para utilizar as ações da API especificadas no elemento `Action`. O elemento `Resource` usa um caractere curinga * para indicar que os usuários podem especificar todos os recursos com essas ações da API. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso. Para obter mais informações sobre quais ARNs é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Os usuários não têm permissão para usar qualquer outra ação da API (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API são negadas para os usuários.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas

A política a seguir permite que os usuários descrevam todas as instâncias, iniciem e parem somente as instâncias i-1234567890abcdef0 e i-0598c7d356eba48d7 e encerrem somente instâncias na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) com a tag de recurso "`purpose=test`".

A primeira declaração usa um caractere curinga * para o elemento `Resource` para indicar que os usuários podem especificar todos os recursos com a ação. Nesse caso, os usuários podem listar todas as instâncias. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com permissões em nível de recurso (nesse caso, `ec2:DescribeInstances`). Para obter mais informações sobre quais ARNs é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

A segunda declaração usa permissões em nível de recurso para as ações `StopInstances` e `StartInstances`. As instâncias específicas são indicadas por seus ARNs no elemento `Resource`.

A terceira instrução permite que os usuários encerrem todas as instâncias na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) que pertencem à conta da AWS especificada, mas somente quando a instância tiver a etiqueta `"purpose=test"`. O elemento `Condition` qualifica quando a declaração de política está em vigor.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
```

```
        }
    }

    ]
}
```

Executar instâncias (RunInstances)

A ação da API RunInstances inicia uma ou mais Instâncias on-demand ou uma ou mais Instâncias spot. `RunInstances` requer uma AMI e cria uma instância. Os usuários podem especificar um par de chaves e um grupo de segurança na solicitação. A inicialização em uma VPC requer uma sub-rede, e cria uma interface de rede. A inicialização de uma AMI baseada no Amazon EBS cria um volume. Portanto, o usuário deve ter permissões para usar esses recursos do Amazon EC2. É possível criar um declaração de política que exija que os usuários especifiquem um parâmetro opcional em `RunInstances` ou restringir os usuários a valores específicos para um parâmetro.

Para obter mais informações sobre as permissões em nível de recurso que são necessárias para executar uma instância, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Observe que, por padrão, os usuários não têm permissões para descrever, iniciar, interromper ou encerrar as instâncias resultantes. Uma maneira de conceder aos usuários permissão para gerenciar as instâncias resultantes é criar uma tag específica para cada instância e criar uma declaração que permita que eles gerenciem instâncias com aquela tag. Para obter mais informações, consulte Trabalhar com instâncias.

Recursos

- AMIs
- Tipos de instância
- Subredes
- Volumes do EBS
- Tags
- Tags em um modelo de execução
- GPUs elásticas
- Modelos de execução

AMIs

A política a seguir permite que os usuários iniciem instâncias usando apenas as AMIs especificadas, `ami-9e1670f7` e `ami-45cf5c3c`. Os usuários não podem executar uma instância usando outras AMIs (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

Como alternativa, a política a seguir permite que os usuários executem instâncias em todas as AMIs pertencentes à Amazon ou a determinados parceiros confiáveis e verificados. O elemento `Condition` da primeira declaração testa se `ec2:Owner` é `amazon`. Os usuários não podem executar uma instância usando outras AMIs (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
```

```
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Tipos de instância

A política a seguir permite que os usuários executem instâncias usando somente o tipo de instância `t2.micro` ou `t2.small`, o que é possível fazer para controlar os custos. Os usuários não podem executar instâncias maiores porque o elemento `Condition` da primeira declaração testa se `ec2:InstanceType` é `t2.micro` ou `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Se desejar, é possível criar uma política que negue aos usuários permissões para executar qualquer instância, com exceção dos tipos de instância `t2.micro` e `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
```

```
        ]
      }
   ]
}
```

Subredes

A política a seguir permite que os usuários executem instâncias usando apenas a sub-rede especificada, `subnet-`*`12345678`*. O grupo não pode executar instâncias em outra sub-rede (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
   ]
}
```

Se desejar, é possível criar uma política que negue aos usuários permissões para executar uma instância em qualquer outra sub-rede. A declaração faz isso negando permissão para criar uma interface de rede, exceto quando a sub-rede `subnet-`*`12345678`* for especificada. Essa negação substitui qualquer outra política criada para permitir a execução de instâncias em outras sub-redes.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
```

```
            "arn:aws:ec2:region:account-id:network-interface/*"
        ],
        "Condition": {
            "ArnNotEquals": {
                "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:region::image/ami-*",
            "arn:aws:ec2:region:account-id:network-interface/*",
            "arn:aws:ec2:region:account-id:instance/*",
            "arn:aws:ec2:region:account-id:subnet/*",
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:key-pair/*",
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}
```

Volumes do EBS

A política a seguir permite que os usuários executem instâncias somente se os volumes do EBS para a instância estiverem criptografados. O usuário deve executar uma instância em uma AMI criada com snapshots criptografados, para garantir que o volume raiz esteja criptografado. Qualquer volume adicional que o usuário anexe à instância durante a execução também deve estar criptografado.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tags

Marque instâncias na criação

A política a seguir permite que os usuários executem instâncias e as marquem durante a criação. Para ações de criação de recursos que aplicam tags, os usuários devem ter permissões para usar a ação `CreateTags`. A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `RunInstances` e somente para instâncias. Os usuários não podem marcar recursos existentes e não podem marcar volumes usando a solicitação `RunInstances`.

Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Marque instâncias e volumes na criação com tags específicas

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todas as instâncias e os volumes criados por `RunInstances` com as tags `environment=production` e `purpose=webserver`. Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
```

```
            "arn:aws:ec2:region:account-id:instance/*"
        ],
        "Condition": {
           "StringEquals": {
               "aws:RequestTag/environment": "production" ,
               "aws:RequestTag/purpose": "webserver"
            }
         }
      },
      {
        "Effect": "Allow",
        "Action": [
           "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:region:account-id:*/*",
        "Condition": {
           "StringEquals": {
               "ec2:CreateAction" : "RunInstances"
            }
         }
      }
   ]
}
```

Marque instâncias e volumes na criação com pelo menos uma tag específica

A política a seguir usa o modificador `ForAnyValue` na condição `aws:TagKeys` para indicar que pelo menos uma tag deve ser especificada na solicitação e deve conter a chave `environment` ou `webserver`. A tag deve ser aplicada a instâncias e a volumes. Qualquer valor de tag pode ser especificado na solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
```

```
          "arn:aws:ec2:region:account-id:security-group/*",
          "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
          "ForAnyValue:StringEquals": {
              "aws:TagKeys": ["environment","webserver"]
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Se forem marcadas na criação, as instâncias deverão ser marcadas com uma tag específica

Na política a seguir, os usuários não precisam especificar tags na solicitação, mas se o fizerem, a tag deverá ser `purpose=test`. Nenhuma outra tag é permitida. Os usuários podem aplicar as tags a qualquer recurso marcável na solicitação `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Para não permitir que ninguém adicione tags na criação para RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
```

```
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Permitir apenas tags específicas para spot-instances-request. A inconsistência surpresa número 2 entra em jogo aqui. Em circunstâncias normais, não especificar tag alguma resultará em Não autenticado. No caso de spot-instances-request, esta política não será avaliada se não houver tags spot-instances-request, portanto, uma solicitação Spot on Run sem tag será bem-sucedida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
```

```
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Tags em um modelo de execução

No exemplo a seguir, os usuários poderão executar instâncias, mas apenas se usarem um modelo de execução específico (`lt-09477bcd97b0d310e`). A chave de condição `ec2:IsLaunchTemplateResource` impede que os usuários substituam alguns recursos especificados no modelo de execução. A segunda parte da instrução permite que os usuários marquem instâncias durante a criação; essa parte da instrução será necessária se as tags forem especificadas para a instância no modelo de execução.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
```

```
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
           }
        }
     }
  ]
}
```

GPUs elásticas

Na política a seguir, os usuários podem executar uma instância e especificar uma GPU elástica para anexar à instância. Os usuários podem executar instâncias em qualquer região, mas só podem anexar uma GPU elástica durante uma execução na região `us-east-2`.

A chave de condição `ec2:ElasticGpuType` garante que as instâncias usem o tipo de GPU elástico `eg1.medium` ou `eg1.large`.

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
```

```
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

Modelos de execução

No exemplo a seguir, os usuários poderão executar instâncias, mas apenas se usarem um modelo de execução específico (`lt-09477bcd97b0d310e`). Os usuários podem substituir quaisquer parâmetros no modelo de execução especificando os parâmetros na ação `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

Neste exemplo, os usuários poderão executar instâncias apenas se usarem um modelo de execução. A política usa a chave de condição `ec2:IsLaunchTemplateResource` para impedir que os usuários substituam os ARNs pré-existentes no modelo de execução.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

No exemplo a seguir, a política permitirá que o usuário execute instâncias, mas apenas se usarem um modelo de execução. Os usuários não podem substituir os parâmetros de interface de rede e sub-rede na solicitação; esses parâmetros só podem ser especificados no modelo de execução. A primeira parte da instrução usa o elemento NotResource para permitir todos os outros recursos, exceto interfaces de rede e sub-redes. A segunda parte da instrução permite recursos de interface de rede e sub-rede, mas somente se eles forem originários do modelo de execução.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
```

```
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

O exemplo a seguir permitirá que os usuários executem instâncias somente se usarem um modelo de execução, e somente se o modelo de execução tiver a tag `Purpose=Webservers`. Os usuários não podem substituir nenhum dos parâmetros do modelo de execução na ação `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
```

```
}
```

Trabalhar com Instâncias spot

É possível usar a ação RunInstances para criar solicitações de instância spot e marcar solicitações de instância spot na criação. O recurso a ser especificado para RunInstances é `spot-instances-request`.

O recurso `spot-instances-request` é avaliado na política do IAM da seguinte forma:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use RunInstances para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada terá êxito.
- Caso use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, será necessário incluir o recurso `spot-instances-request` na instrução de permissão RunInstances, caso contrário, a chamada falhará.
- Caso você use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou um curinga `*` na instrução de permissão CreateTags, caso contrário, a chamada falhará.

É possível solicitar Instâncias spot usando RunInstances ou RequestSpotInstances. Os exemplos de políticas do IAM a seguir se aplicam somente ao solicitar Instâncias spot usando RunInstances.

Exemplo: solicitar Instâncias spot usando RunInstances

A política a seguir permite que os usuários solicitem Instâncias spot usando a ação RunInstances. O recurso `spot-instances-request`, que é criado por RunInstances, solicita Instâncias spot.

> **Note**
>
> Para usar RunInstances a fim de criar solicitações de instância spot, é possível omitir `spot-instances-request` da lista `Resource` caso pretenda marcar as solicitações de instância spot na criação. Isso ocorre porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

> **Warning**
>
> NÃO COMPATÍVEL – Exemplo: negar permissão aos usuários para solicitar Instâncias spot usando RunInstances
>
> A política a seguir não é compatível com o recurso `spot-instances-request`.
>
> A política a seguir destina-se a conceder permissão aos usuários para iniciar Instâncias on-demand, mas negar a permissão de solicitação Instâncias spot. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot.

A segunda instrução destina-se a negar a ação RunInstances para o recurso `spot-instances-request`. No entanto, esta condição não é compatível porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Exemplo: marcar solicitações de instância spot na criação

A política a seguir permite que os usuários marquem todos os recursos criados durante o lançamento da instância. A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga * para permitir que todos os recursos sejam marcados quando criados no momento da execução da instância.

> **Note**
>
> Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances. Portanto, permita explicitamente o recurso `spot-instances-request` para a ação RunInstances, caso contrário, a chamada falhará.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemplo: negar marcações na criação para solicitações de instância spot

A política a seguir nega aos usuários a permissão para marcar os recursos criados durante a execução da instância.

A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga * para evitar que todos os recursos sejam marcados, quando criados, no momento da execução da instância. Se `spot-instances-request` ou qualquer outro recurso estiver marcado na criação, a chamada RunInstances falhará.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

NÃO COMPATÍVEL – Exemplo: permitir a criação de uma solicitação de instância spot apenas se lhe for atribuída uma etiqueta específica

A política a seguir não é compatível com o recurso `spot-instances-request`.

A política a seguir destina-se a conceder permissão à RunInstances para criar uma solicitação de instância spot somente se a solicitação for marcada com uma tag específica. A primeira instrução permite que RunInstances crie os recursos listados.
A segunda instrução destina-se a conceder permissão aos usuários para criar uma solicitação de instância spot somente se a solicitação tiver a etiqueta `environment=production`. Se essa condição for aplicada a outros recursos criados por RunInstances, não especificar nenhuma tag gerará um erro `Unauthenticated`. No entanto, se nenhuma etiqueta for especificada para a solicitação de instância spot, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances, o que resultará em solicitações de instância spot não marcadas sendo criadas pela RunInstances. Observe que especificar outra etiqueta, além de `environment=production` gera um erro `Unauthenticated`, pois se um usuário marca uma solicitação de instância spot, o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Exemplo: negar a criação de uma solicitação de instância spot se lhe for atribuída uma etiqueta específica

A política a seguir nega à RunInstances a permissão para criar uma solicitação de instância spot se a solicitação estiver marcada com `environment=production`.

A primeira instrução permite que RunInstances crie os recursos listados.

A segunda instrução nega permissão aos usuários para criar uma solicitação de instância spot se a solicitação tiver a etiqueta `environment=production`. Especificar `environment=production` como tag gerará um erro `Unauthenticated`. Especificar outras tags ou não especificar tags resultará na criação de uma solicitação de instância spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
```

```
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemplo: trabalhar com Instâncias reservadas

A política a seguir concede aos usuários permissão para visualizar, modificar e comprar Instâncias reservadas na sua conta.

Não é possível definir permissões em nível de recurso para instâncias reservadas. Essa política significa que os usuários têm acesso a todas as Instâncias reservadas na conta.

O elemento `Resource` usa um caractere curinga * para indicar que os usuários podem especificar todos os recursos com a ação. Nesse caso, os usuários podem listar e modificar todas as Instâncias reservadas na conta. Eles também podem comprar Instâncias reservadas usando as credenciais da conta. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso.

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Para permitir que os usuários exibam e modifiquem as Instâncias reservadas na conta, mas não comprem novas Instâncias reservadas.

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemplo: marcar recursos

A política a seguir permite que os usuários usem a ação `CreateTags` para aplicar tags a uma instância somente se a tag contiver a chave `environment` e o valor `production`. Nenhuma outra etiqueta é permitida, e o usuário não pode marcar outros tipos de recurso.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

A política a seguir permite que os usuários marquem qualquer recurso marcável que já tenha uma tag com a chave `owner` e um valor do nome de usuário. Além disso, os usuários devem especificar uma tag com uma chave de `anycompany:environment-type` e um valor de `test` ou de `prod` na solicitação. Os usuários podem especificar tags adicionais na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

É possível criar uma política do IAM que permite que os usuários excluam tags específicas de um recurso. Por exemplo, a política a seguir permite que os usuários excluam tags de um volume se

as chaves das tags especificadas na solicitação forem `environment` ou `cost-center`. Qualquer valor pode ser especificado para a tag, mas a chave da tag deve corresponder a uma das chaves especificadas.

> **Note**
>
> Se você excluir um recurso, todas as tags associadas ao recurso também serão excluídas. Os usuários não precisam de permissões para utilizar a ação `ec2:DeleteTags` para excluir um recurso que tenha tags. Eles precisam apenas das permissões para executar a ação de exclusão.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Essa política permite que os usuários excluam somente a tag `environment=prod` em qualquer recurso e apenas se o recurso já estiver marcado com a chave do `owner` e com um valor do nome de usuário. Os usuários não podem excluir nenhuma outra tag de um recurso.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
```

```
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Exemplo: trabalhar com funções do IAM

A política a seguir permite que os usuários anexem, substituam e desanexem uma função do IAM para instâncias que tenham a tag `department=test`. As substituição ou a desanexação de uma função do IAM requer um ID de associação, portanto, a política também concede aos usuários permissão para usar a ação `ec2:DescribeIamInstanceProfileAssociations`.

Os usuários devem ter permissão para usar a ação `iam:PassRole` para passar o perfil para a instância.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
```

```
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
}
```

A política a seguir permite que os usuários anexem ou substituam uma função do IAM para qualquer instância. Os usuários podem anexar ou substituir apenas funções do IAM com nomes que começam com `TestRole-`. Para a ação `iam:PassRole`, especifique o nome da função do IAM e não o perfil da instância (se os nomes forem diferentes). Para obter mais informações, consulte Perfis de instância.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

Exemplo: trabalhar com tabelas de rotas

A política a seguir permite aos usuários adicionar, remover e substituir rotas em tabelas de rotas associadas à VPC `vpc-ec43eb89` somente. Para especificar uma VPC para a chave de condição `ec2:Vpc`, especifique o ARN total da VPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS

O exemplo a seguir é de uma política que é possível anexar a uma função do IAM. A política permite que uma instância exiba recursos em vários serviços da AWS. Ela usa a chave de condição global `ec2:SourceInstanceARN` para especificar que a instância na qual a solicitação é feita deve ser a instância `i-093452212644b0dd6`. Se a mesma função do IAM estiver associada a outra instância, a outra instância não poderá executar nenhuma dessas ações.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

Exemplo: trabalhar com modelos de execução

A política a seguir permite que os usuários criem uma versão de modelo de execução e alterem um modelo de execução, mas somente um modelo de execução específico (`lt-09477bcd97b0d3abc`). Os usuários não podem trabalhar com outros modelos de execução.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

A política a seguir permite que os usuários excluam qualquer modelo de execução e versão de modelo de execução, desde que o modelo tenha a tag `Purpose=Testing`.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Trabalhar com metadados de instância

As políticas a seguir garantem que os usuários possam recuperar somente metadados de instância usando o Serviço de metadados da instância versão 2 (IMDSv2). É possível combinar as quatro políticas a seguir em uma única política com quatro instruções. Quando combinadas como uma única política, é possível usar a política como uma política de controle de serviço (SCP). Ela pode funcionar tão bem como uma política de negação aplicada a uma política existente do IAM (retirando e limitando a permissão existente) ou como uma SCP aplicada globalmente em uma conta, uma unidade organizacional (UO) ou uma organização inteira.

> **Note**
>
> As seguintes políticas de opções de metadados de RunInstances devem ser usadas em conjunto com uma política que concede ao principal permissões para executar uma instância com RunInstances. Se o principal também não tiver permissões para RunInstances, não poderá executar uma instância. Para obter mais informações, consulte as políticas em Trabalhar com instâncias e Executar instâncias (RunInstances).

Important

Se você usar grupos do Auto Scaling e precisar exigir o uso do IMDSv2 em todas as novas instâncias, seus grupos do Auto Scaling deverão usar modelos de execução.
Quando um grupo do Auto Scaling usa um modelo de execução, as permissões de `ec2:RunInstances` do principal do IAM são verificadas quando um novo grupo do Auto Scaling é criado. Elas também são verificadas quando um grupo existente do Auto Scaling é atualizado para usar um novo modelo de execução ou uma nova versão de um modelo de execução.
As restrições sobre o uso do IMDSv1 em principais do IAM para `RunInstances` são verificadas somente quando um grupo do Auto Scaling que está usando um modelo de inicialização é criado ou atualizado. Para um grupo do Auto Scaling configurado para usar o modelo de execução `Latest` ou `Default`, as permissões não são verificadas quando uma nova versão do modelo de execução é criada. Para que as permissões sejam verificadas, configure o grupo do Auto Scaling para usar uma versão específica do modelo de execução.

Para impor o uso do IMDSv2 em instâncias executadas por grupos do Auto Scaling, as seguintes etapas adicionais são necessárias:

1. Desabilite o uso de configurações de execução para todas as contas em sua organização usando SCPs (service control policies - políticas de controle de serviço) ou limites de permissões do IAM para novos principais criados. Para principais existentes do IAM com permissões de grupo do Auto Scaling, atualize suas políticas associadas com essa chave de condição. Para desabilitar o uso de configurações de execução, crie ou modifique a SCP relevante, o limite de permissões ou a política do IAM com a `"autoscaling:LaunchConfigurationName"` chave de condição com o valor especificado como `null`.
2. Para novos modelos de execução, configure as opções de metadados da instância no modelo de execução. Para modelos de execução existentes, crie uma versão do modelo de execução e configure as opções de metadados da instância na nova versão.
3. Na política que concede a qualquer principal permissão para usar um modelo de execução, restrinja a associação de `$latest` e `$default` especificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Ao restringir o uso a uma versão específica de um modelo de execução, é possível garantir que novas instâncias serão executadas usando a versão na qual as opções de metadados da instância estão configuradas. Para obter mais informações, consulte

LaunchTemplateSpecification no Referência da API do Amazon EC2 Auto Scaling, especificamente o parâmetro `Version`.

4. Para um grupo do Auto Scaling que usa uma configuração de execução, substitua a configuração de execução por um modelo de execução. Para obter mais informações, consulte Substituir uma configuração de execução por um modelo de execução no Guia do usuário do Amazon EC2 Auto Scaling.
5. Para um grupo do Auto Scaling que usa um modelo de execução, certifique-se de que ele usa um novo modelo de execução com as opções de metadados da instância configuradas ou usa uma nova versão do modelo de execução atual com as opções de metadados da instância configuradas. Para obter mais informações, consulte update-auto-scaling-group na Referência de comandos da AWS CLI.

Exemplos

- Exigir o uso de IMDSv2
- Negar a rejeição do IMDSv2
- Especificar o limite máximo de saltos
- Limitar quem pode modificar as opções de metadados da instância
- Exigir que as credenciais de função sejam recuperadas de IMDSv2

Exigir o uso de IMDSv2

A política a seguir especifica que não é possível chamar a API RunInstances a menos que a instância também esteja optada para exigir o uso de IMDSv2 (indicado por `"ec2:MetadataHttpTokens": "required"`). Se você não especificar que a instância requer IMDSv2, receberá um erro `UnauthorizedOperation` ao chamar a API RunInstances.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
```

```
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Negar a rejeição do IMDSv2

A política a seguir especifica que não é possível chamar a API `ModifyInstanceMetadataOptions` e permitir a opção de IMDSv1 ou IMDSv2. Se você chamar a API `ModifyInstanceMetadataOptions`, o atributo `HttpTokens` deverá ser definido como `required`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Especificar o limite máximo de saltos

A política a seguir especifica que não é possível chamar a API RunInstances a menos que também especifique um limite de saltos, que não pode ser superior a 3. Se isso não for feito, você receberá um erro `UnauthorizedOperation` ao chamar a API RunInstances.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
               {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Limitar quem pode modificar as opções de metadados da instância

A política a seguir permite que apenas usuários com o perfil `ec2-imds-admins` façam alterações. nas opções de metadados da instância. Se qualquer principal diferente da função `ec2-imds-admins` tentar chamar a API ModifyInstanceMetadataOptions, receberá um erro `Unauthorized0peration`. Essa instrução pode ser usada para controlar o uso da API ModifyInstanceMetadataOptions. No momento, não há controles de acesso refinados (condições) para a API ModifyInstanceMetadataOptions.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

Exigir que as credenciais de função sejam recuperadas de IMDSv2

A política a seguir especifica que, se essa política for aplicada a uma função e a função for assumida pelo serviço do EC2 e as credenciais resultantes forem usadas para assinar uma solicitação, a solicitação deverá ser assinada pelas credenciais de função do EC2 recuperadas do IMDSv2. Caso contrário, todas as suas chamadas de API receberão um erro `Unauthorized0peration`. Essa instrução/política pode ser aplicada de modo geral porque, se a solicitação não for assinada por credenciais de função do EC2, ela não terá efeito.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Trabalhar com volumes e snapshots do Amazon EBS

Para obter exemplos de políticas para trabalhar com volumes e snapshots do Amazon EBS, consulte Exemplos de políticas baseadas em identidade para o Amazon EBS.

Políticas de exemplo para trabalhar no console do Amazon EC2

Você deve conceder aos usuários as permissões necessárias para o Amazon EC2 usando as políticas do IAM. É possível usar as políticas do IAM para conceder permissões aos usuários para visualizarem e trabalharem com recursos específicos no console do Amazon EC2. É possível usar os exemplos de políticas da seção anterior. No entanto, eles foram criados para solicitações feitas com a AWS CLI ou com um AWS SDK. Para obter mais informações, consulte Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK e Criação de políticas do IAM no Guia do usuário do IAM.

O console usa ações de API adicionais para seus recursos, portanto, essas políticas talvez não funcionem como esperado. Por exemplo, um usuário que tem permissão para usar somente a ação da API `DescribeVolumes` encontrará erros ao tentar visualizar volumes no console. Esta seção demonstra políticas que permitem que os usuários trabalhem com partes específicas do console. Para obter informações adicionais sobre como criar políticas para o console do Amazon EC2, consulte a seguinte postagem do Blog de segurança da AWS: Granting Users Permission to Work in the Amazon EC2 Console (Conceder permissão aos usuários para trabalhar no console do Amazon EC2).

> **Tip**
>
> Para ajudar a descobrir quais ações de API são necessárias para realizar tarefas no console, é possível usar um serviço como o AWS CloudTrail. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail. Se sua política não conceder permissão para criar ou modificar um recurso específico, o console exibirá uma mensagem codificada com informações de diagnóstico. É possível decodificar a mensagem usando a ação de API DecodeAuthorizationMessage para AWS STS, ou o comando decode-authorization-message na AWS CLI.

Exemplos

- Exemplo: acesso somente leitura
- Exemplo: uso do assistente de início de instância do EC2
- Exemplo: trabalhar com grupos de segurança
- Exemplo: trabalhar com endereços IP elásticos
- Exemplo: trabalhar com Instâncias reservadas

Exemplo: acesso somente leitura

Para permitir que os usuários visualizem todos os recursos no console do Amazon EC2, é possível usar a mesma política como no exemplo a seguir: Exemplo: acesso somente leitura. Os usuários não podem executar nenhuma ação nesses recursos ou criar novos recursos, a menos que outra declaração conceda permissão a eles para fazer isso.

Visualizar instâncias, AMIs e snapshots

Como alternativa, é possível fornecer acesso somente leitura a um subconjunto de recursos. Para fazer isso, substitua o caractere curinga * na ação de API `ec2:Describe` por ações `ec2:Describe` específicas para cada recurso. A política a seguir permite que os usuários visualizem todas as instâncias, AMIs e snapshots no console do Amazon EC2. A ação `ec2:DescribeTags` permite que os usuários visualizem AMIs públicas. O console requer que as informações de marcação exibam AMIs públicas. No entanto, é possível remover essa ação para permitir que os usuários visualizem somente AMIs privadas.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> As ações da API `ec2:Describe*` do Amazon EC2 não oferecem suporte a permissões em nível de recurso, portanto, não é possível controlar quais recursos individuais os usuários podem visualizar no console. Portanto, o caractere curinga * é necessário no elemento `Resource` da declaração acima. Para obter mais informações sobre quais ARNs é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Visualizar instâncias e métricas do CloudWatch

A política a seguir permite que os usuários visualizem instâncias no console do Amazon EC2, bem como alarmes e métricas do CloudWatch na guia Monitoring (Monitoramento) da página Instances (Instâncias). O console do Amazon EC2 usa a API do CloudWatch para exibir os alarmes e as métricas, portanto, você deve conceder aos usuários permissão para usar as

ações `cloudwatch:DescribeAlarms`, `cloudwatch:DescribeAlarmsForMetric`, `cloudwatch:ListMetrics`, `cloudwatch:GetMetricStatistics` e `cloudwatch:GetMetricData`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Exemplo: uso do assistente de início de instância do EC2

O assistente de início de instância do Amazon EC2 é uma tela com opções para configurar e iniciar uma instância. Sua política deve incluir permissão para usar as ações de API que permitem que os usuários trabalhem com as opções do assistente. Se a política não incluir a permissão para usar essas ações, alguns itens do assistente poderão não ser carregados corretamente, e os usuários não poderão concluir uma execução.

Acesso básico ao assistente de início de instância

Para concluir uma execução com êxito, os usuários devem receber permissão para usar a ação de API `ec2:RunInstances` e, pelo menos, as seguintes ações de API:

- `ec2:DescribeImages`: para visualizar e selecionar uma AMI.
- `ec2:DescribeInstanceTypes`: para visualizar e selecionar um tipo de instância.
- `ec2:DescribeVpcs`: para ver as opções de rede disponíveis.
- `ec2:DescribeSubnets`: para visualizar todas as sub-redes disponíveis da VPC escolhida.

- `ec2:DescribeSecurityGroups` ou `ec2:CreateSecurityGroup`: para visualizar e selecionar um grupo de segurança existente ou criar um.
- `ec2:DescribeKeyPairs` ou `ec2:CreateKeyPair`: para selecionar um par de chaves ou criar um par.
- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

É possível adicionar ações de API à sua política para fornecer mais opções aos usuários, por exemplo:

- `ec2:DescribeAvailabilityZones`: para ver e selecionar uma zona de disponibilidade específica.
- `ec2:DescribeNetworkInterfaces`: para visualizar e selecionar interfaces de rede existentes para a sub-rede selecionada.

- Para adicionar regras de saída para grupos de segurança da VPC, os usuários devem receber a permissão para usar a ação de API `ec2:AuthorizeSecurityGroupEgress`. Para modificar ou excluir regras existentes, os usuários devem receber permissão para usar a ação de API relevante `ec2:RevokeSecurityGroup*`.
- `ec2:CreateTags`: para marcar os recursos criados por `RunInstances`. Para ter mais informações, consulte Conceder permissão para marcar recursos durante a criação. Se os usuários não tiverem permissão para usar essa ação e tentarem aplicar tags na página de marcação do assistente de início de instância, haverá falha na execução.

  > **Important**
  >
  > Especifique um Name (Nome) ao iniciar uma instância cria uma etiqueta e exige a ação `ec2:CreateTags`. Tenha cuidado ao conceder aos usuários permissão para usar a ação `ec2:CreateTags`, pois isso limita sua capacidade de usar a chave de condição `aws:ResourceTag` para restringir o uso de outros recursos. Se você conceder aos usuários permissão para usar a ação `ec2:CreateTags`, eles poderão alterar a tag de um recurso para contornar essas restrições. Para ter mais informações, consulte Controlar o acesso aos recursos do EC2 usando tags de recursos.

- Para usar parâmetros do Systems Manager ao selecionar uma AMI, você deve adicionar `ssm:DescribeParameters` e `ssm:GetParameters` à sua política. O `ssm:DescribeParameters` concede aos usuários a permissão para visualizar e selecionar parâmetros do Systems Manager. O `ssm:GetParameters` concede aos usuários a permissão para obter os valores dos parâmetros do Systems Manager. Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações, consulte Restringir acesso a parâmetros específicos do Systems Manager posteriormente nesta seção.

Atualmente, as ações da API `Describe*` do Amazon EC2 não oferecem suporte a permissões em nível de recurso, portanto, não é possível restringir quais recursos individuais os usuários podem visualizar no assistente de início de instância. Contudo, é possível aplicar permissões em nível de recurso na ação de API `ec2:RunInstances` para restringir os recursos que os usuários podem usar para executar uma instância. Haverá falha na execução se os usuários selecionarem opções que não estão autorizados a usar.

Restringir o acesso a um tipo de instância, uma sub-rede e uma região específicos

A política a seguir permite que os usuários executem instâncias `t2.micro` usando AMIs de propriedade da Amazon e apenas em uma sub-rede específica (`subnet-1a2b3c4d`). Os usuários só podem iniciar na região `sa-east-1`. Se os usuários selecionarem uma região diferente ou se selecionarem outro tipo de instância, outra AMI ou outra sub-rede no assistente de início de instância, a execução falhará.

A primeira declaração concede aos usuários permissão para visualizar as opções no assistente de início de instância ou criar novas, conforme explicado no exemplo acima. A segunda declaração concede aos usuários permissão para usarem a interface de rede, o volume, o par de chaves, o grupo de segurança e os recursos de sub-rede para a ação `ec2:RunInstances`, que são necessários para executar uma instância em uma VPC. Para obter mais informações sobre como usar a ação `ec2:RunInstances`, consulte Executar instâncias (RunInstances). A terceira e a quarta declaração concedem aos usuários permissão para usarem a instância e os recursos das AMIs respectivamente, mas somente se a instância for uma instância `t2.micro` e somente se a AMI pertencer à Amazon ou a determinados parceiros confiáveis e verificados.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
   "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action":"ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:sa-east-1:111122223333:volume/*",
         "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
```

```
            "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
            "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
        ]
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2:sa-east-1:111122223333:instance/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
              "arn:aws:ec2:sa-east-1::image/ami-*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:Owner": "amazon"
            }
        }
    }
    ]
}
```

Restringir o acesso a parâmetros específicos do Systems Manager

A política a seguir concede acesso para usar parâmetros do Systems Manager com um nome específico.

A primeira instrução concede aos usuários permissão para visualizar parâmetros do Systems Manager ao selecionar uma AMI no assistente de início de instância. A segunda instrução concede aos usuários a permissão para usar somente parâmetros denominados `prod-*`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
```

```
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
   }
   ]
}
```

Exemplo: trabalhar com grupos de segurança

Visualizar grupos de segurança e adicionar e remover regras

A política a seguir concede aos usuários permissão para visualizar grupos de segurança no console do Amazon EC2, adicionar e remover regras de entrada e de saída, bem como listar e modificar descrições de regras de grupo de segurança existentes que têm a etiqueta `Department=Test`.

Na primeira declaração, a ação `ec2:DescribeTags` permite que os usuários visualizem tags no console, o que facilita a identificação dos grupos de segurança que eles têm permissão para modificar.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
```

```
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:ModifySecurityGroupRules",
            "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
            "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Department": "Test"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySecurityGroupRules"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group-rule/*"
        ]
    }
]}
```

Trabalhar com a caixa de diálogo Create Security Group (Criar grupo de segurança)

É possível criar uma política que permita que os usuários trabalhem com a caixa de diálogo Create Security Group (Criar grupo de segurança) no console do Amazon EC2. Para usar essa caixa de diálogo, os usuários devem receber a permissão para usar pelo menos as seguintes ações de API:

- `ec2:CreateSecurityGroup`: para criar um novo grupo de segurança.
- `ec2:DescribeVpcs`: para visualizar uma lista de VPCs existentes na lista VPC.

Com essas permissões, os usuários podem criar um novo grupo de segurança com êxito, mas não podem adicionar nenhuma regra a ele. Para trabalhar com regras na caixa de diálogo Create Security Group (Criar grupo de segurança), é possível adicionar as seguintes ações de API à sua política:

- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.
- `ec2:AuthorizeSecurityGroupEgress`: para adicionar regras de saída aos grupos de segurança da VPC.
- `ec2:RevokeSecurityGroupIngress`: para modificar ou excluir regras de entrada existentes. Isso é útil para permitir que os usuários usem o recurso Copy to new no console. Esse recurso abre a caixa de diálogo Create Security Group (Criar grupo de segurança) e preenche-a com as mesmas regras do security group que foi selecionado.
- `ec2:RevokeSecurityGroupEgress`: para modificar ou excluir regras de saída de grupos de segurança da VPC. Isso é útil para permitir que os usuários modifiquem ou excluam a regra de saída padrão que permite todo o tráfego de saída.
- `ec2:DeleteSecurityGroup`: para prover quando regras inválidas não podem ser salvas. O console primeiro cria o grupo de segurança e, em seguida, adiciona as regras especificadas. Se as regras forem inválidas, a ação falhará, e o console tentará excluir o grupo de segurança. O usuário permanece na caixa de diálogo Create Security Group (Criar grupo de segurança) para que possa corrigir a regra inválida e tentar criar o security group novamente. Essa ação de API não é necessária, mas se um usuário não receber permissão para usá-la e tentar criar um grupo de segurança com regras inválidas, o grupo de segurança será criado sem nenhuma regra, e o usuário deverá adicioná-las posteriormente.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: para adicionar ou atualizar descrições de regras de grupo de segurança de entrada (inbound).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: para adicionar ou atualizar descrições de regras de grupo de segurança de saída (outbound).
- `ec2:ModifySecurityGroupRules`: para modificar as regras do grupo de segurança.
- `ec2:DescribeSecurityGroupRules`: para listar as regras do grupo de segurança.

A política a seguir concede aos usuários permissão para usar a caixa de diálogo Create Security Group (Criar grupo de segurança) e criar regras de entrada e de saída para grupos de segurança associados a uma VPC específica (`vpc-1a2b3c4d`). Os usuários podem criar grupos de segurança para uma VPC, mas não podem adicionar nenhuma regra a eles. Da mesma forma, os usuários não podem adicionar nenhuma regra aos grupos de segurança existentes não associados à VPC `vpc-1a2b3c4d`. Os usuários também recebem permissão para visualizar todos os grupos de segurança no console. Isso facilita aos usuários identificar os grupos de segurança aos quais podem adicionar regras de entrada. Essa política também concede permissão aos usuários para excluir grupos de segurança associados à VPC `vpc-1a2b3c4d`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Exemplo: trabalhar com endereços IP elásticos

Para permitir que os usuários visualizem endereços IP elásticos no console do Amazon EC2, conceda aos usuários permissão para usar a ação `ec2:DescribeAddresses`.

Para permitir que os usuários trabalhem com endereços IP elásticos, é possível adicionar as seguintes ações à política.

- `ec2:AllocateAddress`: para alocar um endereço IP elástico.
- `ec2:ReleaseAddress`: para liberar um endereço IP elástico.
- `ec2:AssociateAddress`: para associar um endereço IP elástico a uma instância ou a uma interface de rede.

- `ec2:DescribeNetworkInterfaces` e `ec2:DescribeInstances`: para trabalhar com a tela Associate address. A tela exibe as instâncias disponíveis ou as interfaces de rede para que você possa associar um endereço IP elástico.
- `ec2:DisassociateAddress`: para desassociar um endereço IP elástico de uma instância ou de uma interface de rede.

As políticas a seguir permitem que os usuários visualizem, aloquem e associem endereços IP elásticos a instâncias. Os usuários não podem associar endereços IP elásticos a interfaces de rede, desassociar endereços IP elásticos ou liberá-los.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: trabalhar com Instâncias reservadas

A política a seguir permite que os usuários visualizem e modifiquem instâncias reservadas em sua conta e que adquiram novas instâncias reservadas no AWS Management Console.

Esta política permite que os usuários visualizem todas as Instâncias reservadas, bem como Instâncias on-demand, na conta. Não é possível definir permissões em nível de recurso para Instâncias reservadas individuais.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
```

```
            "ec2:ModifyReservedInstances",
            "ec2:PurchaseReservedInstancesOffering",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeReservedInstancesOfferings"
        ],
        "Resource": "*"
    }
    ]
}
```

A ação `ec2:DescribeAvailabilityZones` é necessária para garantir que o console do Amazon EC2 possa exibir informações sobre as zonas de disponibilidade nas quais é possível comprar Instâncias reservadas. A ação `ec2:DescribeInstances` não é necessária, mas garante que o usuário possa visualizar as instâncias na conta e comprar reservas para atender às especificações corretas.

É possível ajustar as ações de API para limitar o acesso do usuário, por exemplo, a remoção de `ec2:DescribeInstances` e de `ec2:DescribeAvailabilityZones` significa que o usuário tem acesso somente leitura.

Políticas gerenciadas pela AWS para o Amazon EC2

Para adicionar permissões a usuários, grupos e perfis, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, é possível usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela denominada ReadOnlyAccess AWS fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

Política gerenciada da AWS: AmazonEC2FullAccess

É possível anexar a política `AmazonEC2FullAccess` a suas identidades do IAM. Essa política concede permissões que possibilitam acesso total ao Amazon EC2.

Para visualizar as permissões para esta política, consulte AmazonEC2FullAccess na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AmazonEC2ReadOnlyAccess

É possível anexar a política `AmazonEC2ReadOnlyAccess` a suas identidades do IAM. Esta política concede permissões que oferecem acesso somente leitura ao Amazon EC2.

Para visualizar as permissões para esta política, consulte AmazonEC2ReadOnlyAccess na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AWSEC2CapacityReservationFleetRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2CapacityReservationFleet para permitir que as reservas de capacidade criem, modifiquem e cancelem reservas de capacidade em seu nome. Para obter mais informações, consulte Função vinculada ao serviço para a frota de reserva de capacidade.

Para visualizar as permissões para esta política, consulte AWSEC2CapacityReservationFleetRolePolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AWSEC2FleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2Fleet para permitir que o EC2 Fleet solicite, inicie, encerre e aplique tags nas instâncias para você. Para ter mais informações, consulte Função vinculada ao serviço para Frota do EC2.

Para visualizar as permissões para esta política, consulte AWSEC2FleetServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AWSEC2SpotFleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2SpotFleet para permitir que a frota spot inicie e gerencie instâncias para você. Para ter mais informações, consulte Função vinculada ao serviço para frota spot.

Para visualizar as permissões para esta política, consulte AWSEC2SpotFleetServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AWSEC2SpotServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2Spot para permitir que o Amazon EC2 inicie e gerencie instâncias spot para você. Para ter mais informações, consulte Função vinculada ao serviço para solicitações de instâncias spot.

Para visualizar as permissões para esta política, consulte AWSEC2SpotServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AWSEC2VssSnapshotPolicy

É possível anexar essa política gerenciada à função do perfil de instância do IAM usada para as instâncias do Windows do Amazon EC2. A política concede permissões que possibilitam que o Amazon EC2 crie e gerencie snapshots do VSS em seu nome.

Para visualizar as permissões para esta política, consulte AWSEC2VssSnapshotPolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: EC2FastLaunchFullAccess

Você pode anexar a política de `EC2FastLaunchFullAccess` ao perfil de instância ou a outro perfil do IAM. Essa política concede total acesso às ações e às permissões direcionadas do EC2 Fast Launch como se segue.

Detalhes da permissão

- EC2 Fast Launch: acesso administrativo é concedido para que o perfil possa habilitar ou desabilitar o EC2 Fast Launch e descrever as imagens do EC2 Fast Launch.
- Amazon EC2: acesso é concedido para as ações RunInstances, CreateTags e Describe do Amazon EC2 que são necessárias para verificar permissões de recursos.
- IAM: acesso é concedido para obter e usar perfis de instância cujo nome contenha `ec2fastlaunch` para criar o perfil vinculada ao serviço EC2FastLaunchServiceRolePolicy.

Para visualizar as permissões para esta política, consulte EC2FastLaunchFullAccess na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: EC2FastLaunchServiceRolePolicy

Esta política é anexada ao perfil vinculado ao serviço denominado AWSServiceRoleForEC2FastLaunch para permitir que o Amazon EC2 crie e gerencie um conjunto de snapshots pré-provisionados que reduzem o tempo necessário para iniciar instâncias usando a AMI habilitada para EC2 Fast Launch. Para ter mais informações, consulte the section called “Perfil vinculado a serviço”.

Para visualizar as permissões para esta política, consulte EC2FastLaunchServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: Ec2InstanceConnectEndpoint

Essa política é anexada a um perfil vinculado a serviço chamado AWSServiceRoleForEC2InstanceConnect para permitir que o EC2 Instance Connect Endpoint execute ações em seu nome. Para ter mais informações, consulte Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint.

Para visualizar as permissões para esta política, consulte Ec2InstanceConnectEndpoint na Referência de políticas gerenciadas pela AWS.

Atualizações do Amazon EC2 para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o Amazon EC2 desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
EC2FastLaunchFullAccess – Nova política	O Amazon EC2 adicionou essa política para realizar ações de API relacionadas ao atributo EC2 Fast Launch em uma instância. A política pode ser anexada ao perfil de instância para uma instância que é iniciada usando uma	14 de maio de 2024

Alteração	Descrição	Data
	AMI habilitada para o EC2 Fast Launch.	
AWSEC2VssSnapshotPolicy – Nova política	O Amazon EC2 adicionou a política `AWSEC2VssSnapshotPolicy` que contém permissões para criar e adicionar tags a images de máquina da Amazon (AMIs) e a snapshots do EBS.	28 de março de 2024
EC2FastLaunchServiceRolePolicy – Nova política	O Amazon EC2 adicionou o atributo EC2 Fast Launch para habilitar as AMIs do Windows a executar instâncias mais rapidamente criando um conjunto de snapshots pré-provisionados.	26 de novembro de 2021
O Amazon EC2 passou a monitorar as alterações	O Amazon EC2 passou a controlar as alterações nas políticas gerenciadas pela AWS.	1º de março de 2021

Funções do IAM para Amazon EC2

As aplicações devem assinar suas solicitações de API com as credenciais da AWS. Portanto, se você for um desenvolvedor de aplicações, precisará de uma estratégia para gerenciar credenciais para suas aplicações que executam em instâncias do EC2. Por exemplo, é possível distribuir de maneira segura suas credenciais da AWS para as instâncias, permitindo que as aplicações nessas instâncias usem suas credenciais para assinar solicitações, enquanto protege suas credenciais de outros usuários. Contudo, é um desafio distribuir credenciais para cada instância de maneira segura, especialmente aquelas que a AWS cria em seu nome, como instâncias spot ou instâncias em grupos do Auto Scaling. Você também deve poder atualizar as credenciais em cada instância quando alterna suas credenciais da AWS.

> **Note**
>
> Para suas workloads do Amazon EC2, recomendamos recuperar as credenciais da sessão usando o método descrito abaixo. Essas credenciais devem permitir que sua workload faça solicitações da API da AWS sem precisar usar `sts:AssumeRole` para assumir a mesma função que já está associada à instância. A menos que seja necessário passar etiquetas de sessão para controle de acesso por atributo (ABAC) ou passar uma política de sessão para restringir ainda mais as permissões da função, essas chamadas de suposição de função são desnecessárias, pois criam um novo conjunto das mesmas credenciais de sessão de função temporária.
>
> Se sua workload usa uma função para assumir a si mesma, é necessário criar uma política de confiança que permita explicitamente que essa função se assuma sozinha. Se a política de confiança não for criada, o erro `AccessDenied` ocorrerá. Para obter mais informações, consulte Modificar uma política de confiança de função no Guia do usuário do IAM.

Projetamos funções do IAM para que suas aplicações possam fazer solicitações de API de suas instâncias de maneira segura, sem exigir que você gerencie as credenciais de segurança que as aplicações usam. Em vez de criar e distribuir suas credenciais da AWS, é possível delegar permissão para fazer solicitações de API usando funções do IAM da seguinte forma:

1. Crie uma função do IAM.
2. Defina quais contas ou serviços da AWS podem assumir a função.
3. Defina quais ações e recursos de API a aplicação pode usar depois de assumir a função.
4. Especifique a função quando você executar a instância ou anexe a função a uma instância existente.
5. Faça com que a aplicação recupere um conjunto de credenciais temporárias e use-as.

Por exemplo, é possível usar funções do IAM para conceder permissões a aplicações em execução em suas instâncias que precisam usar um bucket no Amazon S3. É possível especificar permissões para funções do IAM criando uma política em formato JSON. Essas são semelhantes às políticas que você cria para os usuários do . Se você alterar uma função, a alteração será propagada para todas as instâncias.

> **Note**
>
> As credenciais do perfil do IAM do Amazon EC2 não estão sujeitas às durações máximas de sessão configuradas no perfil. Para obter mais informações, consulte Como usar funções do IAM no Guia do usuário do IAM.

Ao criar funções do IAM, associe políticas do IAM de privilégio mínimo que restringem o acesso às chamadas de API específicas exigidas pelo aplicativo. Para comunicação Windows para Windows, use grupos e funções bem definidos e bem documentados do Windows para conceder acesso no nível de aplicação entre instâncias do Windows. Grupos e funções permitem que os clientes definam permissões de aplicação de privilégio mínimo e no nível de pasta do NTFS para limitar o acesso a requisitos específicos da aplicação.

Você só pode anexar uma função do IAM a uma instância, mas pode anexar a mesma função a muitas instâncias. Para obter mais informações sobre como criar e usar funções do IAM, consulte Funções no Guia do usuário do IAM.

É possível aplicar permissões em nível de recurso às políticas do IAM para controlar a capacidade de anexar, substituir ou desanexar funções do IAM de uma instância. Para obter mais informações, consulte Permissões no nível do recurso com suporte para ações de API do Amazon EC2 e o seguinte exemplo: Exemplo: trabalhar com funções do IAM.

Tópicos

- Perfis de instância
- Recuperar credenciais de segurança dos metadados da instância
- Conceder uma permissão de usuário do IAM para passar um perfil do IAM para uma instância
- Trabalhar com funções do IAM

Perfis de instância

O Amazon EC2 usa um perfil de instância como um contêiner para uma função do IAM. Se você criar uma função do IAM usando o console do IAM o console criará automaticamente um perfil de instância e dará a ele o mesmo nome da função correspondente. Se você usar o console do Amazon EC2 para executar uma instância com uma função do IAM ou anexar uma função do IAM a uma instância, deve escolher a função com base em uma lista de nomes de perfis de instância.

Se você usar a AWS CLI, a API ou um AWS SDK para criar uma função, você cria a função e o perfil da instância como ações separadas, com nomes potencialmente diferentes. Se você usar a AWS CLI, a API ou o AWS SDK para iniciar uma instância com uma função do IAM ou para anexar uma função do IAM a uma instância, especifique o nome do perfil da instância.

Um perfil de instância pode conter somente uma função do IAM. Este limite não pode ser aumentado.

Para obter mais informações, consulte Perfis de instâncias no Guia do usuário do IAM.

Recuperar credenciais de segurança dos metadados da instância

Uma aplicação na instância recupera as credenciais de segurança fornecidas pela função no item `iam/security-credentials/`role-name dos metadados da instância. A aplicação recebe as permissões para as ações e recursos que você definiu para a função por meio das credenciais de segurança associadas à função. Essas credenciais de segurança são temporárias e são alternadas automaticamente. Tornamos novas credenciais disponíveis pelo menos cinco minutos antes da expiração das credenciais antigas.

> **Warning**
>
> Se você usar serviços que usam os metadados da instância com funções do IAM, não exponha suas credenciais quando os serviços criarem chamadas HTTP em seu nome. Os tipos de serviços que podem expor suas credenciais incluem proxies HTTP, serviços de validação HTML/CSS e processadores XML que são compatíveis com a inclusão XML.

O comando a seguir recupera as credenciais de segurança para uma função do IAM denominada `s3access`.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/
s3access
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/s3access
```

O seguinte é um exemplo de saída.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Para comandos de aplicações, AWS CLI e Tools for Windows PowerShell que são executados na instância, não é necessário obter as credenciais de segurança temporárias explicitamente – os AWS SDKs, a AWS CLI e o Tools for Windows PowerShell obtêm automaticamente as credenciais do serviço de metadados da instância do EC2 e as usam. Para fazer uma chamada fora da instância usando credenciais de segurança temporárias (por exemplo, para testar as políticas do IAM), forneça a chave de acesso, a chave secreta e o token da sessão. Para obter mais informações, consulte

Usar credenciais de segurança temporárias para solicitar acesso aos recursos da AWS no Manual do usuário do IAM.

Para obter mais informações sobre os metadados da instância, consulte Trabalhar com metadados de instância. Para obter informações sobre o endereço IP dos metadados da instância, consulte Recuperar metadados da instância.

Conceder uma permissão de usuário do IAM para passar um perfil do IAM para uma instância

Para permitir que um usuário inicie uma instância com um perfil do IAM ou anexe ou substitua um perfil do IAM em uma instância existente, conceda ao usuário permissão para usar as seguintes ações de API.

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

A política do IAM a seguir concede permissão aos usuários para iniciar instâncias com uma função do IAM ou para anexar ou substituir uma função do IAM em uma instância existente usando a AWS CLI.

> **Note**
>
> Se quiser que a política conceda aos usuários acesso a todos os seus perfis, especifique o recurso como * na política. No entanto, avalie o princípio de privilégio mínimo como uma prática recomendada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Para conceder permissão aos usuários para iniciar instâncias com uma função do IAM ou para anexar ou substituir uma função do IAM para uma instância existente usando o console do Amazon EC2, você conceda-lhes permissão para usar `iam:ListInstanceProfiles`, `iam:PassRole`, `ec2:AssociateIamInstanceProfile` e `ec2:ReplaceIamInstanceProfileAssociation`, além de quaisquer outras permissões necessárias. Para obter exemplos de políticas do , consulte Políticas de exemplo para trabalhar no console do Amazon EC2.

Trabalhar com funções do IAM

É possível criar uma função do IAM e anexá-la a uma instância durante ou depois da execução. Também é possível substituir ou desanexar uma função do IAM para uma instância.

Tópicos

- Criar uma função do IAM
- Executar uma instância com uma função do IAM
- Anexar uma função do IAM a uma instância
- Substituir uma função do IAM
- Desanexar uma função do IAM
- Gerar uma política para sua função do IAM com base na atividade de acesso

Criar uma função do IAM

Crie uma função do IAM para poder executar uma instância com essa função ou anexá-la a uma instância.

Console

Para criar uma função do IAM usando o console do IAM

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis e escolha Criar perfil.
3. Na página Selecionar entidade confiável, escolha AWS service (Serviço da AWS) e selecione o caso de uso EC2. Escolha Próximo.
4. Na página Adicionar permissões, selecione as políticas que concedem conceda às suas instâncias acesso aos recursos de que precisam. Escolha Próximo.
5. Na página Nome, revisar e criar, insira um nome e uma descrição para o perfil. Opcionalmente, adicione tags ao perfil. Selecione Criar função.

Command line

O exemplo a seguir cria uma função do IAM com uma política que permite que a função use um bucket do Amazon S3.

Para criar uma função do IAM e um perfil de instância (AWS CLI)

1. Crie a seguinte política de confiança e salve-a em um arquivo de texto chamado `ec2-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Crie a função `s3access` e especifique a política de confiança que você criou usando o comando create-role.

```
aws iam create-role \
    --role-name s3access \
```

```
    --assume-role-policy-document file://ec2-role-trust-policy.json
```

Exemplo de resposta

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2013-12-12T23:46:37.247Z",
        "RoleName": "s3access",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/s3access"
    }
}
```

3. Crie uma política de acesso e salve-a em um arquivo de texto chamado `ec2-role-access-policy.json`. Por exemplo, essa política concede permissões administrativas para o Amazon S3 a aplicações que executam na instância.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:*"],
      "Resource": ["*"]
    }
  ]
}
```

4. Anexe a política de acesso à função usando o comando put-role-policy.

```
aws iam put-role-policy \
    --role-name s3access \
    --policy-name S3-Permissions \
    --policy-document file://ec2-role-access-policy.json
```

5. Crie um perfil de instância chamado `s3access-profile` usando o comando create-instance-profile.

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

Exemplo de resposta

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. Adicione a função `s3access` ao perfil de instância `s3access-profile`.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name s3access-profile \
    --role-name s3access
```

Como alternativa, é possível usar os seguintes comandos do AWS Tools for Windows PowerShell:

- New-IAMRole
- Register-IAMRolePolicy
- New-IAMInstanceProfile

Executar uma instância com uma função do IAM

Depois de criar uma função do IAM, é possível executar uma instância e associar essa função à instância durante a execução.

> **Important**
>
> Depois de criar uma função do IAM, pode demorar vários segundos para as permissões serem propagadas. Se sua primeira tentativa de executar uma instância com uma função falhar, aguarde alguns segundos antes de tentar novamente. Para obter mais informações, consulte Solução de problemas dos perfis do IAM no Guia do usuário do IAM.

New console

Para executar uma instância com uma função do IAM (console)

1. Siga o procedimento para iniciar uma instância.
2. Em Advanced details (Detalhes avançados), em IAM instance profile (Perfil de instância do IAM), selecione o perfil do IAM que você criou.

   > **Note**
   >
   > A lista IAM instance profile (Perfil de instância do IAM) exibe o nome do perfil da instância que você criou ao criar o perfil do IAM. Se você tiver criado a função do IAM usando o console, o perfil da instância terá sido criado para você e recebido o mesmo nome da função. Se você tiver criado a função do IAM usando a AWS CLI, a API ou um SDK da AWS, será possível ter dado um nome diferente para o perfil da instância.

3. Configure outros detalhes necessários para a instância ou aceite os padrões e selecione um par de chaves. Para obter informações sobre os campos do assistente de execução de instâncias, consulte Iniciar uma instância usando parâmetros definidos.
4. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
5. Se você estiver usando as ações da API do Amazon EC2 em sua aplicação, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O AWS SDK da cuida disso para você.

IMDSv2

Para instâncias do Linux, consulte o seguinte exemplo:

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/iam/security-credentials/role_name
```

Para instâncias do Windows, consulte o seguinte exemplo:

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Para instâncias do Linux, consulte o seguinte exemplo:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Para instâncias do Windows, consulte o seguinte exemplo:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Old console

Para executar uma instância com uma função do IAM (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Selecione um AMI e um tipo de instância e escolha Next: Configure Instance Details.

4. Na página Configure Instance Details, para IAM role, selecione a função do IAM que você criou.

   > **Note**
   >
   > A lista IAM role exibe o nome do perfil da instância que você criou ao criar a função do IAM. Se você tiver criado a função do IAM usando o console, o perfil da instância terá sido criado para você e recebido o mesmo nome da função. Se você tiver criado a função do IAM usando a AWS CLI, a API ou um SDK da AWS, será possível ter dado um nome diferente para o perfil da instância.

5. Configure todos os outros detalhes e siga as instruções no restante do assistente, ou escolha Review and Launch para aceitar as configurações padrão e vá diretamente para a página Review Instance Launch.
6. Reveja as configurações e selecione Launch para escolher um par de chaves e executar a instância.
7. Se você estiver usando as ações da API do Amazon EC2 em sua aplicação, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O AWS SDK da cuida disso para você.

   IMDSv2

   Para instâncias do Linux, consulte o seguinte exemplo:

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

   Para instâncias do Windows, consulte o seguinte exemplo:

   ```
   PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
   ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
   credentials/role_name
   ```

IMDSv1

Para instâncias do Linux, consulte o seguinte exemplo:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Para instâncias do Windows, consulte o seguinte exemplo:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Command line

Você pode usar a AWS CLI para associar um perfil a uma instância durante a inicialização. Especifique o perfil da instância no comando.

Para iniciar uma instância com uma função do IAM (AWS CLI)

1. Use o comando run-instances para executar uma instância usando o perfil da instância. O exemplo a seguir mostra como executar uma instância com o perfil da instância.

```
aws ec2 run-instances \
    --image-id ami-11aa22bb \
    --iam-instance-profile Name="s3access-profile" \
    --key-name my-key-pair \
    --security-groups my-security-group \
    --subnet-id subnet-1a2b3c4d
```

   Como alternativa, use o comando New-EC2Instance do Tools for Windows PowerShell.

2. Se você estiver usando as ações da API do Amazon EC2 em sua aplicação, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O AWS SDK da cuida disso para você.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Anexar uma função do IAM a uma instância

Para anexar uma função do IAM a uma instância sem função, a instância pode estar no estado `stopped` ou `running`.

Console

Como anexar uma função do IAM a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).
4. Selecione a função do IAM a ser anexada à instância e selecione Save (Salvar).

Command line

Para anexar uma função do IAM a uma instância (AWS CLI)

1. Se necessário, descreva as instâncias para obter o ID da instância à qual anexar a função.

```
aws ec2 describe-instances
```

2. Use o comando associate-iam-instance-profile para anexar a função do IAM à instância especificando o perfil de instância. É possível usar o Nome de recursos da Amazon (ARN) do perfil da instância ou o seu nome.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

Exemplo de resposta

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
```

```
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

Como alternativa, use os seguintes comandos do Tools for Windows PowerShell:

- Get-EC2Instance
- Register-EC2IamInstanceProfile

Substituir uma função do IAM

Para substituir a função do IAM em uma instância que já tenha uma função do IAM anexa, a instância deve estar no estado `running`. Será possível fazer isso se quiser alterar a função do IAM de uma instância sem desanexar a existente primeiro. Por exemplo, é possível fazer isso para garantir que as ações de API desempenhadas por aplicações executadas na instância não sejam interrompidas.

Console

Como substituir uma função do IAM para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).
4. Selecione a função do IAM a ser anexada à instância e selecione Save (Salvar).

Command line

Para substituir uma função do IAM em uma instância (AWS CLI)

1. Se necessário, descreva as associações do perfil da instância do IAM para obter o ID da associação do perfil da instância do IAM a ser substituído.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Use o comando replace-iam-instance-profile-association para substituir o perfil de instância do IAM especificando o ID da associação do perfil da instância existente e o ARN ou o nome do perfil da instância que deve substituí-lo.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

Exemplo de resposta

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

Como alternativa, use os seguintes comandos do Tools for Windows PowerShell:

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

Desanexar uma função do IAM

É possível desanexar uma função do IAM de uma instância em execução ou parada.

Console

Como desanexar uma função do IAM de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).

4. Em IAM role (Função do IAM), selecione No IAM Role (Nenhuma função do IAM). Escolha Save (Salvar).
5. Na caixa de diálogo de confirmação, insira Detach (Desanexar) e selecione Detach (Desanexar).

Command line

Para desanexar uma função do IAM de uma instância (AWS CLI)

1. Se necessário, use describe-iam-instance-profile-associations para descrever as associações do perfil da instância do IAM e obter o ID da associação do perfil da instância do IAM a ser desanexado.

```
aws ec2 describe-iam-instance-profile-associations
```

Exemplo de resposta

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Use o comando disassociate-iam-instance-profile para desanexar o perfil da instância do IAM usando o ID da associação.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

Exemplo de resposta

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

Como alternativa, use os seguintes comandos do Tools for Windows PowerShell:

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

Gerar uma política para sua função do IAM com base na atividade de acesso

Quando você cria uma função do IAM pela primeira vez para suas aplicações, às vezes é possível conceder permissões além do que é necessário. Antes de iniciar sua aplicação em seu ambiente de produção, é possível gerar uma política do IAM baseada na atividade de acesso para uma função do IAM. O IAM Access Analyzer revisa seus logs do AWS CloudTrail e gera um modelo de política que contém as permissões que foram usadas pela função no intervalo de datas especificado. É possível usar o modelo para criar uma política gerenciada com permissões refinadas e anexá-la à função do IAM. Dessa forma, você concede apenas as permissões necessárias à interação com os recursos da AWS, de acordo com a especificidade do caso de uso. Isso ajuda você a aderir às melhores práticas de conceder privilégio mínimo. Para saber mais, consulte Gerar políticas com base na atividade de acesso no Guia do usuário do IAM.

Acessar o Amazon EC2 usando um endpoint da VPC de interface

É possível melhorar o procedimento de segurança de sua VPC criando uma conexão privada entre sua VPC e o Amazon EC2. É possível acessar o Amazon EC2 como se estivesse em sua VPC, sem usar um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para acessar o Amazon EC2.

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink.

Conteúdo

- Criar um VPC endpoint de interface
- Criar uma política de endpoint

Criar um VPC endpoint de interface

Crie um endpoint de interface para o Amazon EC2 usando o seguinte nome de serviço:

- com.amazonaws.*região*.ec2: cria um endpoint para as ações da API do Amazon EC2.

Para obter mais informações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint de VPC de interface, no Guia do AWS PrivateLink.

Criar uma política de endpoint

Uma política de endpoint é um recurso do IAM que você pode anexar ao endpoint de interface. A política de endpoint padrão permite acesso total à API do Amazon EC2 por meio do endpoint de interface. Para controlar o acesso permitido à API do Amazon EC2 pela VPC, anexe uma política de endpoint personalizada ao endpoint de interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem executar ações.
- As ações que podem ser executadas.
- O recurso no qual as ações podem ser executadas.

> **Important**
>
> Quando uma política não padrão é aplicada a um endpoint da VPC de interface para o Amazon EC2, determinadas solicitações de API com falha, como as com falha de `RequestLimitExceeded`, podem não ser registradas no AWS CloudTrail nem no Amazon CloudWatch.

Para obter mais informações, consulte Control access to services using endpoint policies (Controlar o acesso a serviços usando políticas de endpoint) no Guia do AWS PrivateLink.

O exemplo a seguir mostra uma política de VPC endpoint que nega permissão para criar volumes não criptografados ou executar instâncias com volumes não criptografados. O exemplo de política também concede permissão para executar todas as outras ações do Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Gerenciamento de atualizações para instâncias do Windows do Amazon EC2

Recomendamos que você aplique patches, atualize e proteja regularmente o sistema operacional e as aplicações em suas instâncias do EC2. É possível usar o Gerenciador de patches do AWS Systems Manager para automatizar o processo de instalação de atualizações relacionadas à segurança para o sistema operacional e para a aplicação.

Para instâncias do EC2 em um grupo de Auto Scaling, você pode usar o AWS-PatchAsgInstance runbook para ajudar a evitar que instâncias que estão passando por patches sejam substituídas Como alternativa, é possível usar qualquer serviço de atualização automática ou processos recomendados para instalar atualizações fornecidas pelo fornecedor da aplicação.

Recursos

- AL2023: Updating AL2023 no Guia do usuário do Amazon Linux 2023.
- AL2: Manage software on your Amazon Linux 2 instance no Guia do usuário do Amazon Linux 2.
- Instâncias do Windows: the section called “Gerenciamento de atualizações”.

Práticas recomendadas de segurança para instâncias do Windows

Recomendamos seguir estas práticas recomendadas de segurança para as instâncias do Windows.

Conteúdo

- Práticas recomendadas de segurança de alto nível
- Gerenciamento de atualizações
- Gerenciamento de configuração
- Gerenciamento de alterações
- Auditoria e responsabilidade para instâncias do Windows do Amazon EC2

Práticas recomendadas de segurança de alto nível

Você deve seguir as seguintes práticas recomendadas de segurança de alto nível para as instâncias do Windows:

- Menos acesso: conceda acesso somente a sistemas e locais confiáveis e esperados. Isso se aplica a todos os produtos da Microsoft, como o Active Directory, servidores de produtividade empresarial da Microsoft e serviços de infraestrutura, como Serviços de área de trabalho remota, servidores de proxy reverso, servidores Web IIS e outros. Use os recursos da AWS, como os grupos de segurança da instância do Amazon EC2, listas de controle de acesso (ACLs) à rede e sub-redes públicas/privadas da Amazon VPC, para colocar a segurança em camadas em vários locais em uma arquitetura. Em uma instância do Windows, os clientes podem usar o Firewall do Windows para colocar mais uma camada na estratégia de defesa completa em sua implantação. Instale apenas os componentes e aplicativos do sistema operacional necessários para que o sistema funcione conforme projetado. Configure serviços de infraestrutura, como o IIS, para serem executados em contas de serviço ou para usar recursos como identidades de grupo de aplicações para acessar recursos local e remotamente na infraestrutura.
- Privilégio mínimo: determine o conjunto mínimo de privilégios de que as instâncias e contas precisam para executar as funções. Restringir esses servidores e usuários para permitir apenas essas permissões definidas. Use técnicas, como controles de acesso baseados em função, para reduzir a área de superfície das contas administrativas e criar as funções mais limitadas para realizar uma tarefa. Use recursos do sistema operacional, como o Encrypting File System (EFS – Criptografia do sistema de arquivos) dentro do NTFS, para criptografar dados confidenciais em repouso e controlar o acesso de aplicações e de usuários a ele.
- Gerenciamento de configuração: crie uma configuração de linha de base do servidor que incorpore a aplicação de patches de segurança atualizados e pacotes de proteção baseados em host que incluem antivírus, antimalware, detecção e prevenção de invasões, e monitoramento da integridade dos arquivos. Avalie cada servidor em relação à linha de base registrada atual para identificar e sinalizar quaisquer desvios. Verifique se cada servidor está configurado para gerar e armazenar com segurança os dados adequados de log e auditoria.
- Gerenciamento de alterações: crie processos para controlar as alterações nas linhas de base da configuração do servidor e trabalhe em processos de alterações totalmente automatizados. Além disso, aproveite Just Enough Administration (JEA) com o Windows PowerShell DSC para limitar o acesso administrativo às funções mínimas necessárias.
- Gerenciamento de patches: implemente processos que corrijam, atualizem e protejam o sistema operacional e as aplicações, regularmente, nas instâncias do EC2.
- Logs de auditoria: audite o acesso e todas as alterações nas instâncias do Amazon EC2 para verificar a integridade do servidor e garantir que somente alterações autorizadas sejam feitas. Utilize funcionalidades como Enhanced Log for IIS (Log aprimorado para IIS) para melhorar os recursos de registo de log padrão. Os recursos da AWS como Logs de fluxo da VPC e

AWS CloudTrail também estão disponíveis para auditar o acesso à rede, incluindo solicitações permitidas/negadas e chamadas de API, respectivamente.

Gerenciamento de atualizações

Para garantir os melhores resultados ao executar o Windows Server no Amazon EC2, recomendamos implantar as seguintes práticas recomendadas:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Reiniciar a instância do Windows após instalar as atualizações. Para ter mais informações, consulte Reinicializar a instância.

Para obter informações sobre como atualizar ou migrar uma instância do Windows para uma versão mais recente do Windows Server, consulte Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server..

Configurar o Windows Update

Por padrão, as instâncias iniciadas usando AMIs do AWS Windows Server não recebem atualizações por meio do Windows Update.

Atualizar drivers do Windows

Mantenha os drivers mais recentes em todas as instâncias do EC2 do Windows para garantir que as correções de problemas e melhorias de performance mais recentes sejam aplicadas em toda a sua frota. Dependendo do tipo de instância, você deve atualizar os drivers PV da AWS, do Amazon ENA e do AWS NVMe.

- Use tópicos do SNS para receber atualizações de novos lançamentos de driver.
- Use o runbook do AWS Systems Manager Automation AWSSupport-UpgradeWindowsAWSDrivers para aplicar facilmente as atualizações em todas as instâncias.

Iniciar instâncias usando as AMIs mais recentes do Windows

A AWS realiza o lançamento de AMIs do Windows todos os meses. Essas AMIs contêm os patches, os drivers e os agentes de inicialização mais recentes para o sistema operacional. É necessário utilizar a AMI mais recente ao executar novas instâncias ou ao criar suas próprias imagens personalizadas.

- Para visualizar atualizações para cada versão das AMIs do Windows na AWS, consulte Histórico de versões da AMI do Windows na AWS.
- Para criar com as AMIs mais recentes disponíveis, consulte Consulta para a AMI mais recente do Windows usando o Systems Manager Parameter Store.
- Para obter mais informações sobre as AMIs do Windows especializadas que você pode usar para iniciar instâncias para o seu banco de dados e casos de uso de proteção de conformidade, consulte Specialized Windows AMIs na Referência de AMI do Windows da AWS.

Testar a performance do sistema/aplicação antes da migração

Migrar aplicativos empresariais para a AWS pode envolver muitas variáveis e configurações. Sempre teste a performance da solução do EC2 para garantir que:

- Os tipos de instância estão configurados corretamente, incluindo o tamanho da instância, as redes avançadas e a locação (compartilhada ou dedicada).
- A topologia da instância é apropriada para a workload e utiliza recursos de alta performance quando necessário, com locação dedicada, grupos de alocação, volumes de armazenamento de instâncias e bare metal.

Atualizar agentes de inicialização

Atualize para o agente EC2Launch v2 mais recente para garantir que os aprimoramentos mais recentes sejam aplicados em toda a sua frota. Para ter mais informações, consulte the section called “Migrar”.

Se você tiver uma frota mista ou quiser continuar usando os agentes EC2Launch (Windows Server 2016 e 2019) ou EC2 Config (somente SO herdado), atualize para as versões mais recentes dos respectivos agentes.

Há suporte para as atualizações automáticas nas seguintes combinações de agentes de execução e versão do Windows Server. É possível optar por receber atualizações automáticas no console SSM Quick Setup Host Management em Amazon EC2 Launch Agents.

Versão do Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Para obter mais informações sobre a atualização para o EC2Launch v2, consulte the section called “Instalar”.
- Para obter informações sobre como atualizar manualmente o EC2Config, consulte the section called “Instalar o EC2Config”.
- Para obter informações sobre como atualizar manualmente o EC2Launch, consulte the section called “Instalar o EC2Launch”.

Gerenciamento de configuração

As imagens de máquina da Amazon (AMIs) fornecem uma configuração inicial para uma instância do Amazon EC2, que inclui o sistema operacional Windows e personalizações opcionais específicas do cliente, como aplicações e controles de segurança. Crie um catálogo de AMI que contém linhas de base de configuração de segurança personalizadas para garantir que todas as instâncias do Windows sejam iniciadas com controles de segurança padrão. As linhas de base de segurança podem ser incorporadas em uma AMI, inicializadas dinamicamente quando uma instância do EC2 é executada ou empacotadas como um produto para distribuição uniforme por meio de portfólios do AWS Service Catalog. Para obter mais informações sobre como proteger uma AMI, consulte Práticas recomendadas para criar uma AMI.

Cada instância do Amazon EC2 deve aderir aos padrões de segurança organizacional. Não instale nenhuma função e recurso do Windows que não seja necessário e instale software (antivírus, antimalware, mitigação de vulnerabilidades) para proteger contra códigos mal-intencionados, monitore a integridade do host e execute a detecção de intrusões. Configure o software de segurança para monitorar e manter as configurações de segurança do SO, proteger a integridade

de arquivos críticos do SO e alertar sobre desvios da linha de base de segurança. Considere implementar benchmarks recomendados de configuração de segurança publicados pela Microsoft, pelo Centro de Segurança da Internet (CIS) ou pelo National Institute of Standards and Technology (NIST). Considere usar outras ferramentas da Microsoft para servidores de aplicações específicos, como o Analisador de melhores práticas para SQL Server.

Os clientes da AWS também podem executar avaliações do Amazon Inspector para aprimorar a segurança e a conformidade das aplicações implantadas nas instâncias do Amazon EC2. O Amazon Inspector avalia automaticamente as aplicações quanto a vulnerabilidades ou desvios das práticas recomendadas e inclui uma base de conhecimento de centenas de regras mapeadas para padrões comuns de conformidade de segurança (por exemplo, PCI DSS) e definições de vulnerabilidade. Exemplos de regras incorporadas incluem verificar se o início remoto de sessão raiz está habilitado ou se versões de software vulneráveis estão instaladas. Essas regras são atualizadas regularmente pelos pesquisadores de segurança da AWS.

Ao proteger instâncias do Windows, recomendamos que você implemente os Serviços de Domínio do Active Directory para habilitar uma infraestrutura escalável, segura e gerenciável para locais distribuídos. Além disso, depois de iniciar instâncias por meio do console do Amazon EC2 ou usar uma ferramenta de provisionamento do Amazon EC2, como AWS CloudFormation, é recomendável utilizar recursos nativos do SO, como o Microsoft Windows PowerShell DSC, para manter o estado de configuração em caso de oscilação de configuração.

Gerenciamento de alterações

Depois que as linhas de base de segurança iniciais forem aplicadas às instâncias do Amazon EC2 durante a execução, controle as alterações contínuas do Amazon EC2 para manter a segurança das máquinas virtuais. Estabeleça um processo de gerenciamento de alterações para autorizar e incorporar alterações aos recursos da AWS (como grupos de segurança, tabelas de rotas e ACLs de rede), bem como a configurações do SO e de aplicações (como aplicação de patches do Windows ou da aplicação, atualizações de software ou atualizações de arquivos de configuração).

A AWS fornece várias ferramentas para ajudar a gerenciar alterações nos recursos da AWS, incluindo o AWS CloudTrail, o AWS Config, o AWS CloudFormation, o AWS Elastic Beanstalk, o AWS OpsWorks, e pacotes de gerenciamento para o Systems Center Operations Manager e o System Center Virtual Machine Manager. Observe que a Microsoft lança patches do Windows na segunda terça-feira de cada mês (ou conforme necessário), e a AWS atualiza todas as AMIs do Windows gerenciadas pela AWS em até cinco dias após a Microsoft lançar um patch. Portanto, é importante corrigir continuamente todas as AMIs de linha de base, atualizar modelos do AWS

CloudFormation e configurações de grupo de Auto Scaling com os IDs de AMI mais recentes e implementar ferramentas para automatizar o gerenciamento de patches de instâncias em execução.

A Microsoft fornece várias opções para gerenciar o sistema operacional Windows e as alterações de aplicações. O SCCM, por exemplo, fornece cobertura completa do ciclo de vida das modificações do ambiente. Selecione ferramentas que atendam aos requisitos comerciais e controlem como as alterações afetarão os SLAs de aplicações, a capacidade, a segurança e os procedimentos de recuperação de desastres. Evite alterações manuais e, em vez disso, utilize o software de gerenciamento de configuração automatizado ou ferramentas da linha de comando, como o Run Command do EC2 ou o Windows PowerShell, para implementar processos de alteração com script e repetíveis. Para ajudar com esse requisito, use bastion hosts com registro em log aprimorado para todas as interações com suas instâncias do Windows para garantir que todos os eventos e tarefas sejam gravados automaticamente.

Auditoria e responsabilidade para instâncias do Windows do Amazon EC2

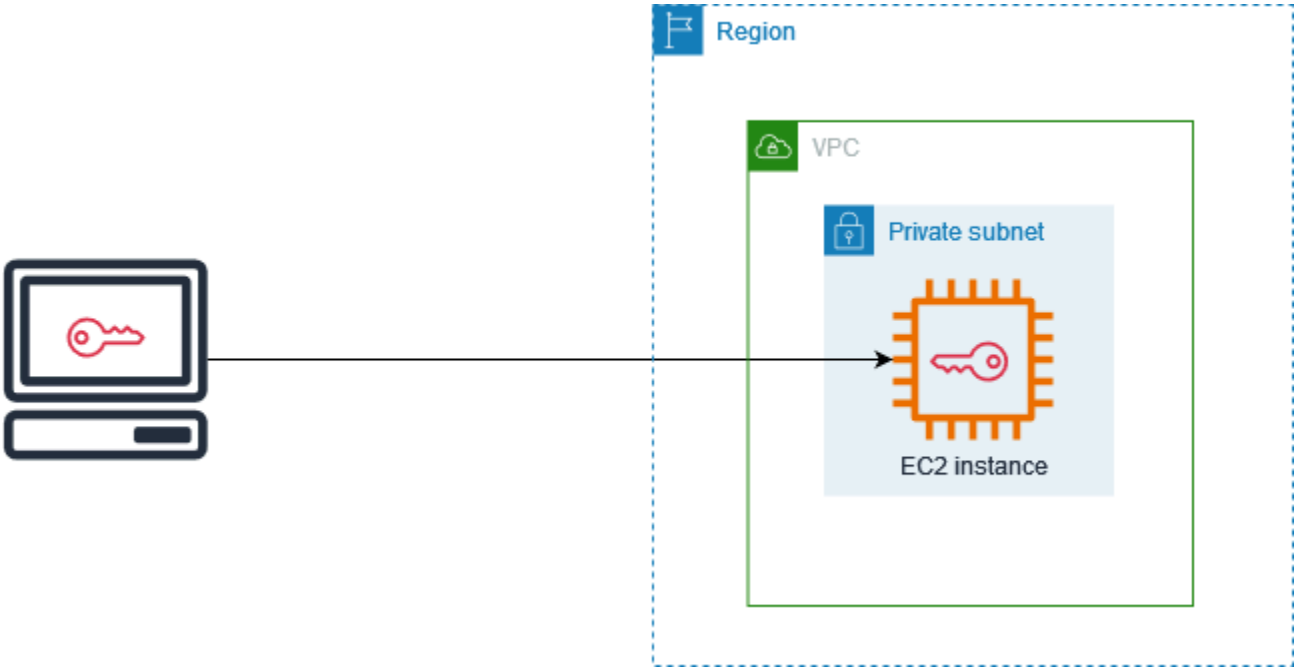
O AWS CloudTrail, o AWS Config e o Regras do AWS Config fornecem recursos de auditoria e controle de alterações para a auditoria de alterações de recursos da AWS. Configure os logs de eventos do Windows para enviar arquivos de log locais a um sistema centralizado de gerenciamento de logs a fim de preservar os dados de log para a análise de comportamento operacional e de segurança. O Microsoft System Center Operations Manager (SCOM) agrega informações sobre aplicações da Microsoft implantadas em instâncias do Windows e aplica conjuntos de regras pré-configurados e personalizados com base em funções e serviços de aplicações. Os Pacotes de Gerenciamento do System Center são baseados no SCOM para fornecer monitoramento e orientações de configuração específicos da aplicação. Esses Pacotes de Gerenciamento oferecem suporte ao Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 e muitos mais servidores e tecnologias.

Além das ferramentas de gerenciamento de sistemas da Microsoft, os clientes podem usar o Amazon CloudWatch para monitorar a utilização da CPU da instância, a performance do disco, a E/S da rede e realizar verificações de status do host e da instância. Os agentes de inicialização EC2Config, EC2Launch e EC2Launch v2 fornecem acesso a recursos avançados adicionais para instâncias do Windows. Por exemplo, eles podem exportar logs do sistema, de segurança, de aplicações e de Serviços de Informações da Internet (IIS) do Windows para o CloudWatch Logs, os quais poderão ser integrados a métricas e alarmes do Amazon CloudWatch. Os clientes também podem criar scripts que exportam contadores de performance do Windows para métricas personalizadas do Amazon CloudWatch.

Pares de chaves do Amazon EC2 e instâncias do Amazon EC2

Um par de chaves, que consiste em uma chave pública e uma chave privada, trata-se de um conjunto de credenciais de segurança usadas para provar sua identidade ao se conectar a uma instância do Amazon EC2. Para instâncias do Linux, a chave privada permite usar o SSH com segurança en sua instância. Para instâncias do Windows, a chave privada é necessária para descriptografar a senha de administrador, que você poderá então usar para se conectar à instância.

O Amazon EC2 armazena a chave pública na instância, e você armazena a chave privada, conforme mostrado no diagrama a seguir. É importante armazenar sua chave privada em um local seguro, pois qualquer pessoa que tiver acesso a ela poderá se conectar a suas instâncias que usam o par de chaves.



Ao iniciar uma instância, é possível especificar um par de chaves para poder se conectar à instância usando um método que requer um par de chaves. Dependendo de como você gerencia sua segurança, é possível especificar o mesmo par de chaves para todas as suas instâncias ou especificar pares de chaves diferentes.

Para instâncias do Linux, quando a instância é inicializada pela primeira vez, a chave pública que você especificou na inicialização é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`. Ao conectar-se à instância do Linux usando SSH, especifique a chave privada que corresponde à chave pública para fazer login.

Para obter mais informações sobre como se conectar à instância do EC2, consulte Conexão com a instância do EC2.

> **Important**
>
> Como o Amazon EC2 não mantém uma cópia da sua chave privada, não há como recuperar a chave privada caso você a perca. No entanto, ainda pode haver uma maneira de se conectar a instâncias para as quais você perdeu a chave privada. Para ter mais informações, consulte Perdi minha chave privada. Como posso me conectar à minha instância do Linux?.

Como alternativa aos pares de chaves, é possível usar AWS Systems Manager Session Manager para se conectar à instância como um shell interativo de um clique baseado no navegador ou a AWS Command Line Interface (AWS CLI).

Conteúdo

- Criar um par de chaves para sua instância do Amazon EC2
- Marcar um par de chaves
- Descrever seus pares de chaves
- Excluir o par de chaves
- Adição ou remoção de uma chave pública na instância do Linux
- Verificar a impressão digital do par de chaves

Criar um par de chaves para sua instância do Amazon EC2

É possível usar o Amazon EC2 para criar seus pares de chaves ou usar uma ferramenta de terceiros para criar seus pares de chaves e depois importá-los para o Amazon EC2.

O Amazon EC2 é compatível com as chaves SSH-2 RSA de 2.048 bits para instâncias do Linux e do Windows. Além disso, o Amazon EC2 é compatível com chaves ED25519 para instâncias do Linux.

Para obter as etapas de conexão à instância do Linux usando SSH depois de criar um par de chaves, consulte the section called “Conecte-se à sua instância do Linux”.

Para obter as etapas de conexão à instância do Windows usando RDP depois de criar um par de chaves, consulte the section called “Conectar-se à sua instância do Windows do ”.

Conteúdo

- Criar um par de chaves usando o Amazon EC2
- Criar um par de chaves usando o AWS CloudFormation
- Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

Criar um par de chaves usando o Amazon EC2

Quando você criar um par de chaves usando o Amazon EC2, a chave pública será armazenada no Amazon EC2 e você armazenará a chave privada.

É possível criar até 5.000 pares de chaves por região. Para solicitar um aumento de cota, crie um caso de suporte. Para obter mais informações, consulte Criação de um caso de suporte no Guia do usuário do AWS Support.

Console

Para criar um par de chaves usando o Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Rede e segurança, selecione Pares de chaves.
3. Escolha Create key pair (Criar par de chaves).
4. Em Name (Nome), insira um nome descritivo para o par de chaves. O Amazon EC2 associa a chave pública ao nome especificado como o nome da chave. Um nome de chave pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.
5. Selecione um tipo de par de chaves apropriado para seu sistema operacional:

   (Instâncias do Linux) Em Tipo de par de chaves, escolha RSA ou ED25519.

   (Instâncias do Windows) Em Tipo de par de chaves, escolha RSA. As chaves ED25519 não são compatíveis com as instâncias do Windows.
6. Para Formato de arquivo de chave privada, escolha o formato no qual salvar a chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha ppk.
7. Para adicionar uma etiqueta à chave pública, escolha Adicionar etiqueta, e insira a chave e o valor da etiqueta. Repita esse procedimento para cada tag.

8. Escolha Create key pair (Criar par de chaves).
9. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como o nome do par de chaves, e a extensão do nome do arquivo é determinada pelo formato do arquivo escolhido. Salve o arquivo de chave privada em um lugar seguro.

   > **Important**
   >
   > Esta é a única chance de você salvar o arquivo de chave privada.

10. (Instâncias do Linux) Se você planeja usar um cliente SSH em um computador macOS ou Linux para se conectar à instância do Linux, use o comando apresentado a seguir para definir as permissões do arquivo de chave privada para que somente você possa lê-lo.

    ```
    chmod 400 key-pair-name.pem
    ```

    Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para ter mais informações, consulte Erro: arquivo de chave privada desprotegido.

AWS CLI

Para criar um par de chaves usando o Amazon EC2

1. Use o comando create-key-pair da seguinte forma para gerar um par de chaves e salvar a chave privada em um arquivo `.pem`.

   Para o `--key-name`, especifique um nome para a chave pública. O nome pode incluir até 255 caracteres ASCII.

   Para o `--key-type`, especifique `rsa` ou `ed25519`. Se você não incluir o parâmetro `--key-type`, qualquer chave `rsa` é criada por padrão. Observe que não há suporte para chaves ED25519 para instâncias do Windows.

   Para o `--key-format`, especifique `pem` ou `ppk`. Se você não incluir o parâmetro `--key-format`, um arquivo `pem` será criado por padrão.

   `--query "KeyMaterial"` imprime o material da chave privada para a saída.

`--output text > my-key-pair.pem` salva o material da chave privada em um arquivo com a extensão especificada. A extensão pode ser `.pem` ou `.ppk`. A chave privada pode ter um nome diferente do nome da chave pública mas, para facilitar o uso, use o mesmo nome.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. (Instâncias do Linux) Se você planeja usar um cliente SSH em um computador macOS ou Linux para se conectar à instância do Linux, use o comando apresentado a seguir para definir as permissões do arquivo de chave privada para que somente você possa lê-lo.

```
chmod 400 key-pair-name.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para ter mais informações, consulte Erro: arquivo de chave privada desprotegido.

PowerShell

Para criar um par de chaves usando o Amazon EC2

Use o comando New-EC2KeyPair do AWS Tools for Windows PowerShell da seguinte forma para gerar a chave e salvá-la em um arquivo `.pem` ou `.ppk`.

Para o `-KeyName`, especifique um nome para a chave pública. O nome pode incluir até 255 caracteres ASCII.

Para o `-KeyType`, especifique `rsa` ou `ed25519`. Se você não incluir o parâmetro `-KeyType`, qualquer chave `rsa` é criada por padrão. Observe que não há suporte para chaves ED25519 para instâncias do Windows.

Para o `-KeyFormat`, especifique `pem` ou `ppk`. Se você não incluir o parâmetro `-KeyFormat`, um arquivo `pem` será criado por padrão.

`KeyMaterial` imprime o material da chave privada para a saída.

`Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem` salva o material da chave privada em um arquivo com a extensão especificada. A extensão pode ser `.pem` ou `.ppk`. A chave privada pode ter um nome diferente do nome da chave pública mas, para facilitar o uso, use o mesmo nome.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Criar um par de chaves usando o AWS CloudFormation

Quando você cria um novo par de chaves usando o AWS CloudFormation, a chave privada é salva no AWS Systems Manager Parameter Store. O nome do parâmetro tem o seguinte formato:

```
/ec2/keypair/key_pair_id
```

Para obter mais informações, consulte o Armazenamento de parâmetros do AWS Systems Manager, no Guia do usuário do AWS Systems Manager.

Para criar um par de chaves usando o AWS CloudFormation

1. Especifique o recurso AWS::EC2::KeyPair em seu modelo.

   ```
   Resources:
     NewKeyPair:
       Type: 'AWS::EC2::KeyPair'
       Properties:
         KeyName: new-key-pair
   ```

2. Use o comando describe-key-pairs da seguinte forma para obter o ID do par de chaves.

   ```
   aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
    KeyPairs[*].KeyPairId --output text
   ```

   O seguinte é um exemplo de saída.

   ```
   key-05abb699beEXAMPLE
   ```

3. Use o comando get-parameter da seguinte forma para obter o parâmetro para sua chave e salvar o material da chave em um arquivo `.pem`.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Permissões obrigatórias do IAM

Para habilitar o AWS CloudFormation a gerenciar parâmetros da Parameter Store em seu nome, o perfil do IAM assumido pelo AWS CloudFormation ou seu usuário devem ter as permissões a seguir:

- `ssm:PutParameter`: concede permissão para criar um parâmetro para o material da chave privada.
- `ssm:DeleteParameter`: concede permissão para excluir o parâmetro que armazenou o material da chave privada. Essa permissão é necessária independentemente de o par de chaves ter sido importado ou criado pelo AWS CloudFormation.

Quando o AWS CloudFormation exclui um par de chaves criado ou importado por uma pilha, ele realiza uma verificação de permissões para determinar se você tem permissão para excluir os parâmetros, embora o AWS CloudFormation só crie um parâmetro quando cria um par de chaves, não quando importa um par de chaves. O AWS CloudFormation testa a permissão necessária usando um nome de parâmetro fabricado que não corresponde a nenhum parâmetro em sua conta. Portanto, você pode ver um nome de parâmetro fabricado na mensagem de erro `AccessDeniedException`.

Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

Instâncias do Linux

Em vez de usar o Amazon EC2 para criar um par de chaves, é possível criar um par de chaves de RSA ou ED25519 usando uma ferramenta de terceiros e, então, importar a chave pública para o Amazon EC2.

Requisitos para pares de chaves

- Tipos compatíveis: RSA e ED25519. O Amazon EC2 não aceita chaves DSA.
- Formatos com suporte

  - O formato de chave pública OpenSSH (o formato em `~/.ssh/authorized_keys`). Se você se conectar usando SSH enquanto usa a API EC2 Instance Connect, o formato do SSH2 também será compatível.
  - O formato de arquivo de chave privada SSH deve ser PEM ou PPK
  - (Apenas RSA) Formato DER codificado em Base64
  - (Apenas RSA) Formato de arquivo de chave pública SSH, conforme especificado em RFC 4716
- Tamanhos compatíveis: 1024, 2048 e 4096. Se você se conectar usando SSH enquanto usa a API EC2 Instance Connect, os tamanhos compatíveis serão 2048 e 4096.

Para criar um par de chaves usando uma ferramenta de terceiros

1. Gere um par de chaves com uma ferramenta de terceiros de sua escolha. Por exemplo, é possível usar ssh-keygen (uma ferramenta fornecida com a instalação padrão de OpenSSH). Como alternativa, Java, Ruby, Python e muitas outras linguagens de programação fornecem bibliotecas padrão que é possível usar para criar um par de chaves de RSA ou ED25519.

   > **Important**
   >
   > A chave privada deve estar no formato PEM ou PPK. Por exemplo, use `ssh-keygen -m PEM` para gerar a chave OpenSSH no formato PEM.

2. Salve a chave pública em um arquivo local. Por exemplo, `~/.ssh/my-key-pair.pub`. A extensão do nome de arquivo para esse arquivo não é importante.
3. Salve a chave privada em um arquivo local que tenha a extensão `.pem` ou `.ppk`. Por exemplo, o `~/.ssh/my-key-pair.pem` ou o `~/.ssh/my-key-pair.ppk`.

   > **Important**
   >
   > Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome da chave pública ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Instâncias do Windows

Em vez de usar o Amazon EC2 para criar seu par de chaves, é possível criar um par de chaves RSA usando uma ferramenta de terceiros e, então, importar a chave pública para o Amazon EC2.

Requisitos para pares de chaves

- Tipos compatíveis: RSA. O Amazon EC2 não aceita chaves DSA.

> **Note**
>
> As chaves ED25519 não são compatíveis com as instâncias do Windows.

- Formatos com suporte
  - Formato de chave pública OpenSSH
  - O formato de arquivo de chave privada SSH deve ser PEM ou PPK
  - (Apenas RSA) Formato DER codificado em Base64
  - (Apenas RSA) Formato de arquivo de chave pública SSH, conforme especificado em RFC 4716
- Tamanhos compatíveis: 1024, 2048 e 4096.

Para criar um par de chaves usando uma ferramenta de terceiros

1. Gere um par de chaves com uma ferramenta de terceiros de sua escolha. Por exemplo, é possível usar ssh-keygen (uma ferramenta fornecida com a instalação padrão de OpenSSH). Como alternativa, Java, Ruby, Python e muitas outras linguagens de programação fornecem bibliotecas padrão que você pode usar para criar um par de chaves de RSA.

   > **Important**
   >
   > A chave privada deve estar no formato PEM ou PPK. Por exemplo, use `ssh-keygen -m PEM` para gerar a chave OpenSSH no formato PEM.

2. Salve a chave pública em um arquivo local. Por exemplo, `C:\keys\my-key-pair.pub`. A extensão do nome de arquivo para esse arquivo não é importante.
3. Salve a chave privada em um arquivo local que tenha a extensão `.pem` ou `.ppk`. Por exemplo, o `C:\keys\my-key-pair.pem` ou o `C:\keys\my-key-pair.ppk`. A extensão do nome do

arquivo para este arquivo é importante porque somente arquivos `.pem` podem ser selecionados quando você se conecta com a instância do Windows usando o console do EC2.

> **Important**
>
> Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome da chave pública ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Depois de criar o par de chaves, use um dos seguintes métodos para importar o par de chaves para Amazon EC2.

Console

Para importar a chave pública para o Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione Import key pair (Importar par de chaves).
4. Em Name (Nome), insira um nome descritivo para a chave pública. O nome pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.

   > **Note**
   >
   > Quando você se conecta à instância pelo console do EC2, o console sugere esse nome para o arquivo de chave privada.

5. Escolha Browse (Procurar) para navegar e selecionar a chave pública ou cole o conteúdo da chave pública no campo Public key contents (Conteúdo da chave pública).
6. Selecione Import key pair (Importar par de chaves).
7. Verifique se a chave pública que você importou aparece na lista de pares de chaves.

AWS CLI

Para importar a chave pública para o Amazon EC2

Use o comando import-key-pair da AWS CLI.

Como verificar se o par de chaves foi importado com êxito

Use o comando describe-key-pairs da AWS CLI.

PowerShell

Para importar a chave pública para o Amazon EC2

Use o comando Import-EC2KeyPair da AWS Tools for Windows PowerShell.

Como verificar se o par de chaves foi importado com êxito

Use o comando Get-EC2KeyPair da AWS Tools for Windows PowerShell.

Marcar um par de chaves

Para categorizar e gerenciar os pares de chaves que você criou usando o Amazon EC2 ou importou para o Amazon EC2, é possível marcá-las com metadados personalizados. Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Console

Para visualizar, adicionar ou excluir uma tag para um par de chaves

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione uma chave pública e escolha Actions (Ações), Manage tags (Gerenciar etiquetas).
4. A página Manage tags (Gerenciar etiquetas) exibe todas as etiquetas atribuídas à chave pública.
   - Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. É possível adicionar até 50 etiquetas por chave. Para obter mais informações, consulte Restrições de tags.
   - Para excluir uma tag, escolha Remove (Remover) ao lado da tag que será excluída.
5. Escolha Salvar.

AWS CLI

Para visualizar as tags para seus pares de chaves

Use o comando describe-tags da AWS CLI. No exemplo a seguir, descreva as etiquetas para todos as suas chaves o públicas.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

Para descrever as tags para um par de chaves

Use o comando describe-key-pairs da AWS CLI.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
}
```

Para marcar um par de chaves

Use o comando create-tags da AWS CLI. No exemplo a seguir, a chave pública está marcada com `Key=Cost-Center` e `Value=CC-123`.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

Como excluir uma tag de um par de chaves

Use o comando delete-tags da AWS CLI. Para obter exemplos, consulte Exemplos na Referência de Comandos da AWS CLI.

PowerShell

Para visualizar tags para seus pares de chaves

Use o comando Get-EC2Tag.

Para descrever as tags para um par de chaves

Use o comando Get-EC2KeyPair.

Para marcar um par de chaves

Use o comando New-EC2Tag.

Como excluir uma tag de um par de chaves

Use o comando Remove-EC2Tag.

Descrever seus pares de chaves

É possível descrever os pares de chaves que você armazenou no Amazon EC2. Também é possível recuperar o material da chave pública e identificar a chave pública especificada na inicialização.

Tópicos

- Descrever seus pares de chaves
- Recuperar o material da chave pública
- Identifique a chave pública que foi especificada na inicialização

Descrever seus pares de chaves

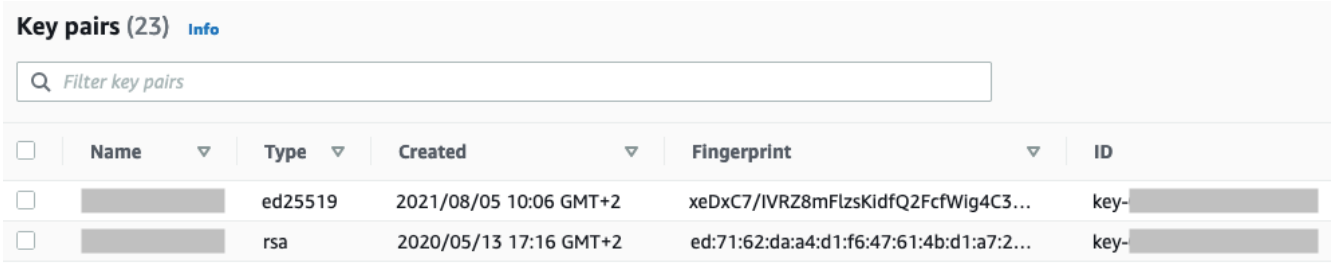
É possível visualizar as seguintes informações sobre suas chaves públicas armazenadas no Amazon EC2: nome da chave pública, ID, tipo de chave, impressão digital, material da chave pública, a data e a hora (no fuso horário UTC) em que a chave foi criada pelo Amazon EC2 (se a chave foi criada por uma ferramenta de terceiros, será mostrado a data e a hora em que a chave foi importada para o Amazon EC2) e todas as etiquetas associadas à chave pública.

É possível usar o console do Amazon EC2 ou a AWS CLI para visualizar informações sobre suas chaves públicas.

Console

Para visualizar informações sobre suas chaves públicas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Key Pairs (Pares de chaves).
3. É possível visualizar as informações sobre cada chave pública na tabela Key pairs (Pares de chaves).



4. Para visualizar as etiquetas de uma chave pública, marque a caixa de seleção ao lado da chave e escolha Actions (Ações) Manage tags (Gerenciar etiquetas).

AWS CLI

Para descrever uma chave pública

Use o comando describe-key-pairs e especifique o parâmetro `--key-names`.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Exemplo de saída

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Se preferir, em vez de `--key-names`, você pode especificar o parâmetro `--key-pair-ids` para identificar a chave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Para visualizar o material da chave pública na saída, é necessário especificar o parâmetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemplo de saída: na saída, o campo `PublicKey` contém o material da chave pública.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Recuperar o material da chave pública

É possível usar vários métodos para obter acesso ao material da chave pública. É possível recuperar o material da chave pública usando a chave privada correspondente no computador local, usando os metadados da instância que foi iniciada com a chave pública ou ao usar o comando `describe-key-pairs` da AWS CLI. Para instâncias do Linux, o material da chave pública também pode ser recuperado do arquivo `authorized_keys` na instância.

Use um dos métodos a seguir para recuperar o material da chave pública.

Instâncias do Linux

From the private key

Para recuperar o material da chave pública na chave privada

No computador Linux ou macOS local, é possível usar o comando ssh-keygen para recuperar a chave pública de seu par de chaves. Especifique o caminho onde você fez download de sua chave privada (o arquivo `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

O comando retorna a chave pública, como mostrado no exemplo a seguir.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Se o comando falhar, execute o comando a seguir para verificar se você alterou as permissões no arquivo de par de chaves privadas de forma que somente você possa visualizá-lo.

```
chmod 400 key-pair-name.pem
```

From the instance metadata

É possível usar o serviço de metadados da instância versão 2 ou o serviço de metadados da instância versão 1 para recuperar a chave pública dos metadados da instância.

> **Note**
>
> Se você alterar o par de chaves usado para se conectar à instância, o Amazon EC2 não atualizará os metadados da instância para mostrar a nova chave pública. Os metadados da instância continuam a mostrar a chave pública do par de chaves especificado quando você iniciou a instância.

Para recuperar o material da chave pública por meio de metadados de instância

Para se conectar na instância, use um dos comandos a seguir.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Exemplo de saída

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Para obter mais informações sobre os metadados da instância, consulte Recuperar metadados da instância.

From the instance

Quando a instância é inicializada pela primeira vez, a chave pública especificada na inicialização é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`.

Para recuperar o material da chave pública de uma instância

1. Conecte-se à sua instância.
2. Na janela do terminal, abra o arquivo `authorized_keys` usando seu editor de texto favorito (como vim ou nano).

```
[ec2-user ~]$ nano ~/.ssh/authorized_keys
```

O arquivo `authorized_keys` é aberto, exibindo a chave pública seguida pelo nome do par de chaves. A seguir está uma entrada de exemplo do par de chaves chamado de *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Para recuperar o material da chave pública pelo comando **`describe-key-pairs`** da AWS CLI

Use o comando describe-key-pairs e especifique o parâmetro `--key-names` para identificar a chave pública. Para incluir o material da chave pública na saída, especifique o parâmetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemplo de saída: na saída, o campo `PublicKey` contém o material da chave pública.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
```

```
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Se preferir, em vez de `--key-names`, você pode especificar o parâmetro `--key-pair-ids` para identificar a chave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Instâncias do Windows

From the private key

Para recuperar o material da chave pública na chave privada

Em seu computador Windows local, é possível usar o PuTTYgen para obter a chave pública do seu par de chaves.

Inicie o PuTTYgen e selecione Load (Carregar). Selecione o arquivo `.ppk` ou `.pem` de chave privada. O PuTTYgen exibe a chave pública em Public key for pasting into OpenSSH authorized_keys file (Chave pública para colar no arquivo authorized_keys do OpenSSH). Também é possível visualizar a chave pública selecionando Save public key (Salvar a chave pública), especificando um nome para o arquivo, salvando-o e abrindo-o.

From the instance metadata

É possível usar o serviço de metadados da instância versão 2 ou o serviço de metadados da instância versão 1 para recuperar a chave pública dos metadados da instância.

> **Note**
>
> Se você alterar o par de chaves usado para se conectar à instância, o Amazon EC2 não atualizará os metadados da instância para mostrar a nova chave pública. Os metadados da instância continuam a mostrar a chave pública do par de chaves especificado quando você iniciou a instância.

Para recuperar o material da chave pública por meio de metadados de instância

Para se conectar na instância, use um dos comandos a seguir.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Exemplo de saída

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Para obter mais informações sobre os metadados da instância, consulte Recuperar metadados da instância.

From describe-key-pairs

Para recuperar o material da chave pública pelo comando **`describe-key-pairs`** da AWS CLI

Use o comando describe-key-pairs e especifique o parâmetro `--key-names` para identificar a chave pública. Para incluir o material da chave pública na saída, especifique o parâmetro `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemplo de saída: na saída, o campo `PublicKey` contém o material da chave pública.

```
{
```

```
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Se preferir, em vez de `--key-names`, você pode especificar o parâmetro `--key-pair-ids` para identificar a chave pública.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identifique a chave pública que foi especificada na inicialização

Se você especificar uma chave pública ao iniciar uma instância, o nome da chave pública será registrado pela instância.

Como identificar a chave pública que foi especificada na inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Detalhes, em Detalhes da instância, o campo Par de chaves atribuído no início exibe o nome da chave pública especificado quando você iniciou a instância.

> **Note**
>
> O valor do Par de chaves atribuído no início não será alterado mesmo que você altere a chave pública na instância ou adicione pares de chaves.

Excluir o par de chaves

É possível excluir um par de chaves, o que remove a chave pública armazenada no Amazon EC2. A exclusão de um par de chaves não exclui a chave privada correspondente.

Ao excluir uma chave pública usando os métodos a seguir, você só exclui a chave pública que foi armazenada no Amazon EC2 quando você criou ou importou o par de chaves. A exclusão de uma chave pública não a remove de nenhuma instância às quais você a adicionou, seja quando você iniciou a instância ou mais tarde. Também não exclui a chave privada do computador local. É possível continuar a se conectar a instâncias iniciadas usando um par de chaves excluído do Amazon EC2, desde que ainda tenha o arquivo (`.pem`) da chave privada.

> **Important**
>
> Se você estiver usando um grupo do Auto Scaling (por exemplo, em um ambiente do Elastic Beanstalk), verifique se a chave pública que você está excluindo não está especificada em um modelo de inicialização associado ou configuração de execução. Se o Amazon EC2 Auto Scaling detectar uma instância não íntegra, executará uma instância de substituição. No entanto, a inicialização da instância falhará se o par de chaves públicas não for encontrado. Para obter mais informações, consulte Modelos de execução no Manual do usuário do Amazon EC2 Auto Scaling.

Console

Exclua sua chave pública no Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione o par de chaves a ser excluído e escolha Actions (Ações), Delete (Excluir).
4. No campo de confirmação, insira `Delete` e escolha Delete (Excluir).

AWS CLI

Exclua sua chave pública no Amazon EC2

Use o comando delete-key-pair da AWS CLI.

PowerShell

Exclua sua chave pública no Amazon EC2

Use o comando Remove-EC2KeyPair da AWS Tools for Windows PowerShell.

Adição ou remoção de uma chave pública na instância do Linux

Se você perder uma chave privada, perderá o acesso a todas as instâncias que usam o par de chaves. Para obter mais informações sobre como se conectar a uma instância usando um par de chaves diferente daquele que você especificou ao iniciar a execução, consulte Eu perdi minha chave privada.

Ao iniciar uma instância, é possível especificar um par de chaves. Quando a instância é iniciada pela primeira vez, a chave pública especificada no lançamento é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`.

É possível alterar o par de chaves usado para acessar a conta de sistema padrão de sua instância adicionando uma nova chave pública na instância ou substituindo a chave pública (excluindo a chave pública existente e adicionando uma nova) na instância. Também é possível remover todas as chaves públicas de uma instância. Para adicionar ou substituir um par de chaves, conecte-se à sua instância.

É possível adicionar ou substituir um par de chaves pelos seguintes motivos:

- Se um usuário da sua organização requisitar acesso ao usuário no sistema usando um par de chaves separado, será possível adicionar a chave pública à sua instância.
- Se alguém tiver uma cópia da chave privada (arquivo `.pem`) e você quiser impedir que essa pessoa se conecte à sua instância (por exemplo, se tiver saído da organização), poderá excluir a chave pública na instância e substituí-la por uma nova.
- Se você criar uma AMI do Linux a partir de uma instância, o material da chave pública será copiado da instância para a AMI. Se você executar uma instância da AMI, a nova instância incluirá a chave pública da instância original. Para impedir que alguém com a chave privada se conecte à nova instância, remova a chave pública da instância original antes de criar a AMI.

Use os procedimentos a seguir para modificar o par de chaves para o usuário padrão, como `ec2-user`. Para obter informações sobre como adicionar usuários à sua instância, consulte a documentação do sistema operacional utilizado na instância.

Para adicionar ou substituir um par de chaves

1. Crie um par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros.
2. Recupere a chave pública do seu novo par de chaves. Para obter mais informações, consulte Recuperar o material da chave pública.
3. Conecte-se à sua instância usando sua chave privada existente.
4. Usando um editor de texto à sua escolha, abra o arquivo `.ssh/authorized_keys` na instância. Cole as informações de chave pública do seu novo par de chaves abaixo das informações de chave pública existentes. Salve o arquivo.
5. Desconecte-se da sua instância e teste se é possível se conectar à sua instância usando novo arquivo de chave privada.
6. (Opcional) Se você estiver substituindo um par de chaves existente, conecte-se à sua instância e exclua as informações de chave pública para o par de chaves original do arquivo `.ssh/authorized_keys`.

> **Important**
>
> Se estiver usando um grupo do Auto Scaling, verifique se o par de chaves que você está substituindo não está especificado em seu modelo de execução ou em sua configuração de execução. Se o Amazon EC2 Auto Scaling detectar uma instância não íntegra, executará uma instância de substituição. No entanto, o lançamento da instância falhará se o par de chaves não puder ser encontrado. Para obter mais informações, consulte Modelos de execução no Manual do usuário do Amazon EC2 Auto Scaling.

Para remover uma chave pública de uma instância

1. Conecte-se à sua instância.
2. Usando um editor de texto à sua escolha, abra o arquivo `.ssh/authorized_keys` na instância. Exclua as informações da chave pública e salve o arquivo.

> **Warning**
>
> Depois de remover todas as chaves públicas da instância e desconectar-se da instância, você não poderá se conectar a ela novamente, a menos que a AMI forneça outra maneira de fazer login.

Verificar a impressão digital do par de chaves

Para verificar a impressão digital do seu par de chaves, compare a impressão digital exibida na página Pares de chaves no console do Amazon EC2 ou a impressão digital retornada pelo comando describe-key-pairs com a impressão digital gerada usando a chave privada em seu computador local. Essas impressões digitais devem coincidir.

Quando o Amazon EC2 calcula uma impressão digital, ele pode incluir preenchimento na impressão digital com caracteres =. Outras ferramentas, como ssh-keygen, podem omitir esse preenchimento.

Se você estiver tentando verificar a impressão digital da instância do Linux do EC2 em vez da impressão digital do par de chaves, consulte Obter a impressão digital da instância.

Como as impressões digitais são calculadas

O Amazon EC2 usa diferentes funções de hash para calcular as impressões digitais de pares de chaves RSA e ED25519. Além disso, para pares de chaves RSA, o Amazon EC2 calcula as impressões digitais de maneira diferente. O serviço usa funções diferentes de hash dependendo de o par de chaves ter sido criado pelo Amazon EC2 ou importado para o Amazon EC2.

A tabela a seguir lista as funções de hash usadas para calcular as impressões digitais para pares de chaves RSA e ED25519 que são criados pelo Amazon EC2 e importados para o Amazon EC2.

(Instâncias do Linux) Funções de hash usadas para calcular impressões digitais

Fonte do par de chaves	Pares de chaves RSA (Windows e Linux)	Pares de chaves ED25519 (Linux)
Criado pelo Amazon EC2	SHA-1	SHA-256
Importado para o Amazon EC2	MD5[1]	SHA-256

[1] Se você importar uma chave RSA pública para o Amazon EC2, a impressão digital será calculada usando uma função hash MD5. Isso continua sendo verdadeiro independentemente de como você tenha criado o par de chaves. Por exemplo, usando uma ferramenta de terceiros ou gerando uma nova chave pública com base em uma chave privada existente criada usando o Amazon EC2.

Ao usar o mesmo par de chaves em regiões diferentes

Se você planeja usar o mesmo par de chaves para se conectar a instâncias em diferentes Regiões da AWS, é necessário importar a chave pública para todas as regiões nas quais você a usará. Se usar o Amazon EC2 para criar o key pair, será possível Recuperar o material da chave pública de forma que você possa importar a chave pública para as outras regiões.

> **Note**
>
> - Se você criar um par de chaves RSA usando o Amazon EC2 e gerar uma chave pública com base na chave privada do Amazon EC2, as chaves públicas importadas terão uma impressão digital diferente da chave pública original. Isso ocorre porque a impressão digital da chave RSA original criada usando o Amazon EC2 é calculada usando uma função de hash SHA-1, enquanto a impressão digital das chaves RSA importadas é calculada usando uma função de hash MD5.
> - Para pares de chaves ED25519, as impressões digitais serão as mesmas, independentemente de terem sido criadas pelo Amazon EC2 ou importadas para o Amazon EC2, porque a mesma função hash SHA-256 é usada para calcular a impressão digital.

Gerar uma impressão digital com base em uma chave privada

Use um dos seguintes comandos para gerar uma impressão digital com base na chave privada em sua máquina local.

Se estiver usando uma máquina local do Windows, poderá executar os comandos a seguir usando o Subsistema do Windows para Linux (WSL). Instale o WSL e uma distribuição do Linux usando as instruções do Guia de instalação do Windows 10. O exemplo fornecido nas instruções instala a distribuição Ubuntu do Linux, mas é possível instalar qualquer distribuição. Você é solicitado a reiniciar o computador para que as alterações sejam implementadas.

- Se tiver criado o par de chaves usando o Amazon EC2

Use as ferramentas OpenSSL para gerar uma impressão digital como apresentado nos exemplos a seguir.

Para pares de chaves do RSA:

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

(Instâncias do Linux) Para pares de chaves ED25519:

```
ssh-keygen -l -f path_to_private_key
```

- (Somente pares de chaves RSA) Se você importou a chave pública para o Amazon EC2

  Você pode seguir este procedimento independentemente de como criou o par de chaves, usando, por exemplo, uma ferramenta de terceiros ou gerando uma nova chave pública a partir de uma chave privada existente criada usando o Amazon EC2

  Use as ferramentas OpenSSL para gerar a impressão digital como apresentado no exemplo a seguir.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Se tiver criado um par de chaves OpenSSH usando o OpenSSH 7.8 ou posterior e importado a chave pública para o Amazon EC2

  Use o ssh-keygen para gerar uma impressão digital como apresentado nos exemplos a seguir.

  Para pares de chaves do RSA:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

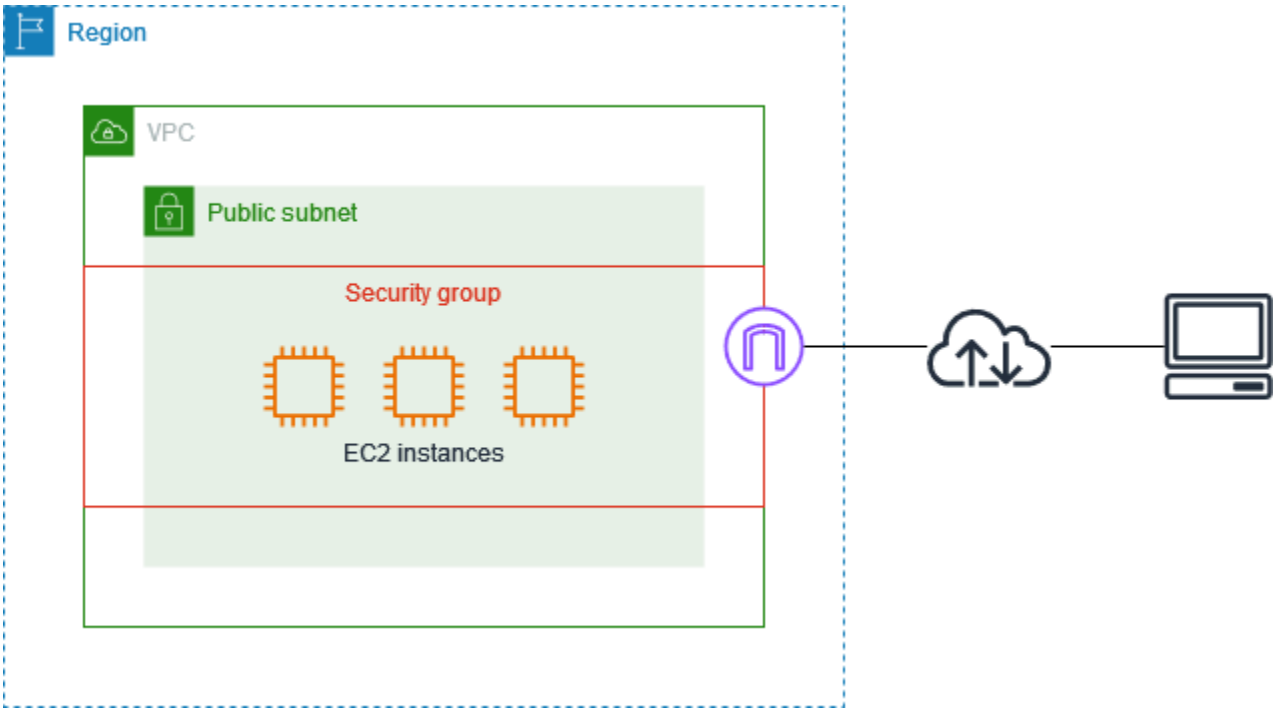
  (Instâncias do Linux) Para pares de chaves ED25519:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Grupos de segurança do Amazon EC2 para as instâncias do EC2

Um grupo de segurança atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída. As regras de entrada controlam o tráfego de entrada para a instância e as regras de saída controlam o tráfego de saída da instância. Ao executar sua instância, é possível especificar um ou mais grupos de segurança. Se você não especificar um grupo de segurança, o Amazon EC2 usará o grupo de segurança padrão para a VPC. É possível adicionar regras a cada grupo de segurança que permite tráfego de entrada ou de saída nas instâncias associadas. É possível modificar as regras de um grupo de segurança a qualquer momento. As regras novas e modificadas são aplicadas automaticamente para todas as instâncias que estão associados ao grupo de segurança. Quando o Amazon EC2 decide se deve permitir que o tráfego atinja uma instância, ele avalia todas as regras de todos os grupos de segurança associados à instância.

O diagrama a seguir mostra uma VPC com uma sub-rede, um gateway da Internet e um grupo de segurança. A sub-rede contém instâncias do EC2. O grupo de segurança está atribuído às instâncias. O único tráfego que chega à instância é aquele permitido pelas regras do grupo de segurança. Por exemplo, se o grupo de segurança contiver uma regra que permita o tráfego SSH da rede, você poderá realizar a conexão com a instância com o computador ao usar SSH. Se o grupo de segurança contiver uma regra que permita todo o tráfego dos recursos atribuídos a ele, cada instância poderá receber qualquer tráfego enviado das outras instâncias.



Depois de executar uma instância, é possível alterar seus grupos de segurança. Os grupos de segurança estão associados a interfaces de rede. A alteração dos grupos de segurança de uma instância altera os grupos de segurança associados à interface de rede primária (eth0). Para ter mais informações, consulte Para mudar o grupo de segurança de uma instância. Também é possível alterar os grupos de segurança associados a qualquer outra interface de rede. Para obter mais informações, consulte Modificar atributos da interface de rede.

A segurança é uma responsabilidade compartilhada entre a AWS e você. Para obter mais informações, consulte Segurança no Amazon EC2. A AWS fornece grupos de segurança como uma das ferramentas para proteger as instâncias, e você precisa configurá-los para atender às suas necessidades de segurança. Se houver requisitos que não sejam totalmente atendidos pelos grupos de segurança, é possível manter seu próprio firewall em qualquer uma das instâncias além de usar grupos de segurança.

Não há cobrança adicional pelo uso de grupos de segurança.

Conteúdo

- Regras de grupos de segurança
- Rastreamento de conexão do grupo de segurança
- Grupos de segurança padrão e personalizados
- Trabalhar com grupos de segurança
- Regras de grupo de segurança para diferentes casos de uso

Regras de grupos de segurança

As regras de um grupo de segurança controlam o tráfego de entrada que tem permissão para atingir as instâncias associadas ao grupo de segurança. As regras também controlam o tráfego de saída que pode deixá-los.

As seguintes são as características das regras de grupos de segurança:

- Por padrão, um grupo de segurança inclui uma regra de saída que permite todo o tráfego de saída. Você pode excluir essas funções. Observe que o Amazon EC2 bloqueia o tráfego na porta 25 por padrão. Para obter mais informações, consulte Restrição para e-mails enviados usando a porta 25.
- As regras do grupo de segurança sempre são permissivas. Você não pode criar regras que negam o acesso.

- As regras do grupo de segurança permitem filtrar o tráfego com base em protocolos e números de porta.
- Os grupos de segurança são stateful — se você enviar uma solicitação da instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de entrada do grupo de segurança. Para grupos de segurança da VPC, isso também significa que as respostas permitidas para o tráfego de entrada são permitidas para saída, independentemente das regras de saída. Para obter mais informações, consulte Rastreamento de conexão do grupo de segurança.
- É possível adicionar e remover regras a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

  O efeito de algumas alterações nas regras pode depender de como o tráfego é acompanhado. Para obter mais informações, consulte Rastreamento de conexão do grupo de segurança.
- Quando você associa vários grupos de segurança a uma instância, as regras de cada security group são efetivamente agregadas para criar um conjunto de regras. O Amazon EC2 usa esse conjunto de regras para determinar se deve permitir acesso.

  É possível atribuir vários grupos de segurança a uma instância. Portanto, uma instância pode ter centenas de regras aplicáveis. Isso pode causar problemas quando você acessar a instância. Recomendamos que você condense suas regras o máximo possível.

> **Note**
>
> Os grupos de segurança não podem bloquear solicitações de DNS de ou para o Route 53 Resolver, às vezes chamadas de “endereço IP VPC+2” (consulte O que é o Amazon Route 53 Resolver? no Guia do desenvolvedor do Amazon Route 53) ou o “AmazonProvidedDNS” (consulte Trabalhar com conjuntos de opções de DHCP no Guia do usuário do Amazon Virtual Private Cloud). Se você quiser filtrar solicitações de DNS por meio do Route 53 Resolver, é possível habilitar o Route 53 Resolver DNS Firewall (consulte Route 53 Resolver DNS Firewall no Guia do desenvolvedor do Amazon Route 53).

Para cada regra, especifique o seguinte:

- Nome: o nome do grupo de segurança (por exemplo, “meu-grupo-de-segurança”).

  Esse nome pode ter até 255 caracteres. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=;{}!$*. Quando o nome contém espaços finais, cortamos os espaços ao salvá-lo. Por

exemplo, se você inserir “Testar grupo de segurança " para o nome, nós o armazenaremos como “Testar grupo de segurança”.

- Protocolo: o protocolo a permitir. Os protocolos mais comuns são 6 (TCP), 17 (UDP) e 1 (ICMP).
- Intervalo de portas: para TCP, UDP ou um protocolo personalizado, o intervalo de portas a ser permitido. É possível especificar um único número de porta (por exemplo, 22) ou um intervalo de números de portas (por exemplo, `7000-8000`).
- Tipo e código do ICMP: para o ICMP, o tipo e o código do ICMP. Por exemplo, use o tipo 8 para solicitação de eco ICMP ou digite 128 para solicitação de eco ICMPv6.
- Origem ou destino: a origem (regras de entrada) ou o destino (regras de saída) para permitir o tráfego. Especifique um dos seguintes:
  - Um endereço IPv4 único. Use o comprimento de prefixo `/32`. Por exemplo, `203.0.113.1/32`.
  - Um endereço IPv6 único. Use o comprimento de prefixo `/128`. Por exemplo, `2001:db8:1234:1a00::123/128`.
  - Um intervalo de endereços IPv4, em notação de bloco CIDR. Por exemplo, `203.0.113.0/24`.
  - Um intervalo de endereços IPv6, em notação de bloco CIDR. Por exemplo, `2001:db8:1234:1a00::/64`.
  - O ID de uma lista de prefixos. Por exemplo, `pl-1234abc1234abc123`. Para obter mais informações, consulte Listas de prefixos no Guia do usuário da Amazon VPC.
  - O ID de um grupo de segurança (referido aqui como grupo de segurança especificado). Por exemplo, o grupo de segurança atual, um grupo de segurança da mesma VPC ou um grupo de segurança para uma VPC emparelhada. Isso permite o tráfego com base nos endereços IP privados dos recursos associados ao grupo de segurança especificado. Isso não adiciona regras do grupo de segurança especificado a esse grupo de segurança.
- (Opcional) Descrição: é possível adicionar uma descrição à regra, que pode ajudá-lo a identificá-la posteriormente. Uma descrição pode ser até 255 caracteres de comprimento. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=;{}!$*.

Quando você cria uma regra para o grupo de segurança, a AWS atribui um ID exclusivo à regra. É possível usar o ID de uma regra ao usar a API ou a CLI para modificar ou excluir a regra.

Quando você especifica um grupo de segurança como a origem ou o destino de uma regra, a regra afeta todas as instâncias associadas ao grupo de segurança. O tráfego de entrada é permitido com base nos endereços IP privados das instâncias associadas ao grupo de segurança de origem (e não aos endereços IP público ou IP elástico). Para obter mais informações sobre endereços IP, consulte

Endereçamento IP de instâncias do Amazon EC2. Se a sua regra de grupo de segurança referenciar um grupo de segurança excluído na mesma VPC ou em uma VPC par, ou se ela referenciar um grupo de segurança em uma VPC par em que a conexão de emparelhamento da VPC tenha sido excluída, a regra será marcada como obsoleta. Para obter mais informações, consulte Como trabalhar com regras de grupos de segurança obsoletas no Amazon VPC Peering Guide.

Se houver mais de uma regra para uma porta específica, o Amazon EC2 aplicará a regra mais permissiva. Por exemplo, se você tiver uma regra que permite o acesso à porta TCP 22 (SSH) do endereço IP 203.0.113.1, e outra regra que permite o acesso à porta TCP 22 para todos, então todos terão acesso à porta TCP 22.

Quando você adiciona, atualiza ou remove regras, elas são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

Rastreamento de conexão do grupo de segurança

Os grupos de segurança usam o acompanhamento da conexão para acompanhar as informações sobre o tráfego de entrada e saída da instância. As regras são aplicadas com base no estado da conexão do tráfego para determinar se o tráfego é permitido ou negado. Com essa abordagem, os grupos de segurança são tipo com estado. Isso significa que as respostas ao tráfego de entrada têm permissão para sair da instância independentemente das regras do grupo de segurança de saída e vice-versa.

Por exemplo, suponha que você inicie um comando como netcat ou similar para instâncias de seu computador doméstico, e as regras de grupo de segurança de entrada permitam tráfego ICMP. As informações sobre a conexão (inclusive as informações da porta) são rastreadas. O tráfego de resposta da instância para o comando não é monitorado como uma nova solicitação, mas sim como uma conexão estabelecida e tem permissão para sair da instância, mesmo que as regras de seu grupo de segurança restrinjam o tráfego de saída ICMP.

Para protocolos diferentes de TCP, UDP ou ICMP, somente o endereço IP e o número do protocolo são acompanhados. Se a instância enviar tráfego para outro host e esse host iniciar o mesmo tipo de tráfego para a instância em 600 segundos, o grupo de segurança para a instância o aceitará independentemente das regras de entrada do grupo de segurança. O grupo de segurança aceitará isso, pois será considerado como tráfego de resposta para o tráfego original.

Quando você altera uma regra do grupo de segurança, suas conexões monitoradas não são imediatamente interrompidas. O grupo de segurança continua a permitir pacotes até o tempo limite das conexões existentes. Para garantir que o tráfego seja interrompido imediatamente, ou que todo

o tráfego esteja sujeito às regras do firewall, independentemente do estado de monitoramento, será possível usar uma Network ACL para a sub-rede. As Network ACLs são stateless e, portanto, não permitem automaticamente o tráfego de resposta. A adição de uma ACL de rede que bloqueia o tráfego em qualquer direção quebra as conexões existentes. Para obter mais informações, consulte Network ACLs no Guia do usuário da Amazon VPC.

> **Note**
>
> Os grupos de segurança não têm efeito sobre o tráfego de DNS de ou para o Route 53 Resolver, às vezes chamadas de "endereço IP VPC+2" (consulte O que é o Amazon Route 53 Resolver? no Guia do desenvolvedor do Amazon Route 53) ou o "AmazonProvidedDNS" (consulte Trabalhar com conjuntos de opções de DHCP no Guia do usuário do Amazon Virtual Private Cloud). Se você quiser filtrar solicitações de DNS por meio do Route 53 Resolver, é possível habilitar o Route 53 Resolver DNS Firewall (consulte Route 53 Resolver DNS Firewall no Guia do desenvolvedor do Amazon Route 53).

Conexões não rastreadas

Nem todos os fluxos de tráfego são acompanhados. Se uma regra do grupo de segurança permitir fluxos TCP ou UDP para todo o tráfego (0.0.0.0/0 ou ::/0) e houver uma regra correspondente na outra direção que permita todo o tráfego de resposta (0.0.0.0/0 ou ::/0) para qualquer porta (0-65535), esse fluxo de tráfego não será monitorado, a menos que faça parte de uma conexão monitorada automaticamente. O tráfego de resposta para um fluxo não monitorado é permitido com base na regra de entrada ou de saída que permite o tráfego de resposta, e não é baseado nas informações de monitoramento.

Um fluxo de tráfego não acompanhado será interrompido imediatamente se a regra que permite o fluxo for removida ou alterada. Por exemplo, se você tiver uma regra de saída aberta (0.0.0.0/0) e remover uma regra que permita todo tráfego (porta TCP 22) SSH de entrada (0.0.0.0/0) para a instância (ou modificá-la de forma que a conexão não seja mais permitida), suas conexões SSH existentes na instância serão imediatamente descartadas. A conexão não estava sendo rastreada anteriormente, então a alteração interromperá a conexão. Por outro lado, se você tiver uma regra de entrada mais restrita que inicialmente permita uma conexão SSH (o que significa que a conexão foi monitorada), mas altere essa regra para não permitir mais novas conexões do endereço do cliente SSH atual, a conexão existente não será interrompida pela alteração da regra.

Conexões rastreadas automaticamente

As conexões feitas a seguir são monitoradas automaticamente, mesmo que a configuração do grupo de segurança não exija monitoramento:

- Gateways da Internet apenas de saída
- Aceleradoras do Global Accelerator
- Gateways NAT
- Endpoints do Network Firewall
- Network Load Balancers
- AWS PrivateLink (endpoints da VPC de interface)
- AWS Lambda (Interfaces de rede elástica hiperplanas)

Subsídios para monitoramento de conexão

O Amazon EC2 define um número máximo de conexões que podem ser rastreadas por instância. Depois que o máximo é atingido, todos os pacotes enviados ou recebidos são descartados, porque não é possível estabelecer uma nova conexão. Quando isso acontece, as aplicações que enviam e recebem pacotes não podem se comunicar corretamente. Use a métrica de desempenho da rede `conntrack_allowance_available` para determinar o número de conexões rastreadas ainda disponíveis para esse tipo de instância.

Para determinar se os pacotes foram descartados porque o tráfego de rede para sua instância excedeu o número máximo de conexões que podem ser rastreadas, use a métrica `conntrack_allowance_exceeded` de performance de rede. Para ter mais informações, consulte Monitorar a performance de rede de sua instância do EC2.

Com o Elastic Load Balancing, se você exceder o número máximo de conexões que podem ser rastreadas por instância, recomendamos que escale o número de instâncias registradas com o balanceador de carga ou o tamanho das instâncias registradas com o balanceador de carga.

Considerações sobre a performance do monitoramento de conexão

O roteamento assimétrico, em que o tráfego entra em uma instância por meio de uma interface de rede e sai por meio de uma interface de rede diferente, pode reduzir a performance máxima que uma instância poderá alcançar se os fluxos forem rastreados.

Para manter a performance máxima quando o monitoramento de conexão estiver habilitado para os grupos de segurança, recomendamos a seguinte configuração:

- Evite topologias de roteamento assimétrico, se possível.
- Em vez de usar grupos de segurança para filtragem, use ACLs de rede.
- Se você precisar usar grupos de segurança com rastreamento de conexão, configure o menor tempo limite de conexão possível.

Para obter mais informações sobre a performance do ajuste no sistema Nitro, consulte Considerações sobre o Nitro System para ajuste de performance.

Tempo limite de rastreamento de conexão ociosa

O grupo de segurança monitora cada conexão estabelecida para garantir que os pacotes de retorno sejam entregues como esperado. Há um número máximo de conexões que podem ser rastreadas por instância. As conexões que permanecem ociosas podem levar à exaustão do rastreamento da conexão e fazer com que as conexões não sejam rastreadas e os pacotes sejam descartados. Você pode definir o tempo limite de rastreamento de conexões em uma interface de rede do Elastic.

> **Note**
>
> Esse recurso está disponível somente para instâncias desenvolvidas no AWS Nitro System.

Há três tempos limite configuráveis:

- Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido. Mín: 60 segundos. Máx: 432.000 segundos (5 dias) Padrão: 432.000 segundos. Recomendado: menos de 432.000 segundos.
- Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta. Mín: 30 segundos. Máx: 60 segundos. Padrão: 30 segundos.
- Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta. Mín: 60 segundos. Máx: 180 segundos (3 minutos). Padrão: 180 segundos.

Talvez você queira modificar os tempos limite padrão para algum dos seguintes casos:

- Se você estiver monitorando conexões rastreadas usando as métricas de performance de rede do Amazon EC2, as métricas conntrack_allowance_exceeded e conntrack_allowance_available permitem monitorar os pacotes descartados e a utilização da conexão rastreada para gerenciar proativamente a capacidade da instância do EC2 com ações de aumento ou redução de escala para ajudar a atender à demanda de conexões de rede antes de descartar pacotes. Se você estiver observando quedas de conntrack_allowance_exceeded nas instâncias do EC2, pode ser benéfico definir um tempo limite de TCP estabelecido mais baixo para levar em conta sessões TCP/UDP paralisadas devido a clientes ou caixas intermediárias de rede inadequados.
- Normalmente, os balanceadores de carga ou os firewalls têm um tempo limite de ociosidade de TCP estabelecido na faixa de 60 a 90 minutos. Se você estiver executando workloads que devem lidar com um número muito alto de conexões (mais de 100 mil) de dispositivos como firewalls de rede, é recomendável configurar um tempo limite semelhante em uma interface de rede do EC2.
- Se você estiver executando uma workload que utiliza uma topologia de roteamento assimétrico, recomendamos que você configure um tempo limite de inatividade estabelecido por TCP de 60 segundos.
- Se você estiver executando workloads com um grande número de conexões, como DNS, SIP, SNMP, Syslog, Radius e outros serviços que usam principalmente UDP para atender a solicitações, definir o tempo limite do ‘fluxo UDP’ como 60 segundos proporciona maior escala/performance para a capacidade existente e evita falhas cinzentas.
- Para conexões TCP/UDP por meio de network load balancers (NLBs) e elastic load balancing (ELB), todas as conexões são rastreadas. O valor do tempo limite de ociosidade para fluxos TCP é de 350 segundos e para fluxos UDP é de 120 segundos e difere dos valores de tempo limite do nível da interface. Talvez você queira configurar tempos limite no nível da interface de rede para permitir maior flexibilidade de tempo limite do que os padrões para ELB/NLB.

Você tem a opção de configurar os tempos limite de rastreamento de conexão ao fazer o seguinte:

- Criar uma interface de rede
- Modificar atributos da interface de rede
- Iniciar uma instância do EC2
- Criar um modelo de inicialização de instância do EC2

Exemplo

No exemplo a seguir, o grupo de segurança tem regras de entrada específicas para tráfego TCP e ICMP, e uma regra de saída que permite todo o tráfego de saída.

Entrada

Tipo de protocolo	Número da porta	Origem
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Todos	0.0.0.0/0

Saída

Tipo de protocolo	Número da porta	Destination (Destino)
Todos	Tudo	0.0.0.0/0
Tudo	Tudo	::/0

Com uma conexão de rede direta com a instância ou interface de rede, o comportamento de rastreamento é o seguinte:

- O tráfego TCP de entrada e saída na porta 22 (SSH) é monitorado porque a regra de entrada permite o tráfego somente de 203.0.113.1/32, e não de todos os endereços IP (0.0.0.0/0).
- O tráfego TCP de entrada e de saída na porta 80 (HTTP) não é monitorado porque as regras de entrada e saída permitem o tráfego de todos os endereços IP.
- O tráfego ICMP é sempre monitorado.

Se você remover a regra de saída para o tráfego IPv4, todo o tráfego IPv4 de entrada e saída será monitorado, incluindo o tráfego na porta 80 (HTTP). O mesmo se aplica ao tráfego IPv6 se você remover a regra de saída para o tráfego IPv6.

Grupos de segurança padrão e personalizados

Sua conta da AWS tem automaticamente um grupo de segurança padrão para a VPC padrão em cada região. Se você não especificar um grupo de segurança ao executar uma instância, ela será associada automaticamente ao grupo de segurança padrão da VPC. Se não quiser que suas instâncias usem o grupo de segurança padrão, será possível criar seus próprios grupos de segurança personalizados e especificá-los quando executar as instâncias.

Conteúdo

- Grupos de segurança padrão
- Os grupos de segurança personalizados

Grupos de segurança padrão

Sua VPC é fornecida com um grupo de segurança padrão. Recomendamos que criar grupos de segurança para instâncias ou grupos de instâncias específicos em vez de usar o grupo de segurança padrão. No entanto, se você não especificar um grupo de segurança ao iniciar uma instância, associaremos a instância ao grupo de segurança padrão para a VPC.

O nome de um grupo de segurança padrão é “default“. Veja a seguir as regras padrão para um grupo de segurança padrão.

Entrada

Origem	Protocolo	Intervalo de portas	Descrição
sg-1234567890abcdef0	Todos	Todos	Permite tráfego de entrada de todos os recursos atribuídos a este grupo de segurança. A origem é o ID deste grupo de segurança.

Saída

Destino	Protocolo	Intervalo de portas	Descrição
0.0.0.0/0	Tudo	Tudo	Permite todo o tráfego IPv4 de saída.

Destino	Protocolo	Intervalo de portas	Descrição
::/0	Tudo	Tudo	Permite todo o tráfego IPv6 de saída. Essa regra será adicionada somente se sua VPC tiver um bloco CIDR IPv6 associado.

Noções básicas do grupo de segurança padrão

- Você pode alterar as regras do grupo de segurança padrão.
- Você não pode excluir um grupo de segurança padrão. Se você tentar excluir um grupo de segurança padrão, retornaremos o seguinte código de erro: `Client.CannotDelete`.

Os grupos de segurança personalizados

É possível criar vários grupos de segurança para refletir as diferentes funções que suas instâncias desempenham. Por exemplo, servidores Web ou servidores de banco de dados.

Ao criar um grupo de segurança, forneça um nome e uma descrição. Os nomes e as descrições de grupos de segurança podem ter até 255 caracteres de comprimento e são limitados aos seguintes caracteres:

a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=&;{}!$*

Um nome de grupo de segurança não pode começar com a seguinte sequência: sg-. Um nome do grupo de segurança deve ser exclusivo da VPC.

As seguintes são as regras padrão para um grupo de segurança que você cria:

- Não permite nenhum tráfego de entrada
- Permite todo o tráfego de saída

Depois de criar um grupo de segurança, é possível alterar as regras de entrada para refletir o tipo de tráfego de entrada que você quer para atingir as instâncias associadas. Também é possível alterar as regras de saída.

Para obter mais informações sobre as regras que é possível adicionar a um grupo de segurança, consulte Regras de grupo de segurança para diferentes casos de uso.

Trabalhar com grupos de segurança

É possível atribuir um security group a uma instância ao executá-la. Quando você adiciona ou remove regras, essas alterações são aplicadas automaticamente a todas as instâncias às quais você atribuiu o security group. Para obter mais informações, consulte Atribuir um grupo de segurança a uma instância.

Depois de executar uma instância, é possível alterar seus grupos de segurança. Para obter mais informações, consulte Para mudar o grupo de segurança de uma instância.

É possível criar, visualizar, atualizar e excluir grupos de segurança e regras de grupos de segurança usando o console do Amazon EC2 e as ferramentas da linha de comando.

Tarefas

- Crie um grupo de segurança
- Copiar um grupo de segurança
- Visualizar seus grupos de segurança
- Adicionar regras a um grupo de segurança
- Atualizar regras do grupo de segurança
- Excluir regras de um grupo de segurança
- Excluir um grupo de segurança
- Atribuir um grupo de segurança a uma instância
- Para mudar o grupo de segurança de uma instância

Crie um grupo de segurança

Embora você possa usar o grupo de segurança padrão para suas instâncias, é possível criar seus próprios grupos para refletir as diferentes funções que as instâncias desempenham no seu sistema.

Por padrão, novos grupos de segurança começam com apenas uma regra de saída que permite que todo o tráfego deixe as instâncias. Adicione regras para permitir qualquer tráfego de entrada ou para restringir o tráfego de saída.

Um grupo de segurança só pode ser usado na VPC na qual ele é criado.

Console

Para criar um security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Create security group (Criar grupo de segurança).
4. Na seção Basic details (Detalhes básicos) faça o seguinte.
   a. Insira um nome descritivo e uma breve descrição para o grupo de segurança. Eles não podem ser editados depois que o grupo de segurança é criado. O nome e a descrição podem ter até 255 caracteres. Os caracteres válidos são a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=&;{}!$*.
   b. Em VPC, escolha a VPC.
5. É possível adicionar regras do grupo de segurança agora ou pode adicioná-las mais tarde. Para obter mais informações, consulte Adicionar regras a um grupo de segurança.
6. É possível adicionar etiquetas agora ou pode adicioná-las mais tarde. Para adicionar uma tag, escolha Add new tag, e insira a chave e o valor da tag.
7. Escolha Create grupo de segurança.

Command line

Como criar um grupo de segurança

Use um dos seguintes comandos:

- create-security-group (AWS CLI)
- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Copiar um grupo de segurança

É possível criar um grupo de segurança com a cópia de um grupo existente. Ao copiar um grupo de segurança, a cópia tem as mesmas regras de entrada e saída que o grupo de segurança original. Se o grupo de segurança original estiver em uma VPC, a cópia será criada na mesma VPC, a menos que você especifique uma diferente.

A cópia receberá um novo ID de grupo de segurança exclusivo e você deverá fornecer um nome a ela. Também é possível adicionar uma descrição.

Não é possível copiar um grupo de segurança de uma região para outra região.

É possível criar uma cópia do grupo de segurança usando o console do Amazon EC2.

Para copiar um security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança a ser copiado e escolha Actions (Ações), Copy to new security group (Copiar para novo grupo de segurança).
4. Especifique um nome e uma descrição opcional e altere as regras da VPC e do grupo de segurança, se necessário.
5. Escolha Criar.

Visualizar seus grupos de segurança

É possível visualizar informações sobre seus grupos de segurança usando um dos seguintes métodos.

Console

Como visualizar seus grupos de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Seus grupos de segurança serão listados. Para visualizar os detalhes de um grupo de segurança específico, incluindo suas regras de entrada e saída, escolha seu ID na coluna Security group ID (ID do grupo de segurança).

Command line

Como visualizar seus grupos de segurança

Use um dos seguintes comandos.

- describe-security-groups (AWS CLI)

- describe-security-group-rules (AWS CLI)
- Get-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

É possível usar o Amazon EC2 Global View para visualizar seus grupos de segurança em todas as regiões para as quais sua conta AWS está habilitada. Para ter mais informações, consulte Amazon EC2 Global View.

Adicionar regras a um grupo de segurança

Quando você adiciona uma regra a um grupo de segurança, a nova regra é aplicada automaticamente a todas as instâncias associadas ao grupo de segurança. Pode haver um pequeno atraso antes de a regra ser aplicada. Para ter mais informações, consulte Regras de grupo de segurança para diferentes casos de uso e Regras de grupos de segurança.

Console

Como adicionar uma regra de entrada a um grupo de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha o grupo de segurança e selecione Actions(Ações), Edit inbound rules.(Editar regras de entrada).
4. Para cada regra, selecione Add Rule (Adicionar regra) e faça o seguinte.
   a. Em Type (Tipo), escolha o tipo de protocolo a ser permitido.
      - Para TCP personalizado ou UDP personalizado, é necessário inserir o intervalo de portas que será permitido. Por exemplo, `0-99`.
      - Para ICMP personalizado, você deverá escolher o tipo ICMP em Protocolo. O intervalo de portas será configurado para você. Por exemplo, para permitir comandos ping, escolha Solicitação eco de Protocolo.
      - Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.
   b. Em Source, (Origem), siga um dos procedimentos a seguir para permitir tráfego.

- Escolha Custom (Personalizado) e insira um endereço IP na notação CIDR, um bloco CIDR, outro grupo de segurança ou uma lista de prefixos.
- Escolha Anywhere (Qualquer lugar) para permitir que todo o tráfego de entrada do protocolo especificado alcance sua instância. Essa opção adiciona automaticamente o bloco CIDR IPv4 0.0.0.0/0 como origem. Se o grupo de segurança estiver em uma VPC habilitada para IPv6, essa opção adicionará automaticamente uma regra para o bloco CIDR IPv6 ::/0.

> **Warning**
>
> Se escolher Anywhere (Qualquer lugar), você habilitará todos os endereços IPv4 e IPv6 para acessar o protocolo especificado da instância. Se você adicionar regras para as portas 22 (SSH) ou 3389 (RDP), deverá autorizar somente um endereço IP específico ou um intervalo de endereços para acessar a instância.

- Escolha My IP (Meu IP) para permitir o tráfego de entrada somente do endereço IPv4 público do computador local.

c. Em Description (Descrição), é possível especificar uma descrição para a regra.

5. Selecione Visualizar alterações, Salvar regras.

Como adicionar uma regra de saída a um grupo de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída).
4. Para cada regra, selecione Add Rule (Adicionar regra) e faça o seguinte.

   a. Em Type (Tipo), escolha o tipo de protocolo a ser permitido.

   - Para TCP personalizado ou UDP personalizado, é necessário inserir o intervalo de portas que será permitido. Por exemplo, `0-99`.
   - Para ICMP personalizado, você deverá escolher o tipo ICMP em Protocolo. O intervalo de portas será configurado para você.

- Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados automaticamente.

b. Em Destination (Destino), siga um dos procedimentos a seguir:

- Escolha Personalizado e insira um endereço IP na notação CIDR, um bloco CIDR, outro grupo de segurança ou uma lista de prefixos para o qual permitir o tráfego de saída.
- Escolha Anywhere (Qualquer lugar) para permitir o tráfego de saída para todos os endereços IP. Esta opção adiciona automaticamente o bloco CIDR IPv4 0.0.0.0/0 como destino.

  Se o grupo de segurança estiver em uma VPC habilitada para IPv6, essa opção adicionará automaticamente uma regra para o bloco CIDR IPv6 ::/0.
- Escolha My IP (Meu IP) para permitir o tráfego de saída somente do endereço IPv4 público do computador local.

c. (Opcional) Em Description (Descrição), especifique uma breve descrição para a regra.

5. Escolha Preview changes (Visualizar alterações), Confirm (Confirmar).

Command line

Para adicionar regras a um security group

Use um dos seguintes comandos.

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Como adicionar uma ou mais regras de saída a um grupo de segurança

Use um dos seguintes comandos.

- authorize-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Atualizar regras do grupo de segurança

É possível atualizar uma regra de grupo de segurança usando um dos seguintes métodos. A regra atualizada é aplicada automaticamente a todas as instâncias associadas ao grupo de segurança.

Console

Quando você modifica o protocolo, o intervalo de portas ou a origem ou o destino de um security group existente usando o console, o console exclui a regra existente e adiciona uma nova para você.

Como atualizar uma regra de grupo de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o security group.
4. Escolha Actions (Ações) e Edit inbound rules (Editar regras de entrada) para atualizar uma regra para tráfego de entrada, ou Actions (Ações) e Edit outbound rules (Editar regras de saída) para atualizar uma regra para tráfego de saída.
5. Atualize a regra conforme necessário.
6. Escolha Preview changes (Visualizar alterações), Confirm (Confirmar).

Para etiquetar uma regra do grupo de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança.
4. Na guia Inbound rules (Regras de entrada) ou Outbound rules (Regras de saída), marque a caixa de seleção da regra e escolha Manage tags (Gerenciar tags).
5. A seção Manage tags (Gerenciar tags) exibe todas as tags atribuídas à regra. Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. Para excluir uma tag, escolha Remove (Remover) ao lado da tag que você deseja excluir.
6. Escolha Salvar alterações.

Command line

Não é possível modificar o protocolo, o intervalo de portas ou a origem ou o destino de uma regra existente usando a API do Amazon EC2 ou uma ferramenta da linha de comando. Em vez disso, exclua a regra existente e adicionar uma regra nova. No entanto, é possível atualizar a descrição de uma regra existente.

Para atualizar uma regra

Use um dos comandos a seguir.

- modify-security-group-rules (AWS CLI)

Como atualizar a descrição de uma regra de entrada existente

Use um dos seguintes comandos.

- update-security-group-rule-descriptions-ingress (AWS CLI)
- Update-EC2SecurityGroupRuleIngressDescription (AWS Tools for Windows PowerShell)

Como atualizar a descrição de uma regra de saída existente

Use um dos seguintes comandos.

- update-security-group-rule-descriptions-egress (AWS CLI)
- Update-EC2SecurityGroupRuleEgressDescription (AWS Tools for Windows PowerShell)

Para etiquetar uma regra do grupo de segurança

Use um dos seguintes comandos.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Excluir regras de um grupo de segurança

Quando você excluir uma regra de um security group, a alteração é aplicada automaticamente a todas as instâncias associadas ao grupo de segurança.

É possível excluir regras de um grupo de segurança usando um dos métodos a seguir.

Console

Para excluir uma regra de security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança a ser atualizado, escolha Actions (Ações) e Edit inbound rules (Editar regras de entrada) para remover uma regra de entrada ou Edit outbound rules (Editar regras de saída) para remover uma regra de saída.
4. Escolha o botão Delete (Excluir) à direita da regra que será excluída.
5. Escolha Salvar regras. Como alternativa, escolha Visualizar alterações, analise suas alterações e escolha Confirmar.

Command line

Como remover uma ou mais regras de entrada de um grupo de segurança

Use um dos seguintes comandos.

- revoke-security-group-ingress (AWS CLI)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Como remover uma ou mais regras de saída de um grupo de segurança

Use um dos seguintes comandos.

- revoke-security-group-egress (AWS CLI)
- Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Excluir um grupo de segurança

Você não pode excluir um grupo de segurança que esteja associado a uma instância. Você não pode excluir o grupo de segurança padrão. Você não pode excluir um grupo de segurança referenciado por uma regra em outro grupo de segurança na mesma VPC. Se o grupo de segurança for referenciado por uma de suas próprias regras, exclua a regra para poder excluir o grupo de segurança.

Console

Para excluir um security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança e escolha Ações, Excluir grupos de segurança.
4. Quando a confirmação for solicitada, escolha Excluir.

Command line

Para excluir um security group

Use um dos seguintes comandos.

- delete-security-group (AWS CLI)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Atribuir um grupo de segurança a uma instância

É possível atribuir um ou mais grupos de segurança a uma instância quando executá-la. Também é possível especificar um ou mais grupos de segurança em um modelo de execução. Os grupos de segurança são atribuídos a todas as instâncias que são executadas usando o modelo de execução.

- Para atribuir um grupo de segurança a uma instância ao iniciá-la, consulte Configurações de rede de Iniciar uma instância usando parâmetros definidos (novo console) ou Etapa 6: configurar o grupo de segurança (console antigo).
- Para especificar um grupo de segurança em um modelo de inicialização, consulte Configurações de rede de Criar um modelo de execução usando parâmetros.

Para mudar o grupo de segurança de uma instância

Depois de executar uma instância, é possível mudar os grupos de segurança dela adicionando ou removendo grupos de segurança.

Requisitos

- A instância deve estar no estado `running` ou `stopped`.

- Um grupo de segurança é específico de uma VPC. Você pode atribuir um grupo de segurança a uma ou mais instâncias lançadas na VPC para a qual o grupo de segurança foi criado.

Console

Para modificar os grupos de segurança de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, em seguida, escolha Actions (Ações), Security (Segurança), Change security groups (Alterar grupos de segurança).
4. Em Associated security groups (Grupos de segurança associados), selecione um grupo de segurança na lista e escolha Add security group (Adicionar grupo de segurança).

   Para remover um grupo de segurança já associado, escolha Remove (Remover) para esse grupo de segurança.
5. Escolha Salvar.

Command line

Para modificar os grupos de segurança de uma instância

Use um dos seguintes comandos.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Regras de grupo de segurança para diferentes casos de uso

É possível criar um grupo de segurança e adicionar regras que reflitam a função da instância associada ao grupo de segurança. Por exemplo, uma instância configurada como servidor Web precisa de regras de grupo de segurança que permitam acesso HTTP e HTTPS de entrada. Da mesma forma, uma instância de banco de dados precisa de regras que permitam o acesso para o tipo de banco de dados, como acesso pela porta 3306 para MySQL.

Os seguintes são exemplos de tipos de regras que é possível adicionar aos grupos de segurança para tipos específicos de acesso.

Exemplos

- Regras do servidor da Web
- Regras do servidor de banco de dados
- Regras para se conectar a instâncias pelo computador
- Regras para se conectar a instâncias por uma instâncias com o mesmo grupo de segurança
- Regras de ping/ICMP
- Regras do servidor DNS
- Regras do Amazon EFS
- Regras do Elastic Load Balancing
- Regras de emparelhamento de VPC

Regras do servidor da Web

As seguintes regras de entrada permitem acesso HTTP e HTTPS de qualquer endereço IP. Se a VPC estiver habilitada para IPv6, será possível adicionar regras para controlar o tráfego de entrada HTTP e HTTPS em endereços IPv6.

Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de entrada em qualquer endereço IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de entrada em qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	Permite acesso HTTP de entrada em qualquer endereço IPv6
TCP	6	443 (HTTPS)	::/0	Permite acesso HTTPS de entrada em qualquer endereço IPv6

Regras do servidor de banco de dados

As seguintes regras de entrada são exemplos de regras que é possível adicionar para acesso ao banco de dados, dependendo do tipo de banco de dados que você está executando na instância. Para obter mais informações sobre instâncias do Amazon RDS, consulte o Manual do usuário do Amazon RDS.

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP específico ou um intervalo de endereços IP (na notação de bloco CIDR) em sua rede local
- Um ID de grupo de segurança para um grupo de instâncias que acessa o banco de dados

Tipo de protocolo	Número do protocolo	Porta	Observações
TCP	6	1433 (MS SQL)	A porta padrão para acessar um banco de dados Microsoft SQL Server, por exemplo, em uma instância do Amazon RDS
TCP	6	3306 (MYSQL/Aurora)	A porta padrão para acessar um banco de dados MySQL ou Aurora, por exemplo, em uma instância do Amazon RDS
TCP	6	5439 (Redshift)	A porta padrão para acessar um banco de dados de cluster do Amazon Redshift.
TCP	6	5432 (PostgreSQL)	A porta padrão para acessar um banco de dados PostgreSQL, por exemplo, em uma instância do Amazon RDS
TCP	6	1521 (Oracle)	A porta padrão para acessar um banco de dados Oracle, por exemplo, em uma instância do Amazon RDS

Também é possível restringir o tráfego de saída de seus servidores de banco de dados. Por exemplo, talvez você queira permitir o acesso à Internet para atualizações de software, mas restringir todos os outros tipos de tráfego. Primeiro, remova a regra de saída padrão que permite todo o tráfego de saída.

Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de saída a qualquer endereço IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de saída a qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTP a qualquer endereço IPv6
TCP	6	443 (HTTPS)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTPS a qualquer endereço IPv6

Regras para se conectar a instâncias pelo computador

Para se conectar à instância, seu grupo de segurança deve ter regras de entrada que permitam acesso SSH (para instâncias do Linux) ou acesso RDP (para instâncias do Windows).

Tipo de protocolo	Número do protocolo	Porta	IP de origem
TCP	6	22 (SSH)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a

Tipo de protocolo	Número do protocolo	Porta	IP de origem
			VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, será possível digitar um endereço IPv6 ou um intervalo.
TCP	6	3389 (RDP)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, será possível digitar um endereço IPv6 ou um intervalo.

Regras para se conectar a instâncias por uma instâncias com o mesmo grupo de segurança

Para permitir que as instâncias associadas ao mesmo grupo de segurança se comuniquem entre si, adicione regras explícitas para isso.

> **Note**
>
> Se você configurar rotas para encaminhar o tráfego entre duas instâncias em sub-redes diferentes por meio de um dispositivo middlebox, deverá garantir que os grupos de segurança de ambas as instâncias permitam o fluxo de tráfego entre as instâncias. O grupo de segurança para cada instância deve fazer referência ao endereço IP privado da outra instância ou ao intervalo CIDR da sub-rede que contém a outra instância, como a origem. Se você fizer referência ao grupo de segurança da outra instância como a origem, isso não permitirá que o tráfego flua entre as instâncias.

A tabela a seguir descreve a regra de entrada para um grupo de segurança que permite que as instâncias associadas se comuniquem entre si. A regra permite todos os tipos de tráfego.

Tipo de protocolo	Número do protocolo	Portas	IP de origem
-1 (todos)	-1 (todos)	-1 (todos)	O ID do grupo de segurança ou o intervalo CIDR da sub-rede que contém a outra instância (consulte a observação).

Regras de ping/ICMP

O comando ping é um tipo de tráfego ICMP. Para emitir um ping para a instância,você deve adicionar uma das seguintes regras de entrada ICMP.

Tipo	Protocolo	Origem		
ICMP personalizado: IPv4	Solicitação de eco	O endereço IPv4 público do computador, um endereço IPv4 específico ou um endereço IPv4 ou IPv6 de qualquer lugar.		
Todos os ICMP - IPv4	ICMP IPv4 (1)	O endereço IPv4 público do computador, um endereço IPv4 específico ou um endereço IPv4 ou IPv6 de qualquer lugar.		

Para usar o comando ping6 para fazer ping no endereço IPv6 da instância, adicione a seguinte regra ICMPv6 de entrada.

Tipo	Protocolo	Origem		
Todos os ICMP: IPv6	ICMP Pv6 (58)	O endereço IPv6 do computador, um endereço IPv4 específico ou um endereço IPv4 ou IPv6 de qualquer lugar.		

Regras do servidor DNS

Se tiver configurado a instância do EC2 como um servidor DNS, você deverá garantir que o tráfego TCP e UDP possa atingir seu servidor DNS pela porta 53.

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP ou um intervalo de endereços IP (na notação de bloco CIDR) em uma rede
- O ID de um grupo de segurança de um conjunto de instâncias na rede que requer acesso ao servidor DNS

Tipo de protocolo	Número do protocolo	Porta
TCP	6	53
UDP	17	53

Regras do Amazon EFS

Se estiver usando um sistema de arquivos do Amazon EFS com instâncias do Amazon EC2, o grupo de segurança que você associa a seus destinos de montagem do Amazon EFS deve permitir tráfego por meio do protocolo NFS.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	2049 (NFS)	O ID do grupo de segurança	Permite acesso NFS de entrada de recursos (incluindo o destino de montagem) associados a esse grupo de segurança

Para montar um sistema de arquivos do Amazon EFS na instância do Amazon EC2, conecte-se à instância. Portanto, o grupo de segurança associado à instância deve ter regras que permitam SSH de entrada do computador local ou da rede local.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	22 (SSH)	O intervalo de endereços IP do computador local ou o intervalo de endereços IP (na notação de bloco CIDR) da rede.	Permite acesso SSH de entrada no computador local.

Regras do Elastic Load Balancing

Se você estiver usando um load balancer, o grupo de segurança associado ao load balancer deve ter regras que permitam comunicação com suas instâncias ou destinos. Para obter mais informações, consulte Configurar grupos de segurança para o Classic Load Balancer em Guia do usuário para Classic Load Balancers e Grupos de segurança para o Application Load Balancer no Guia do usuário para Application Load Balancers.

Regras de emparelhamento de VPC

É possível atualizar as regras de entrada e saída dos grupos de segurança de VPC para referenciar grupos de segurança na VPC emparelhada. Fazendo isso, você permite que o tráfego flua entre as instâncias associadas com o grupo de segurança referenciado na VPC emparelhada. Para obter

mais informações sobre como configurar grupos de segurança para emparelhamento de VPC, consulte Atualizar os grupos de segurança para referenciar grupos de VPC de mesmo nível.

NitroTPM

O Nitro Trusted Platform Module (NitroTPM) é um dispositivo virtual fornecido pelo AWS Nitro System que está em conformidade com a especificação TPM 2.0. Armazena, com segurança, artefatos (como senhas, certificados ou chaves de criptografia) que são usados para autenticar a instância. O NitroTPM pode gerar chaves e usá-las em funções criptográficas (como hash, assinatura, criptografia e descriptografia).

O NitroTPM fornece inicialização medida, um processo em que o carregador de inicialização e o sistema operacional criam hashes criptográficos de cada binário de inicialização e os combinam aos valores anteriores nos registros de configuração de plataforma (PCRs) internos do NitroTPM. Com a inicialização medida, é possível obter valores de PCR assinados do NitroTPM e usá-los para provar às entidades remotas a integridade do software de inicialização da instância. Isto é conhecido como atestado remoto.

Com o NitroTPM, chaves e segredos podem ser marcados com um valor de PCR específico de modo que nunca possam ser acessados se houver alteração no valor da PCR e, portanto, na integridade da instância. Essa forma especial de acesso condicional é chamada de selagem e desselagem. Tecnologias de sistema operacional, como BitLocker, podem usar o NitroTPM para selar uma chave de descriptografia da unidade, de modo que a unidade só possa ser descriptografada quando o sistema operacional for inicializado corretamente e estiver em bom estado.

Para usar o NitroTPM, é necessário selecionar uma imagem de máquina da Amazon (AMI) que tenha sido configurada para oferecer suporte ao NitroTPM e, em seguida, usar a AMI para iniciar instâncias desenvolvidas no AWS Nitro System. Você pode selecionar uma das AMIs pré-criadas da Amazon ou criar a sua própria.

Custos

Não há custo adicional para usar o NitroTPM. Você paga apenas pelos recursos adjacentes que usar.

Tópicos

- Considerações
- Pré-requisitos para a habilitação na inicialização

- Criar uma AMI Linux para suporte ao NitroTPM
- Verifique se a AMI está habilitada para o NitroTPM
- Habilitar ou interromper o uso do NitroTPM em uma instância
- Recuperar a chave pública de endosso de uma instância

Considerações

As seguintes considerações se aplicam ao usar o NitroTPM:

- Os volumes BitLocker criptografados com chaves baseadas no NitroTPM só podem ser usados na instância original.
- O estado do NitroTPM não está incluído nos snapshots do Amazon EBS.
- O estado do NitroTPM não está incluído nas imagens do VM Import/Export.
- O suporte ao NitroTPM é habilitado especificando um valor de `v2.0` para o parâmetro `tpm-support` ao criar uma AMI. Após iniciar uma instância com a AMI, você não poderá modificar os atributos da instância. Instâncias com NitroTPM não oferecem suporte à API ModifyInstanceAttribute.
- Só é possível criar uma AMI com o NitroTPM configurado usando a API RegisterImage pela AWS CLI e não pelo console do Amazon EC2.
- O NitroTPM não é compatível com o Outposts.
- Não há suporte ao NitroTPM em zonas locais ou zonas Wavelength.

Pré-requisitos para a habilitação na inicialização

Para iniciar uma instância com o NitroTPM habilitado, os pré-requisitos apresentados a seguir devem estar em vigor.

Instâncias do Linux

AMI

Requer uma AMI com o NitroTPM habilitado.

Atualmente, não há AMIs do Amazon Linux habilitadas para o NitroTPM. Para usar uma AMI compatível, é necessário executar várias etapas de configuração em sua própria AMI do Linux. Para ter mais informações, consulte Criar uma AMI Linux para suporte ao NitroTPM.

Sistema operacional

A AMI deve conter um sistema operacional com um driver de buffer de resposta do comando (CRB) TPM 2.0. A maioria dos sistemas operacionais atuais, como o Amazon Linux 2, contém um driver TPM 2.0 CRB.

Modo de inicialização UEFI

O NitroTPM necessita que uma instância seja executada no modo de inicialização da UEFI, o que requer que a AMI seja configurada para o modo de inicialização UEFI. Para ter mais informações, consulte UEFI Secure Boot.

Instâncias do Windows

AMI

Requer uma AMI com o NitroTPM habilitado.

As seguintes AMIs do Windows são pré-configuradas para habilitar o NitroTPM e o UEFI Secure Boot com chaves da Microsoft:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Atualmente, não oferecemos suporte à importação do Windows com o NitroTPM usando o comando IMPORT IMAGE.

Sistema operacional

A AMI deve conter um sistema operacional com um driver de buffer de resposta do comando (CRB) TPM 2.0. A maioria dos sistemas operacionais atuais, como o TPM-Windows_Server-2022-English-Full-Base, contém um driver TPM 2.0 CRB.

Modo de inicialização UEFI

O NitroTPM necessita que uma instância seja executada no modo de inicialização da UEFI, o que requer que a AMI seja configurada para o modo de inicialização UEFI. Para ter mais informações, consulte UEFI Secure Boot.

Tipos de instância

Você deve usar um dos seguintes tipos de instância virtualizada:

- Uso geral: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7i, M7i-flex, T3 e T3a
- Otimizada para computação: C5, C5a, C5ad, C5d, C5n, C6a, C6i, C6id, C6in, C7a, C7i e C7i-flex
- Otimizada para memória: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7i, R7iz, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, X2idn, X2iedn, X2iezn e z1d
- Otimizada para armazenamento: D3, D3en, I3en e I4i
- Com computação acelerada: G4dn, G5, G6, Gr6, Inf1 e Inf2
- Com computação de alta performance: Hpc6a e Hpc6id

> **Note**
>
> Não há suporte para instâncias baseadas em Graviton, instâncias do Xen, instâncias do Mac e instâncias bare metal.

Criar uma AMI Linux para suporte ao NitroTPM

É possível configurar a AMI Linux para oferecer suporte ao NitroTPM ao registrar a AMI. Não é possível configurar o suporte ao NitroTPM posteriormente.

Para obter a lista de AMIs do Windows que são configuradas previamente para oferecer suporte ao NitroTPM, consulte Pré-requisitos para a habilitação na inicialização.

Como registrar uma AMI do Linux para oferecer suporte ao NitroTPM

1. Inicie uma instância temporária com a AMI do Linux necessária.
2. Depois que a instância atingir o estado `running`, crie um snapshot do volume raiz da instância.

3. Registre a nova AMI. Use o comando register-image. Para `--tpm-support`, especifique `v2.0`. Para `--boot-mode`, especifique `uefi`. Além disso, especifique um mapeamento de dispositivos de blocos para o volume raiz usando o snapshot criado na etapa anterior.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \
    --tpm-support v2.0
```

Saída esperada

```
{
"ImageId": "ami-0123456789example"
}
```

4. Encerre a instância temporária iniciada na etapa 1, se ela não for mais necessária.

Verifique se a AMI está habilitada para o NitroTPM

Você pode usar `describe-images` ou `describe-image-attributes` para verificar se a AMI está habilitada para o NitroTPM.

Como verificar se a AMI está habilitada para o NitroTPM usando **`describe-images`**

Use o comando describe-images e especifique o ID da AMI.

```
aws ec2 describe-images --image-ids ami-0123456789example
```

Se o NitroTPM estiver habilitado para a AMI, a saída exibirá `"TpmSupport": "v2.0"`.

```
{
    "Images": [
        {
        ...
        "BootMode": "uefi",
        ...
        "TpmSupport": "v2.0"
```

```
        }
    ]
}
```

Como verificar se a AMI está habilitada para o NitroTPM usando **`describe-image-attribute`**

Use o comando describe-image-attribute e especifique o parâmetro `attribute` com o valor `tpmSupport`.

> **Note**
>
> É necessário ser o proprietário da AMI para chamar `describe-image-attribute`.

```
aws ec2 describe-image-attribute \
    --region us-east-1 \
    --image-id ami-0123456789example \
    --attribute tpmSupport
```

Se o NitroTPM estiver habilitado para a AMI, o valor do `TpmSupport` será `"v2.0"`. Observe que `describe-image-attribute` retorna somente os atributos especificados na solicitação.

```
{
    "ImageId": "ami-0123456789example",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Habilitar ou interromper o uso do NitroTPM em uma instância

Ao iniciar uma instância em uma AMI com suporte ao NitroTPM habilitado, a instância será iniciada com o NitroTPM habilitado. É possível configurar a instância para interromper o uso do NitroTPM. É possível verificar se a instância está habilitada para o NitroTPM.

Tópicos

- Iniciar uma instância com o NitroTPM habilitado
- Interromper o uso do NitroTPM em uma instância

- Verificar se o NitroTPM está acessível dentro da instância

Iniciar uma instância com o NitroTPM habilitado

Quando você inicia uma instância com os pré-requisitos, o NitroTPM é habilitado automaticamente na instância. Você só pode habilitar o NitroTPM em uma instância ao iniciar. Para obter mais informações sobre como iniciar uma instância, consulte Executar sua instância.

Interromper o uso do NitroTPM em uma instância

Após iniciar uma instância com o NitroTPM habilitado, não será possível desabilitar o NitroTPM para a instância. No entanto, é possível configurar o sistema operacional para interromper o uso do NitroTPM desabilitando o driver do dispositivo TPM 2.0 na instância com as seguintes ferramentas:

- [Instâncias do Linux] Use tpm-tools.
- [Instâncias do Windows] Use o console de gerenciamento do TPM, tpm.msc.

Para obter mais informações sobre como desabilitar o driver do dispositivo, consulte a documentação do sistema operacional.

Verificar se o NitroTPM está acessível dentro da instância

Para verificar se a instância está habilitada para oferecer suporte ao NitroTPM usando a AWS CLI

Use o comando describe-instances da AWS CLI e especifique o ID da instância. Atualmente, o console do Amazon EC2 não exibe o campo `TpmSupport`.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

Se o suporte ao NitroTPM estiver habilitado na instância, a saída exibirá `"TpmSupport": "v2.0"`.

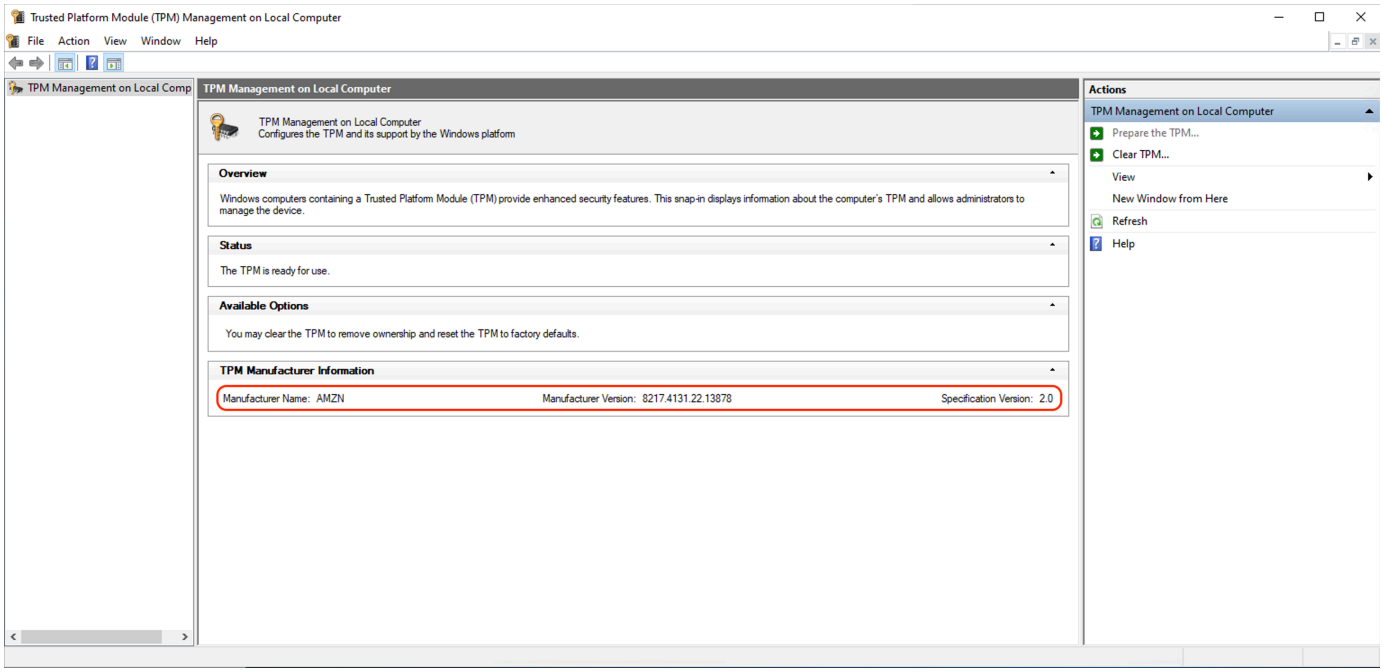
```
"Instances": {
              "InstanceId":"0123456789example",
              "InstanceType":"c5.large",
              ...
              "BootMode": "uefi",
              "TpmSupport": "v2.0"
              ...
```

```
}
```

(Instâncias do Windows) Para verificar se o NitroTPM está acessível em uma instância do Windows do Amazon EC2

1. Conecte-se à instância do Windows do EC2.
2. Na instância, execute o programa tpm.msc.

   Será aberta a janela TPM Management on Local Computer (Gerenciamento do TPM no computador local).
3. Confira o campo TPM Manufacturer Information (Informações do fabricante do TPM). Contém o nome do fabricante e a versão do NitroTPM na instância.



Recuperar a chave pública de endosso de uma instância

É possível recuperar com segurança a chave de criptografia pública de uma instância a qualquer momento usando a AWS CLI.

Para recuperar a chave pública de endosso de uma instância

Use o comando get-instance-tpm-ek-pub da AWS CLI.

Exemplo 1

O comando de exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `tpmt` para a instância `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

A seguir está um exemplo de saída.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Exemplo 2

O comando de exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `der` para a instância `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

A seguir está um exemplo de saída.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
```

```
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

Credential Guard para instâncias do Windows

O AWS Nitro System é compatível com instâncias do Credential Guard para Amazon Elastic Compute Cloud (Amazon EC2) no Windows. O Credential Guard é um recurso de segurança baseada em virtualização (VBS) do Windows que permite a criação de ambientes isolados para proteger ativos de segurança, como credenciais de usuário do Windows e imposição da integridade de código, além das proteções do kernel do Windows. Quando você executa instâncias do Windows no EC2, o Credential Guard usa o AWS Nitro System para impedir que as credenciais de login do Windows sejam extraídas da memória do sistema operacional.

Conteúdos

- Pré-requisitos
- Inicialização de uma instância compatível
- Desabilitação da integridade da memória
- Ativação do Credential Guard
- Verificação se o Credential Guard está em execução

Pré-requisitos

Sua instância do Windows deve cumprir os pré-requisitos a seguir para utilizar o Credential Guard.

Imagens de máquina da Amazon (AMIs)

A AMI deve ser pré-configurada para habilitar o NitroTPM e o UEFI Secure Boot. Para obter mais informações sobre as AMIs compatíveis, consulte the section called “Pré-requisitos”.

Integridade da memória

Não há suporte à integridade da memória, também conhecida como integridade de código protegida por hipervisor (HVCI) ou integridade de código imposta pelo hipervisor. Antes de ativar o Credential Guard, você deve garantir que esse atributo esteja desabilitado. Para ter mais informações, consulte Desabilitação da integridade da memória.

Tipos de instância

Os seguintes tipos de instância são compatíveis com o Credential Guard em todos os tamanhos, exceto se indicado de outra forma: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `C7i`, `C7i-flex`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `M7i`, `M7i-flex`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in` `R7i`, `R7iz`, `T3`.

> **Note**
>
> - Embora o NitroTPM tenha alguns tipos de instância obrigatórios em comum, o tipo de instância deve ser um dos tipos de instância anteriores para ser compatível com o Credential Guard.
> - O Credential Guard não é compatível com:
>   - Instâncias bare metal
>   - Os seguintes tipos de instância: `C7i.48xlarge`, `M7i.48xlarge` e `R7i.48xlarge`.

Para obter mais informações sobre tipos de instância, consulte o Guia de tipos de instância do Amazon EC2.

Inicialização de uma instância compatível

Agora é possível usar o console do Amazon EC2 ou AWS Command Line Interface (AWS CLI) para iniciar uma instância que é compatível com o Credential Guard. Você precisará de um ID de AMI compatível para iniciar sua instância, que seja exclusivo para cada Região da AWS.

> **Tip**
>
> Você pode usar o link a seguir para descobrir e iniciar instâncias com AMIs compatíveis fornecidas pela Amazon no console do Amazon EC2: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

Para iniciar uma instância usando o console do Amazon EC2

Siga as etapas para iniciar uma instância, especificando um tipo de instância compatível e uma AMI do Windows configurada previamente.

AWS CLI

Para iniciar uma instância usando o AWS CLI

Use o comando run-instances para iniciar uma instância usando um tipo de instância compatível e a AMI do Windows pré-configurada.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-id
    --key-name key-name
```

PowerShell

Para iniciar uma instância usando o AWS Tools for PowerShell

Use o comando New-EC2Instance para iniciar uma instância usando um tipo de instância compatível e a AMI do Windows pré-configurada.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-id `
    -KeyName key-name
```

Desabilitação da integridade da memória

É possível usar o Editor de Política de Grupo Local para desativar a integridade da memória em cenários compatíveis. A seguinte orientação pode ser aplicada para cada configuração em Proteção da integridade do código baseada em virtualização:

- Habilitada sem bloqueio: modifique a configuração para Desabilitada para desabilitar a integridade da memória.

- Habilitada com bloqueio de UEFI: a integridade da memória foi habilitada com o bloqueio de UEFI. A integridade da memória não pode ser desabilitada depois de habilitada com o bloqueio de UEFI. Recomendamos criar uma nova instância com a integridade da memória desabilitada e encerrar a instância sem suporte se ela não estiver em uso.

Para desabilitar a integridade da memória com o Editor de Política de Grupo Local

1. Conecte-se à sua instância como uma conta de usuário com privilégios de administrador usando o protocolo do Desktop Remoto (RDP). Para ter mais informações, consulte the section called "Conexão com a instância do Windows usando um cliente RDP".
2. Abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Execute os comandos a seguir para abrir o Editor de Política de Grupo Local: `gpedit.msc`
4. No Editor de Política de Grupo Local, selecione Configuração do Computador, Modelos Administrativos, Sistema, Device Guard.
5. Selecione Ativar Segurança Baseada em Virtualização e, em seguida, selecione Editar configuração de política.
6. Abra o menu suspenso de configurações para Proteção da integridade do código baseada em virtualização, escolha Desabilitada e, em seguida, escolha Aplicar.
7. Reinicie a instância para aplicar as alterações.

Ativação do Credential Guard

Depois de iniciar uma instância do Windows com um tipo de instância e uma AMI compatíveis e confirmar que a integridade da memória está desabilitada, você poderá habilitar o Credential Guard.

> **Important**
>
> São necessários privilégios de administrador para executar as seguintes etapas para ativar o Credential Guard.

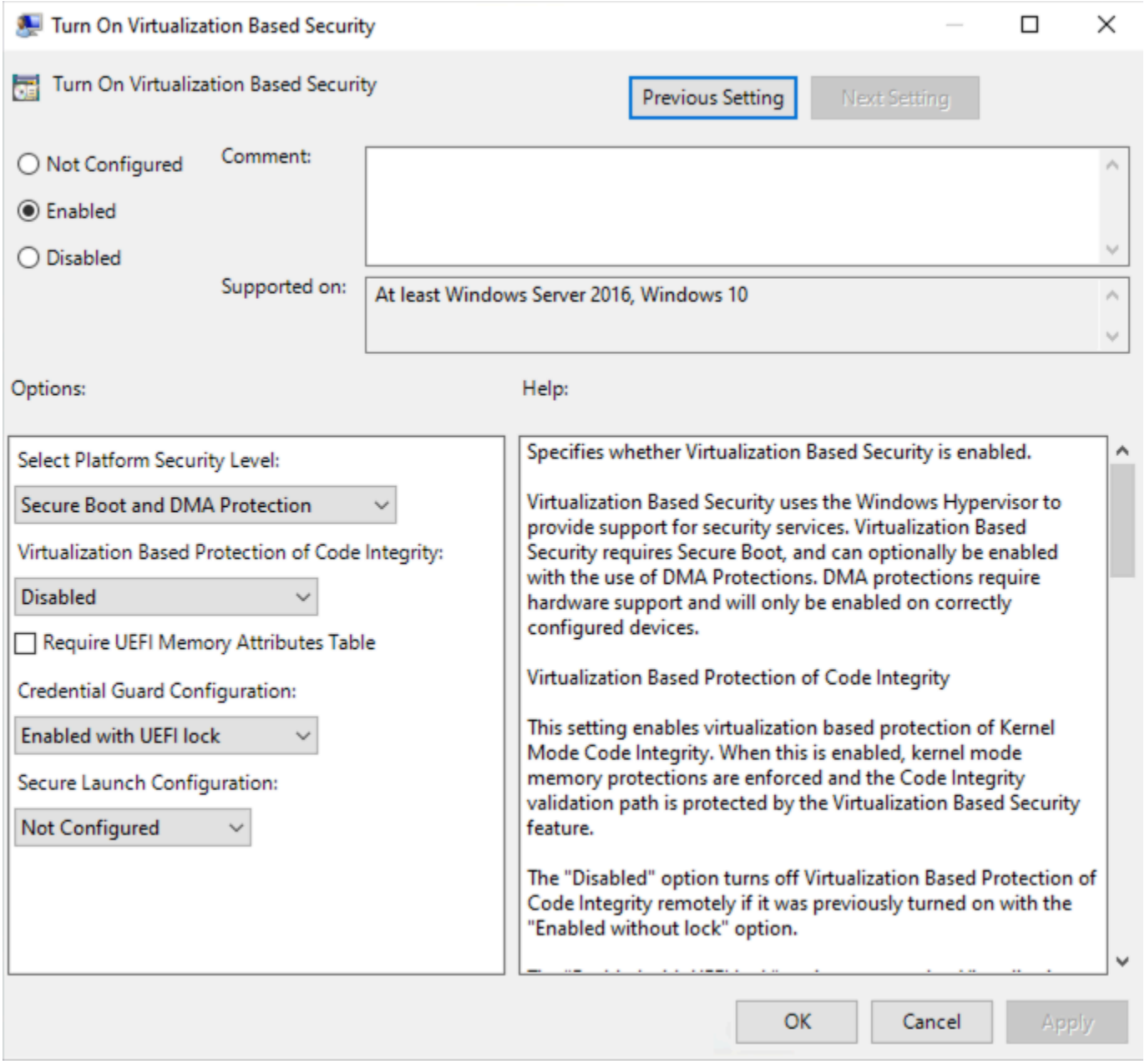
Para ativar o Credential Guard

1. Conecte-se à sua instância como uma conta de usuário com privilégios de administrador usando o protocolo do Desktop Remoto (RDP). Para ter mais informações, consulte the section called "Conexão com a instância do Windows usando um cliente RDP".

2. Abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Execute os comandos a seguir para abrir o Editor de Política de Grupo Local: `gpedit.msc`
4. No Editor de Política de Grupo Local, selecione Configuração do Computador, Modelos Administrativos, Sistema, Device Guard.
5. Selecione Ativar Segurança Baseada em Virtualização e, em seguida, selecione Editar configuração de política.
6. Escolha Ativado no menu Ativar Segurança Baseada em Virtualização.
7. Em Selecione o Nível de Segurança da Plataforma, escolha Inicialização segura e a proteção de DMA.
8. Em Configuração do Credential Guard, escolha Habilitada com bloqueio de UEFI.

> **Note**
>
> As configurações de política restantes não são necessárias para ativar o Credential Guard e podem ser deixadas como Não configuradas.

A imagem a seguir exibe as configurações de VBS definidas conforme descrito anteriormente:



9. Reinicie a instância para aplicar as configurações.

Verificação se o Credential Guard está em execução

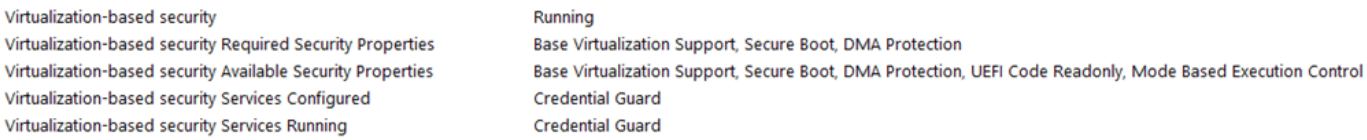
Você pode usar a ferramenta Informações do sistema Microsoft (`Msinfo32.exe`) para confirmar se o Credential Guard está em execução.

> **Important**
>
> Você deve primeiro reinicializar a instância para concluir a aplicação das configurações de política necessárias para ativar o Credential Guard.

Para verificar se o Credential Guard está em execução

1. Conecte-se à sua instância usando o Remote Desktop Protocol (RDP). Para ter mais informações, consulte the section called “Conexão com a instância do Windows usando um cliente RDP”.
2. Na sessão RDP da sua instância, abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Abra as informações do sistema ao executar o comando a seguir: `msinfo32.exe`
4. A ferramenta Informações do sistema Microsoft lista os detalhes da configuração do VBS. Ao lado de Serviços de segurança baseados em virtualização, confirme se o Credential Guard aparece como em execução.

   A imagem a seguir mostra que o VBS está sendo executado conforme descrito anteriormente:



Opções de armazenamento para as instâncias do Amazon EC2

O Amazon EC2 fornece opções de armazenamento físico de dados flexíveis, econômicas e fáceis de usar para suas instâncias. Cada opção tem uma combinação exclusiva de performance e durabilidade. Essas opções de armazenamento podem ser usadas independentemente ou em conjunto para atender às suas necessidades.

Amazon EBS

O Amazon EBS fornece volumes duráveis de armazenamento ao nível do bloco que podem ser anexados e desanexados das instâncias. É possível anexar vários volumes do EBS a uma única instância. Um volume do EBS persiste independentemente da vida útil da instância associada a ele. Você pode criptografar os volumes do EBS. Para manter uma cópia de backup dos dados, você pode criar snapshots dos volumes do EBS. Os snapshots são armazenados no Amazon S3. Você pode criar um volume do EBS a partir de um snapshot.

Armazenamento de instâncias

O armazenamento de instâncias fornece armazenamento temporário em nível de bloco para as instâncias. O número, o tamanho e o tipo dos volumes de armazenamento de instâncias são determinados pelo tipo e tamanho da instância. Os dados em um volume de armazenamento de instâncias só são mantidos durante a vida da instância associada; se você interromper, hibernar ou encerrar uma instância, todos os dados em volumes de armazenamento de instâncias serão perdidos.

Amazon EFS (somente para instâncias do Linux)

O Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. É possível criar um sistema de arquivos de EFS e configurar suas instâncias para montar o sistema de arquivos. É possível usar um sistema de arquivos EFS como uma fonte de dados comum para workloads e aplicações em execução em várias instâncias.

Amazon S3

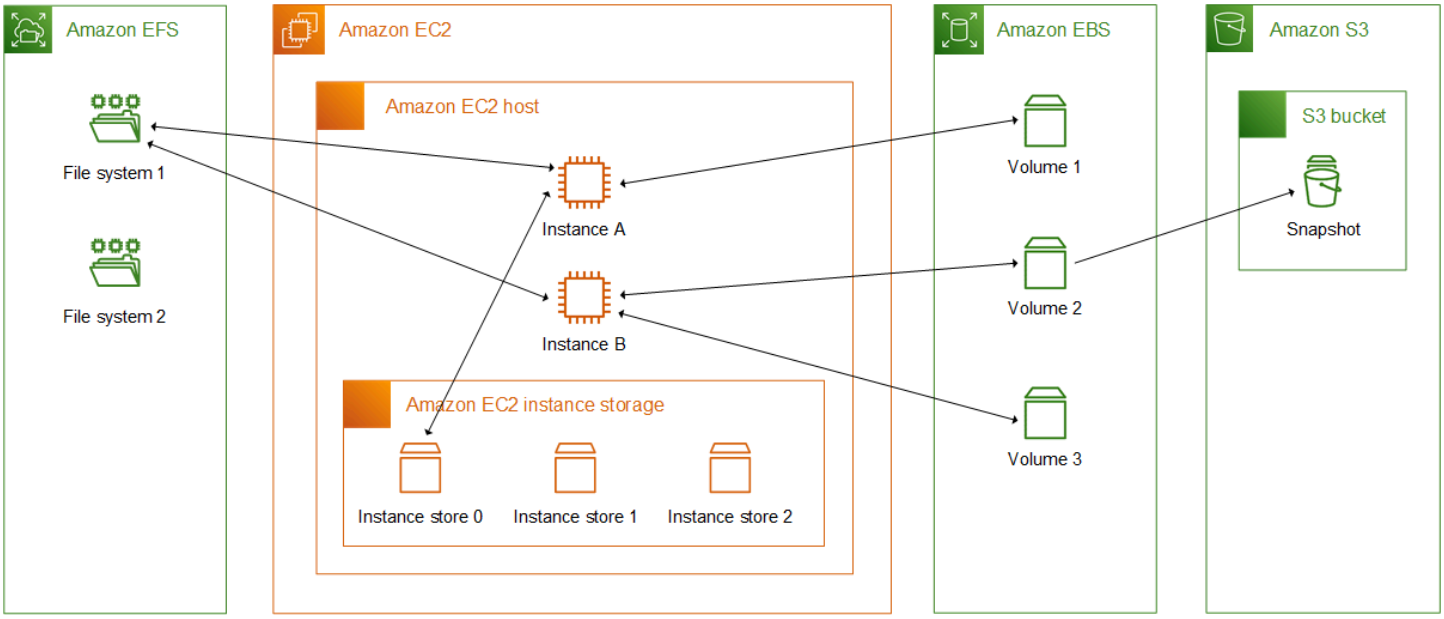
O Amazon S3 fornece acesso a uma infraestrutura de armazenamento físico de dados confiável e econômica. Ele foi projetado para facilitar a computação em escala da Web habilitando o armazenamento e a recuperação de qualquer quantidade de dados, a qualquer momento, no Amazon EC2 ou em qualquer lugar na Web. Por exemplo, é possível usar o Amazon S3 para

armazenar cópias de backup de seus dados e aplicações. O Amazon EC2 usa o Amazon S3 para armazenar snapshots do EBS e AMIs com armazenamento de instâncias.

Amazon FSx

Com o Amazon FSx, você pode iniciar, executar e escalar sistemas de arquivos com muitos atributos e de alta performance na nuvem. O Amazon FSx é um serviço totalmente gerenciado que é compatível com uma ampla variedade de workloads. Você pode escolher entre esses sistemas de arquivos amplamente usados: Lustre, NetApp ONTAP, OpenZFS e Windows File Server.

A figura a seguir mostra a relação entre essas opções de armazenamento e sua instância.



Definição de preço de armazenamento

Abra Preços da AWS, vá até Preços de produtos da AWS e selecione Armazenamento. Escolha o produto de armazenamento para abrir sua página de preços.

Usar o Amazon EBS com o Amazon EC2

O Amazon Elastic Block Store (Amazon EBS) oferece recursos de armazenamento em bloco escaláveis e de alta performance que podem ser usados com instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Com o Amazon EBS, é possível criar e gerenciar os seguintes recursos de armazenamento em blocos:

- Volumes do Amazon EBS: volumes de armazenamento que são anexados a instâncias do Amazon EC2. Após anexar um volume a uma instância, você poderá usá-lo da mesma forma como usaria o armazenamento em bloco. A instância pode interagir com o volume da mesma forma que faria com uma unidade local.
- Snapshots do Amazon EBS: esses são backups pontuais dos volumes do Amazon EBS que persistem independentemente do volume em si. É possível criar snapshots para fazer backup dos dados nos volumes do Amazon EBS. Em seguida, você poderá restaurar novos volumes desses snapshots a qualquer momento.

É possível criar e anexar volumes do Amazon EBS a uma instância durante a execução, e você pode criar e anexar volumes do EBS a uma instância a qualquer momento após o início da execução. Também é possível criar snapshots baseados em um volume a qualquer momento após a criação.

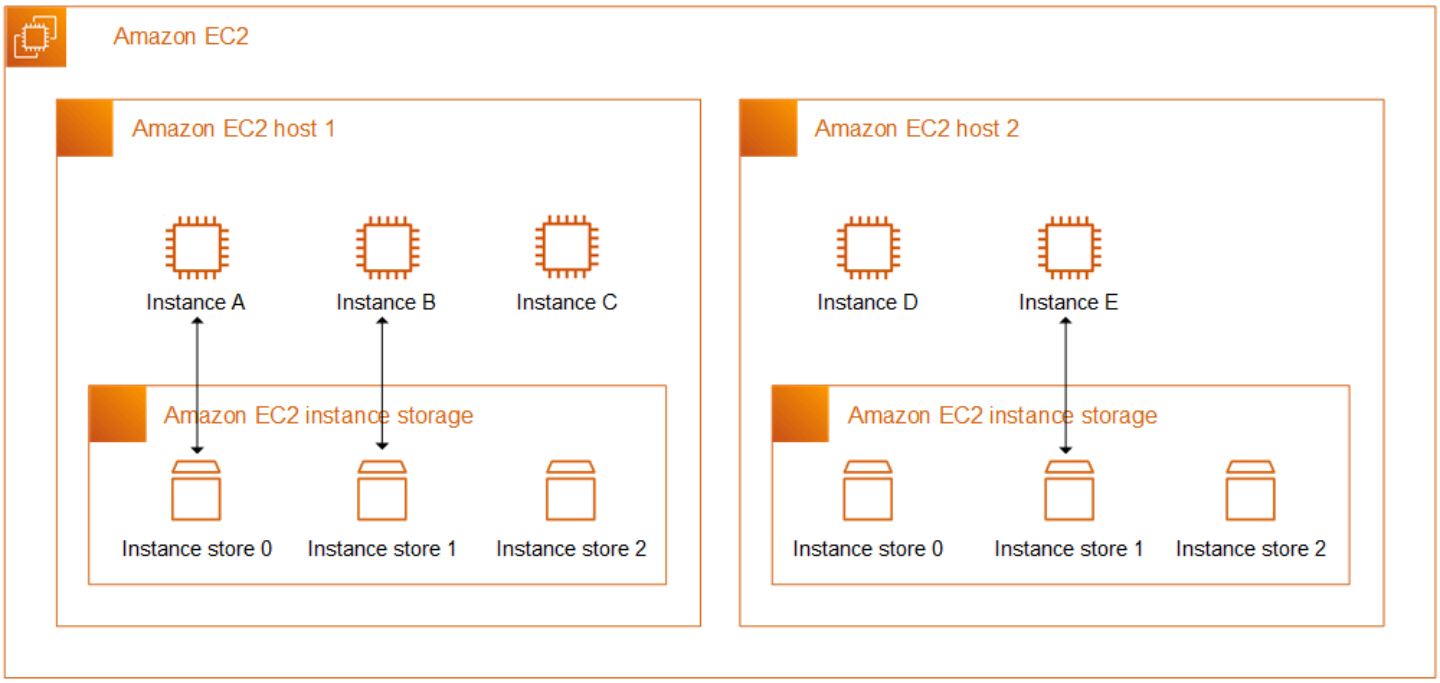
Para obter mais informações sobre como trabalhar com volumes e snapshots, consulte o Guia do usuário do Amazon EBS.

Armazenamento de instâncias do Amazon EC2

Um armazenamento de instâncias fornece armazenamento temporário em nível de bloco para a instância. Esse armazenamento está localizado em discos que estão anexados fisicamente ao computador host. O armazenamento de instância é ideal para armazenamento temporário de informações que mudam com frequência, como buffers, caches, dados temporários e outros conteúdos temporários. Ele também pode ser usado para o armazenamento de dados temporários replicados em toda a frota de instâncias, como um grupo com balanceamento de carga de servidores Web.

Um armazenamento de instâncias consiste em um ou mais volumes de armazenamento de instâncias expostos como dispositivos de bloco. O tamanho de um armazenamento de instâncias e o número de dispositivos disponíveis variam por tipo e tamanho de instância. Para ter mais informações, consulte Volumes de armazenamento de instâncias.

Os dispositivos virtuais para volumes de armazenamento de instâncias são `ephemeral[0-23]`. Tipos de instância que oferecem suporte a um volume de armazenamento de instâncias têm `ephemeral0`. Os tipos de instância que são compatíveis com dois volumes de armazenamento de instâncias ou mais têm `ephemeral0`, `ephemeral1` e assim por diante.



Preço de armazenamento de instância

Os volumes do armazenamento de instâncias são incluídos como parte do custo por uso da instância.

Conteúdo

- Volume de armazenamento de instâncias e vida útil dos dados
- Volumes de armazenamento de instâncias
- Adicionar volumes de armazenamento de instâncias à instância do EC2
- Volumes de armazenamento de instâncias SSD
- Volumes de troca de armazenamento de instância para instâncias do Linux
- Otimização do desempenho do disco para volumes de armazenamento de instância em instâncias do Linux

Volume de armazenamento de instâncias e vida útil dos dados

O número, o tamanho e o tipo dos volumes de armazenamento de instâncias são determinados pelo tipo e tamanho da instância. Para ter mais informações, consulte Volumes de armazenamento de instâncias.

Os volumes de armazenamento de instâncias são anexados somente na execução da instância. Você não pode anexar volumes de armazenamento de instâncias depois de executar. Você não pode desanexar um volume de armazenamento de instâncias de uma instância e anexá-lo a outra instância.

Um volume de armazenamento de instâncias existe somente durante a vida útil da instância à qual está anexado. Você não pode configurar um volume de armazenamento de instâncias para persistir além da vida útil da instância associada.

Os dados em um volume de armazenamento de instâncias persistem mesmo que a instância seja reinicializada. No entanto, os dados não persistem se a instância for interrompida, hibernada ou encerrada. Quando a instância for interrompida, hibernada ou encerrada, todos os blocos do volume de armazenamento de instâncias serão apagados criptograficamente.

Portanto, não dependa dos volumes de armazenamento de instâncias para dados valiosos e de longo prazo. Se você precisar reter os dados armazenados em um volume de armazenamento de instâncias além da vida útil da instância, você precisará copiar manualmente esses dados para um armazenamento mais persistente, como um volume do Amazon EBS, um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS.

Há alguns eventos que podem fazer com que seus dados não persistam durante toda a vida útil da instância. A tabela a seguir indica se os dados nos volumes de armazenamento de instâncias persistem durante eventos específicos, tanto para instâncias virtualizadas quanto para instâncias bare metal.

Evento	O que acontece com seus dados?
Eventos do ciclo de vida da instância iniciados pelo usuário	
A instância foi reinicializada	The data persists
A instância foi interrompida	The data does not persist
A instância está em hibernação	The data does not persist
A instância foi encerrada	The data does not persist
O tipo da instância foi alterado	The data does not persist *

Evento	O que acontece com seus dados?
Uma AMI baseada em EBS é criada na instância	The data does not persist in the created AMI **
Uma AMI com armazenamento de instância é criada na instância (Linux instances)	The data persists in the AMI bundle uploaded to Amazon S3 ***
Eventos do sistema operacional iniciados pelo usuário	
A shutdown is initiated	The data does not persist †
A restart is initiated	The data persists
Eventos agendados da AWS	
Interrupção da instância	The data does not persist
Reinicialização da instância	The data persists
Reinicialização do sistema	The data persists
Desativação da instância	The data does not persist
Eventos não planejados	
Recuperação automática simplificada	The data does not persist
Recuperação baseada em ação do CloudWatch	The data does not persist
The underlying disk fails	The data on the failed disk does not persist
Power failure	The data persists upon reboot

* Se o novo tipo de instância for compatível com o armazenamento de instâncias, a instância receberá o número de volumes de armazenamento de instâncias compatível com o novo tipo de instância, mas os dados não serão transferidos para a nova instância. Se o novo tipo de instância não for compatível com o armazenamento de instâncias, a instância não receberá os volumes de armazenamento de instâncias.

** Os dados não estão incluídos na AMI baseada em EBS e não estão incluídos nos volumes de armazenamento de instâncias anexados às instâncias executadas nessa AMI.

*** Os dados estão incluídos no pacote de AMIs que é carregado no Amazon S3. Quando você executa uma instância nessa AMI, a instância obtém os volumes de armazenamento de instâncias agrupados na AMI com os dados que eles continham no momento em que a AMI foi criada.

† As proteções contra encerramento e interrupção não protegem as instâncias contra interrupções ou encerramentos de instâncias como resultado de desligamentos iniciados por meio do sistema operacional na instância. Os dados armazenados nos volumes de armazenamento de instâncias não persistem nos eventos de interrupção e encerramento de instâncias.

Volumes de armazenamento de instâncias

O número, o tamanho e o tipo dos volumes de armazenamento de instâncias são determinados pelo tipo e tamanho da instância. Alguns tipos de instância, como M6, C6 e R6, não são compatíveis com volumes de armazenamento de instâncias, enquanto outros tipos de instância, como M5d, C6gd e R6gd, são compatíveis com volumes de armazenamento de instâncias. Você não pode anexar mais volumes de armazenamento de instâncias a uma instância do que o compatível com o tipo de instância. Para os tipos de instâncias compatíveis com volumes de armazenamento de instâncias, o número e o tamanho dos volumes de armazenamento de instâncias variam de acordo com o tamanho da instância. Por exemplo, `m5d.large` é compatível com um volume de armazenamento de instâncias de 75 GB, enquanto `m5d.24xlarge` é compatível com quatro volumes de armazenamento de instâncias de 900 GB.

Para tipos de instância com volumes de armazenamento de instâncias NVMe, todos os volumes de armazenamento de instâncias compatíveis são automaticamente anexados à instância na execução. Para tipos de instância com volumes de armazenamento de instância que não tem a especificação NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, é necessário especificar manualmente os mapeamentos de dispositivos de blocos para os volumes de armazenamento de instância que você deseja anexar na inicialização. Depois que a instância for iniciada, você deverá formatar e montar os volumes de armazenamento de instâncias anexados antes de poder usá-los. Você não pode anexar um volume de armazenamento de instâncias depois de executar a instância.

Alguns tipos de instância usam unidades de estado sólido (SSD) NVMe ou SATA, enquanto outros usam unidades de disco rígido (HDD) SATA. SDDs entregam alta performance e aleatória de E/S com latência muito baixa, mas você não precisa que os dados persistam quando a instância é terminada ou você pode tirar proveito de arquiteturas tolerantes a falhas. Para ter mais informações, consulte Volumes de armazenamento de instâncias SSD.

Os dados nos volumes de armazenamento de instâncias do NVMe e alguns volumes de armazenamento de instâncias de HDD são criptografados em repouso. Para ter mais informações, consulte Proteção de dados no Amazon EC2.

Volumes de armazenamento de instâncias disponíveis

O Guia de tipos de instância do Amazon EC2 fornece otimizações de quantidade, de tamanho, de tipo e de performance de volumes de armazenamento de instância disponíveis em cada tipo de instância compatível. Para obter mais informações, consulte as informações a seguir.

- Instance store specifications: General purpose
- Instance store specifications: Compute optimized
- Instance store specifications: Memory optimized
- Instance store specifications: Storage optimized
- Instance store specifications: Accelerated computing
- Instance store specifications: High-performance computing
- Instance store specifications: Previous generation

Como recuperar informações de volume de armazenamento de instância usando a AWS CLI

É possível usar o comando describe-instance-types da AWS CLI para exibir informações sobre um tipo de instância, como seus volumes de armazenamento de instâncias. O exemplo a seguir exibe o tamanho total do armazenamento de instâncias para todas as instâncias R5 com volumes de armazenamento de instâncias.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Exemplo de saída

```
-------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r5ad.24xlarge |  3600  |
|  r5ad.12xlarge |  1800  |
|  r5dn.8xlarge  |  1200  |
```

```
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

O exemplo a seguir exibe os detalhes completos do armazenamento da instância para o tipo de instância especificado.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

O exemplo de resultado mostra que esse tipo de instância tem dois volumes SSD NVMe de 300 GB, para um total de 600 GB de armazenamento de instâncias.

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

Adicionar volumes de armazenamento de instâncias à instância do EC2

Para tipos de instância com volumes de armazenamento de instâncias NVMe, todos os volumes de armazenamento de instâncias compatíveis são automaticamente anexados à instância na execução. Eles são automaticamente enumerados e atribuídos a um nome de dispositivo na execução da instância.

Para tipos de instância com volumes de armazenamento de instância que não tem a especificação NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, é necessário especificar manualmente

os mapeamentos de dispositivos de blocos para os volumes de armazenamento de instância que você deseja anexar na inicialização. Os mapeamentos de dispositivos de blocos podem ser especificados na solicitação de execução da instância ou na AMI usada para executar a instância. O mapeamento de dispositivos de blocos inclui um nome de dispositivo e o volume para o qual ele é mapeado. Para ter mais informações, consulte Mapeamentos de dispositivos de blocos.

> **Important**
>
> Volumes de armazenamento de instâncias podem ser anexados a uma instância somente quando você executá-la. Você não pode anexar volumes de armazenamento de instâncias depois de executar a instância.

Depois de executar uma instância, verifique se os volumes de armazenamento de instâncias da instância estão formatados e montados para poderem ser usados. O volume raiz de uma instância com suporte ao armazenamento de instâncias é montado automaticamente.

Consideração dos volumes raiz

Um mapeamento de dispositivos de blocos sempre especifica o volume raiz da instância. O volume raiz é sempre montado automaticamente.

Instâncias do Linux: o volume raiz corresponde a um volume do Amazon EBS ou a um volume de armazenamento de instância. Para instâncias com um volume de armazenamento de instâncias do volume de raiz, o tamanho desse volume varia por AMI, mas o tamanho máximo é 10 GB. Para ter mais informações, consulte Armazenamento para o dispositivo raiz.

Instâncias do Windows: o volume raiz deve ser um volume do Amazon EBS. O armazenamento de instância não é compatível com o volume raiz.

Conteúdo

- Adicionar volumes de armazenamento de instâncias a uma AMI
- Adicionar volumes de armazenamento de instâncias não NVMe a uma instância
- Disponibilizar volumes de armazenamento de instâncias na instância

Adicionar volumes de armazenamento de instâncias a uma AMI

É possível criar uma AMI com um mapeamento de dispositivos de blocos que inclua volumes de armazenamento de instâncias.

Se você executar uma instância compatível com volumes de armazenamento de instâncias não NVMe usando uma AMI que especifique mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias, a instância incluirá esses volumes de armazenamento de instâncias. Se o número de mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias na AMI exceder o número de volumes de armazenamento de instâncias disponíveis para a instância, os mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias adicionais serão ignorados.

Se você executar uma instância compatível com volumes de armazenamento de instâncias NVMe usando uma AMI que especifique mapeamentos de dispositivos de blocos de volume de armazenamento de instâncias, eles serão ignorados. As instâncias compatíveis com volumes de armazenamento de instâncias NVMe recebem todos os volumes de armazenamento de instâncias compatíveis, independentemente dos mapeamentos de dispositivos de blocos especificados na solicitação de execução da instância e na AMI.

Considerações

- Para instâncias M3, especifique volumes de armazenamento de instância no mapeamento de dispositivos de blocos da instância, não na AMI. O Amazon EC2 pode ignorar mapeamentos de dispositivos de blocos de volumes de armazenamento de instância na AMI.
- Ao executar uma instância, será possível omitir volumes de armazenamento de instâncias não NVMe especificados no mapeamento de dispositivos de blocos da AMI ou adicionar volumes de armazenamentos de instâncias.

New console

Para adicionar volumes de armazenamento de instâncias para uma AMI baseada no Amazon EBS usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances e selecione a instância.
3. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Na página diálogo Create Image (Criar imagem), adicione um nome e uma descrição significativos para imagem.
5. Para cada volume de armazenamento de instâncias a ser adicionado, selecione Add volume (Adicionar volume), em Volume type (Tipo de volume) selecione um volume de

armazenamento de instâncias, e em Device (Dispositivo), selecione um nome de dispositivo. (Para ter mais informações, consulte Nomes de dispositivos em instâncias do Amazon EC2.) O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância. Para instâncias com volumes de armazenamento de instâncias de NVMe, o mapeamento de dispositivos desses volumes depende da ordem na qual o sistema operacional enumera os volumes.

6. Escolha Create Image (Criar imagem).

AWS CLI

Para adicionar volumes de armazenamento de instâncias a uma AMI usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- create-image ou register-image (AWS CLI)
- New-EC2Image e Register-EC2Image (AWS Tools for Windows PowerShell)

Adicionar volumes de armazenamento de instâncias não NVMe a uma instância

Ao executar uma instância compatível com volumes de armazenamento de instâncias não NVMe, é necessário especificar os mapeamentos de dispositivos de blocos dos volumes de armazenamentos de instâncias a serem anexados. Os mapeamentos de dispositivos de blocos devem ser especificados na solicitação de execução da instância ou na AMI usada para executar a instância.

Se a AMI incluir mapeamentos de dispositivos de bloco para os volumes de armazenamento de instâncias, você não precisará especificar mapeamentos de dispositivos de blocos na solicitação de execução da instância, a menos que precise de mais volumes de armazenamento de instâncias do que os incluídos na AMI.

Se a AMI não incluir mapeamentos de dispositivos de blocos para volumes de armazenamento de instâncias, você deverá especificar os mapeamentos de dispositivos de bloco na solicitação de execução da instância.

Considerações

- Para instâncias do M3, é possível receber volumes de armazenamento de instâncias mesmo que você não os especifique no mapeamento de dispositivos de blocos da instância.

Para especificar mapeamentos de dispositivos de blocos na solicitação de execução da instância, use um dos métodos a seguir.

Amazon EC2 console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a AMI a ser usada.
4. Na seção Configurar armazenamento, a seção Volumes de armazenamento de instâncias lista os volumes de armazenamento de instâncias que podem ser anexados à instância. O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância.
5. Para cada volume de armazenamento de instância a ser anexado, em Nome do dispositivo, selecione o nome do dispositivo a ser usado.
6. Defina as configurações de instância restantes conforme necessário e, em seguida, escolha Iniciar instância.

Command line

É possível usar um dos comandos de opções a seguir com a opção correspondente.

- `--block-device-mappings` com run-instances (AWS CLI)
- `-BlockDeviceMapping` com New-EC2Instance (AWS Tools for Windows PowerShell)

Disponibilizar volumes de armazenamento de instâncias na instância

Depois de iniciar uma instância com volumes de armazenamento de instâncias anexados, você deverá montar os volumes antes de poder acessá-los.

> **Note**
>
> Muitos volumes de armazenamento de instâncias são pré-formatados com o sistema de arquivos ext3. Os volumes de armazenamento de instâncias baseados em SSD que oferecem suporte à instrução TRIM não são pré-formatados com nenhum sistema de arquivos. No entanto, é possível formatar volumes com o sistema de arquivos de sua escolha

depois de executar a instância. Para ter mais informações, consulte Suporte a TRIM do volume de armazenamento de instâncias. Em instâncias do Windows, reformatamos os volumes de armazenamento de instâncias com o sistema de arquivos NTFS.

Instâncias do Linux

É possível visualizar e montar os volumes de armazenamento de instância conforme descrito no procedimento a seguir.

Para disponibilizar um volume de armazenamento de instâncias no Linux

1. Conecte-se à instância usando um cliente SSH. Para ter mais informações, consulte Conecte-se à sua instância do Linux.
2. Use o comando `df -h` para visualizar os volumes formatados e montados.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Use o `lsblk` para visualizar todos os volumes que foram mapeados na inicialização, mas não formatados e montados.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Para formatar e montar um volume de armazenamento de instâncias que foi apenas mapeado, faça o seguinte:

   a. Crie um sistema de arquivos no dispositivo usando o comando `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Crie um diretório no qual montar o dispositivo usando o comando `mkdir`.

```
$ sudo mkdir /data
```

c. Monte o dispositivo no diretório recém-criado usando o comando `mount`.

```
$ sudo mount /dev/nvme1n1 /data
```

Instâncias do Windows

Além disso, é possível visualizar os volumes de armazenamento de instância usando o Gerenciamento de Disco do Windows. Para ter mais informações, consulte Listar discos usando o Gerenciamento de disco.

Como montar manualmente um volume de armazenamento de instâncias

1. Escolha Iniciar, insira Gerenciamento de computador e pressione Enter.
2. No painel esquerdo, escolha Gerenciamento de disco.
3. Se você for solicitado a inicializar o volume, escolha o volume a ser inicializado, selecione o tipo de partição necessário dependendo do seu caso de uso e escolha OK.
4. Na lista de volumes, clique com o botão direito do mouse no volume a ser montado e escolha Novo volume simples.
5. No assistente, escolha Avançar.
6. Na tela Especificar tamanho do volume, escolha Avançar para usar o tamanho máximo do volume. Como alternativa, escolha um tamanho de volume que esteja entre o espaço mínimo e o máximo em disco.
7. Na tela Atribuir uma letra ou um caminho de unidade, siga um destes procedimentos e escolha Avançar.

   - Para montar o volume com uma letra de unidade, escolha Atribuir a seguinte letra de unidade e escolha a letra da unidade a ser usada.
   - Para montar o volume como uma pasta, escolha Montar na seguinte pasta NTFS vazia e escolha Procurar para criar ou selecionar a pasta a ser usada.
   - Para montar o volume sem uma letra ou um caminho de unidade, escolha Não atribuir uma letra ou um caminho de unidade.

8. Na tela Formatar partição, especifique se deseja ou não formatar o volume. Se você optar por formatar o volume, escolha o sistema de arquivos e o tamanho da unidade necessários e especifique um rótulo de volume.
9. Escolha Avançar e Concluir.

Para obter instruções sobre como montar um volume associado automaticamente após a reinicialização, consulte Montar um volume associado automaticamente após a reinicialização no Guia do usuário do Amazon EBS.

Volumes de armazenamento de instâncias SSD

Como outros volumes de armazenamento de instâncias, é necessário mapear os volumes de armazenamento de instância SSD para sua instância quando ela é executada. Os dados nos volumes de instância SSD persistem apenas durante a vida útil da instância do associada. Para obter mais informações, consulte Adicionar volumes de armazenamento de instâncias à instância do EC2.

Volumes SSD de NVMe

Algumas instâncias oferecem volumes de armazenamento de instâncias de unidades de estado sólido (SSD) de memória expressa não volátil (NVMe). Para obter mais informações sobre o tipo de volume de armazenamento de instâncias compatível com cada tipo de instância, consulte Volumes de armazenamento de instâncias.

Os dados no armazenamento de instâncias de NVMe são criptografados usando uma criptografia de bloco XTS-AES-256 implementada em um módulo de hardware na instância. As chaves de criptografia são geradas usando o módulo de hardware e são exclusivas para cada dispositivo de armazenamento de instâncias de NVMe. Todas as chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode desativar essa criptografia e não pode fornecer sua própria chave de criptografia.

Instâncias do Linux

Para acessar os volumes de NVMe, os drivers de NVMe devem ser instalados. As AMIs a seguir atendem a este requisito:

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 e posteriores

- Ubuntu 14.04 ou posterior com kernel `linux-aws`

> **Note**
>
> Os tipos de instância baseados no AWS Graviton requerem o Ubuntu 18.04 ou posterior com kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

- Bottlerocket

Depois de se conectar à instância, é possível listar os dispositivos de NVMe usando o comando lspci O seguinte é um exemplo da saída de uma instância `i3.8xlarge` compatível com quatro dispositivos de NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Se você está usando um sistema operacional compatível mas os dispositivos de NVMe não estão sendo exibidos, verifique se o módulo de NVMe está carregado usando o comando a seguir.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

Os volumes de NVMe estão em conformidade com a especificação NVMe 1.0e. É possível usar os comandos de NVMe com os volumes de NVMe. Com o Amazon Linux, é possível instalar o pacote `nvme-cli` no repositório usando o comando yum install. Com outras versões compatíveis do Linux, é possível fazer download do pacote `nvme-cli` se ele não estiver disponível na imagem.

Instâncias do Windows

As AMIs do Windows da AWS mais recentes dos seguintes sistemas operacionais contêm os drivers do AWS NVMe usados para interagir com volumes de armazenamento de instâncias SSD que são expostos como dispositivos de bloco de NVMe para melhor performance:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Depois de se conectar à instância, é possível verificar se você vê os volumes de NVMe no Gerenciador de Disco. Na barra de ferramentas, abra o menu de contexto (clique com o botão direito do mouse) no logotipo do Windows e escolha Disk Management.

As AMIs do Windows da AWS fornecidas pela Amazon incluem o driver do AWS NVMe. Se você não estiver usando as AMIs do Windows da AWS mais recentes, instale o driver atual do AWS NVMe.

Volumes SSD não NVMe

As instâncias apresentadas a seguir oferecem suporte a volumes de armazenamento de instância que usam SSDs não NVMe para fornecer alta performance de E/S randômica: C3, I2, M3, R3 e

X1. Para obter mais informações sobre o suporte a volumes de armazenamento de instâncias com suporte de cada tipo de instância, consulte Volumes de armazenamento de instâncias.

Performance de E/S de volume de armazenamento de instância baseada em SSD

Ao preencher os volumes de armazenamento de instâncias baseados em SSD, o número de IOPS de gravação que é possível atingir diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instância baseados em SSD fornecidos a uma instância não têm espaço reservado para o provisionamento em excesso. Para reduzir a amplificação da gravação, recomendamos reservar 10% do volume como não particionado, de modo que o controlador SSD possa usá-lo para provisionamento em excesso. Isso diminui o armazenamento que é possível usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instância compatíveis com TRIM, é possível usar o comando TRIM para notificar o controlador de SSD sempre que você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar o desempenho. Para ter mais informações, consulte Suporte a TRIM do volume de armazenamento de instâncias.

Suporte a TRIM do volume de armazenamento de instâncias

Alguns tipos de instâncias oferecem suporte a volumes SSD com TRIM. Para ter mais informações, consulte Volumes de armazenamento de instâncias.

> **Note**
>
> (Somente para instâncias do Windows) As instâncias que executam o Windows Server 2012 R2 são compatíveis com a função TRIM a partir da versão 7.3.0 do driver PV da AWS. As instâncias que executam versões anteriores do Windows Server não são compatíveis com TRIM.

Os volumes de armazenamento de instâncias que oferecem suporte ao TRIM são aparados completamente antes de serem alocados à instância. Esses volumes não estão formatados com um sistema de arquivos quando uma instância é iniciada, portanto, é necessário formatá-los para que possam ser montados e usados. Para obter acesso mais rápido a esses volumes, é necessário ignorar a operação TRIM ao formatá-los.

(Instâncias do Windows) Para desabilitar temporariamente o suporte para a função TRIM durante a formatação inicial, use o comando `fsutil behavior set DisableDeleteNotify 1`. Após a conclusão da formatação, habilite novamente o suporte para a função TRIM ao usar `fsutil behavior set DisableDeleteNotify 0`.

Com volumes de armazenamento de instâncias que oferecem suporte ao TRIM, é possível usar o comando TRIM para notificar o controlador de SSD quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Em instâncias do Linux, use o comando `fstrim` para habilitar a função TRIM periódica. Em instâncias do Windows, use o comando `fsutil behavior set DisableDeleteNotify 0` para garantir que o suporte para a função TRIM esteja habilitado durante a operação normal.

Volumes de troca de armazenamento de instância para instâncias do Linux

> **Note**
>
> Este tópico se aplica somente a instâncias do Linux.

O espaço de troca no Linux pode ser usado quando um sistema precisa de mais memória que a que foi alocada fisicamente. Quando o espaço de troca está habilitado, os sistemas Linux podem mudar páginas da memória física usadas infrequentemente para espaço de troca (uma partição dedicada

ou um arquivo de troca em um sistema de arquivos existente) e liberar esse espaço para páginas de memória que exigem acesso de alta velocidade.

> **Note**
>
> O uso do espaço de troca para paginação de memória não é tão rápido ou eficiente quanto usar a RAM. Se a workload estiver paginando a memória regularmente no espaço de troca, é necessário considerar migrar para um tipo de instância maior com mais memória RAM. Para obter mais informações, consulte Alterar o tipo de instância.

Os tipos de instância `c1.medium` e `m1.small` têm uma quantidade limitada de memória física para trabalhar e recebem um volume de troca de 900 MiB no momento do lançamento para atuar como memória virtual para AMIs do Linux. Embora o kernel do Linux veja esse espaço de troca como uma partição no dispositivo raiz, ele é na verdade um volume separado para armazenamento de instâncias, independentemente do tipo de dispositivo raiz.

O Amazon Linux habilita e usa automaticamente esse espaço de troca, mas a AMI pode exigir algumas etapas adicionais para reconhecer e usar esse espaço de troca. Para ver se a instância está usando o espaço de troca, é possível usar o comando swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

A instância acima tem um volume de troca de 900 MiB anexado e habilitado. Se você não vir um volume de troca listado com esse comando, será possível precisar habilitar o espaço de troca para o dispositivo. Verifique os discos disponíveis usando o comando lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

Aqui, o volume de troca `xvda3` está disponível para a instância, mas não está habilitado (observe que o campo `MOUNTPOINT` está vazio). É possível habilitar o volume de troca com o comando swapon.

> **Note**
>
> Você precisa preceder `/dev/` ao nome do dispositivo listado pelo lsblk. Seu dispositivo pode ter um nome diferente, como `sda3`, `sde3` ou `xvde3`. Use o nome do dispositivo de seu sistema no comando abaixo.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Agora o espaço de troca deve ser mostrado na saída do lsblk e do swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Também será necessário editar o arquivo `/etc/fstab` para que esse espaço de troca seja habilitado automaticamente em cada inicialização do sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Acrescente a linha a seguir ao arquivo `/etc/fstab` (usando o nome do dispositivo de troca de seu sistema):

```
/dev/xvda3       none    swap    sw  0       0
```

Para usar um volume de armazenamento de instâncias como espaço de troca

Qualquer volume de armazenamento de instâncias pode ser usado como espaço de troca. Por exemplo, o tipo de instância `m3.medium` inclui um volume de armazenamento de instâncias SSD de 4 GB que é adequado para o espaço de troca. Se o volume de armazenamento de instâncias for muito maior (por exemplo, 350 GB), será possível considerar particionar o volume com uma partição de troca menor de 4 a 8 GB e o restante para um volume de dados.

> **Note**
>
> Esse procedimento se aplica apenas a tipos de instância que oferecem suporte ao armazenamento de instâncias. Para obter uma lista dos tipos de instâncias compatíveis, consulte Volumes de armazenamento de instâncias.

1. Liste os dispositivos de blocos anexados à instância para obter o nome do dispositivo de seu volume de armazenamento de instâncias.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   Neste exemplo, o volume de armazenamento de instâncias é `/dev/xvdb`. Como essa é uma instância do Amazon Linux, o volume de armazenamento de instâncias está formatado e montado em `/media/ephemeral0`. Nem todos os sistemas operacionais Linux fazem isso automaticamente.

2. (Opcional) Se o volume de armazenamento de instâncias está montado (ele é listado como um `MOUNTPOINT` na saída do comando lsblk), você precisa desmontá-lo com o comando a seguir.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configure uma área de troca do Linux no dispositivo com o comando mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Habilite o novo espaço de troca.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifique se o novo espaço de troca está sendo usado.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
```

```
/dev/xvdb                                 partition 4188668 0 -1
```

6. Edite o arquivo `/etc/fstab` para que esse espaço de troca seja habilitado automaticamente em cada inicialização do sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Se o arquivo `/etc/fstab` tiver uma entrada para `/dev/xvdb` (ou para`/dev/sdb`) altere-o para que corresponda à linha abaixo. Se ele não tiver uma entrada para esse dispositivo, adicione a linha a seguir no arquivo `/etc/fstab` (usando o nome do dispositivo de troca de seu sistema):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Os dados do volume de armazenamento de instâncias são perdidos quando uma instância é interrompida ou hibernada. Isso inclui a formatação do espaço de troca do armazenamento de instâncias criadas em Step 3. Se você parar e reiniciar uma instância que foi configurada para usar o espaço de troca de armazenamento de instâncias, deverá repetir a Step 1 até a Step 5 no novo volume de armazenamento de instâncias.

Otimização do desempenho do disco para volumes de armazenamento de instância em instâncias do Linux

> **Note**
>
> Este tópico se aplica somente a instâncias do Linux.

Por causa do modo como o Amazon EC2 virtualiza os discos, a primeira gravação em qualquer local em alguns volumes de armazenamento de instâncias ocorre mais lentamente que as gravações subsequentes. Para a maioria das aplicações, a amortização desse custo ao longo da vida útil da instância é aceitável. Entretanto, se você precisar de alta performance de disco, recomendamos inicializar suas unidades gravando uma vez em todos os locais da unidade antes do uso em produção.

> **Note**
>
> Alguns tipos de instância com discos de estado sólido (SSD) anexados diretamente e suporte a TRIM fornecem performance máxima no momento da inicialização, sem inicialização. Para obter informações sobre o armazenamento de instâncias para cada tipo de instância, consulte Volumes de armazenamento de instâncias.

Se você precisar de maior flexibilidade na latência ou no throughput, recomendamos usar o Amazon EBS.

Para inicializar os volumes de armazenamento de instâncias, use os seguintes comandos dd, dependendo do armazenamento a ser inicializado (por exemplo, `/dev/sdb` ou `/dev/nvme1n1`).

> **Note**
>
> Desmonte a unidade antes de executar esse comando.
> A inicialização pode levar muito tempo (cerca de oito horas para uma instância extragrande).

Para inicializar os volumes de armazenamento de instâncias, use os comandos a seguir nos tipos de instância `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` e `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Para executar a inicialização em todos os volumes de armazenamento de instâncias ao mesmo tempo, use o comando a seguir:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

A configuração de unidades para RAID as inicializa gravando em todos os locais da unidade. Ao configurar o RAID com base em software, altere a velocidade mínima da reconstrução:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Armazenamento de arquivos

O armazenamento de arquivos na nuvem é um método de armazenamento de dados na nuvem que permite que servidores e aplicações acessem os dados por meio de sistemas de arquivos compartilhados. Essa compatibilidade faz do armazenamento de arquivos na nuvem uma opção ideal para workloads que dependem de sistemas de arquivos compartilhados e oferece simplicidade de integração, sem alterações de código.

Há muitas soluções de armazenamento de arquivos, desde um servidor de arquivos de nó único em uma instância de computação que usa armazenamento em blocos como base sem escalabilidade ou poucas redundâncias para proteger os dados a uma solução clusterizada do tipo "faça você mesmo" ou a uma solução totalmente gerenciada. O conteúdo apresentado a seguir introduz alguns dos serviços de armazenamento fornecidos pela AWS para o uso com instâncias do Amazon EC2.

Conteúdo

- Usar o Amazon S3 com a Amazon EC2
- Uso do Amazon EFS com instâncias do Linux
- Use o Amazon FSx com o Amazon EC2
- Usar o Amazon File Cache com o Amazon EC2

Usar o Amazon S3 com a Amazon EC2

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance. Você pode usar o Amazon S3 para armazenar e recuperar qualquer volume de dados para uma variedade de casos de uso, como data lakes, sites, backups e análises de big data, diretamente de uma instância do Amazon EC2 ou de qualquer lugar na Internet. Para obter mais informações, consulte O que é a Amazon S3?

Os objetos são as entidades fundamentais armazenadas no Amazon S3. Cada objeto armazenado no Amazon S3 é contido em um bucket. Os buckets organizam o namespace do Amazon S3 no nível mais alto e identificam a conta responsável por esse armazenamento. Os buckets do Amazon S3 são semelhantes aos nomes de domínio da Internet. Os objetos armazenados em buckets têm um valor de chave exclusiva e são recuperados usando um URL. Por exemplo, se um objeto com um valor de chave `/photos/mygarden.jpg` estiver armazenado no bucket `DOC-EXAMPLE-BUCKET1`, ele será endereçável usando a URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg`. Para obter mais informações, consulte Como o Amazon S3 funciona.

Exemplos de uso

Considerando os benefícios do Amazon S3 para armazenamento, é possívelria usar esse serviço para armazenar arquivos e conjuntos de dados para uso com instâncias do EC2. Há várias maneiras de mover dados do Amazon S3 para suas instâncias e vice-versa. Além dos exemplos discutidos a seguir, há várias ferramentas escritas por pessoas que é possível usar para acessar seus dados no Amazon S3, no computador ou na instância. Algumas das mais comuns são discutidas nos fóruns de discussão da AWS.

Se você tiver permissão, poderá copiar um arquivo entre o Amazon S3 e sua instância usando um dos seguintes métodos.

GET or wget (Linux)

> **Note**
>
> Esse método funciona apenas para objetos públicos. Se o objeto não for público, você receberá uma mensagem `ERROR 403: Forbidden`. Se receber esse erro, será necessário usar o console do Amazon S3, a AWS CLI, a API da AWS, o AWS SDK ou AWS Tools for Windows PowerShell e é necessário ter as permissões necessárias. Para mais informações, consulte Gerenciamento de identidade e acesso no Amazon S3 e Fazer download de um objeto no Guia do usuário do Amazon S3.

O utilitário wget é um cliente FTP e HTTP que permite a você fazer download de objetos públicos no Amazon S3. Por padrão, ele é armazenado no Linux da Amazon e na maioria de outras distribuições e está disponível para download no Windows. Para fazer download de um objeto do Amazon S3, use o comando a seguir substituindo a URL do objeto para download.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

As instâncias do Windows têm o benefício de um navegador gráfico que pode ser usado para acessar o console do Amazon S3 diretamente. No entanto, para fins de script, os usuários do Windows também podem usar o AWS Tools for Windows PowerShell para mover objetos para/do Amazon S3.

Use o seguinte comando para copiar um objeto do Amazon S3 em sua instância do Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

A AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS. A AWS CLI permite que os usuários se autentiquem e baixem itens restritos no Amazon S3 e também façam upload de itens. Para obter mais informações sobre, por exemplo, como instalar e configurar as ferramentas, consulte a página de detalhes do AWS Command Line Interface.

O comando aws s3 cp é semelhante ao comando Unix cp. É possível copiar arquivos do Amazon S3 para sua instância, copiar arquivos de sua instância para o Amazon S3, e copiar arquivos de um local do Amazon S3 para outro.

Use o comando a seguir para copiar um objeto do Amazon S3 em sua instância.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Use o comando a seguir para copiar um objeto de sua instância de volta para o Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

O comando aws s3 sync pode sincronizar um bucket inteiro do Amazon S3 com um diretório local. Isso pode ser útil para fazer download de um banco de dados e manter a cópia local atualizada com o banco remoto. Se tiver as permissões adequadas no bucket do Amazon S3, será possível enviar o backup do diretório local por push para a nuvem quando concluir invertendo os locais de origem e de destino no comando.

Use o seguinte comando para fazer download de todo o bucket do Amazon S3 para um diretório local em sua instância.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Se você for um desenvolvedor, poderá usar uma API para acessar dados no Amazon S3. Você pode usar essa API para ajudar a desenvolver sua aplicação e integrá-la com outras APIs e SDKs. Para obter mais informações, consulte Exemplos de código do Amazon S3 usando SDKs da AWS no Guia do usuário do Amazon S3.

Uso do Amazon EFS com instâncias do Linux

> **Note**
>
> O Amazon EFS não é compatível com instâncias do Windows.

O Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. É possível usar um sistema de arquivos de EFS como uma fonte de dados comum para workloads e aplicativos em execução em várias instâncias. Para obter mais informações, consulte a página do produto Amazon Elastic File System.

Este tutorial demonstra como criar e anexar um sistema de arquivos do Amazon EFS ao usar o assistente de criação rápida do Amazon EFS durante a inicialização da instância. Para obter um tutorial sobre como criar um sistema de arquivos usando o console do Amazon EFS, consulte Getting started with Amazon Elastic File System (Conceitos básicos do Amazon Elastic File System) no Guia do usuário do Amazon Elastic File System.

> **Note**
>
> Quando você cria um sistema de arquivos do EFS usando a Criação rápida do EFS, o sistema de arquivos é criado com as seguintes configurações recomendadas de serviço:
>
> - Backups automáticos habilitados.
> - Destinos de montagem em cada sub-rede padrão na VPC selecionada.
> - Modo de desempenho de uso geral.
> - Modo de throughput intermitente.
> - Criptografia de dados em repouso habilitada usando a chave padrão para o Amazon EFS (`aws/elasticfilesystem`).
> - Gerenciamento do ciclo de vida do Amazon EFS habilitado com uma política de 30 dias.

Tarefas

- Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS
- Testar o sistema de arquivos do EFS
- Excluir o sistema de arquivos do EFS

Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS

É possível criar um sistema de arquivos do EFS e montá-lo na instância ao iniciar a instância usando o recurso de criação rápida do Amazon EFS do assistente de execução de instâncias do Amazon EC2.

Para criar um sistema de arquivos do EFS usando a Criação Rápida do Amazon EFS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Iniciar instância.
3. (Opcional) Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha um sistema operacional Linux e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon [AMI]), selecione uma AMI do Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância ou mantenha o padrão.
6. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
7. Em Network settings (Configurações de rede), escolha Edit (Editar) à direita e, para Subnet (Sub-rede), selecione uma sub-rede.

   > **Note**
   >
   > É necessário selecionar uma sub-rede antes de adicionar um sistema de arquivos do EFS.

8. Em Configure storage (Configurar armazenamento), escolha Edit (Editar) no canto inferior direito e realize estas etapas:

   a. Em Sistemas de arquivos, certifique-se de que EFS esteja selecionado e, em seguida, escolha Criar sistema de arquivos compartilhado.

   b. Em Nome do sistema de arquivos, insira um nome para o sistema de arquivos do Amazon EFS e, em seguida, escolha Criar sistema de arquivos.

   c. Em Ponto de montagem, especifique um ponto de montagem personalizado ou mantenha o padrão.

d. Para habilitar o acesso ao sistema de arquivos, selecione Automatically create and attach security groups (Criar e anexar grupos de segurança automaticamente). Ao selecionar esta caixa de seleção, os seguintes grupos de segurança serão automaticamente criados e anexados à instância e aos destinos de montagem do sistema de arquivos:

   - Grupo de segurança da instância: inclui uma regra de saída que permite o tráfego pela porta NFS 2049, mas não inclui regras de entrada.
   - Grupo de segurança de destinos de montagem do sistema de arquivos: contém uma regra de entrada que permite o tráfego pela porta NFS 2049 proveniente do grupo de segurança da instância (descrito acima) e uma regra de saída que permite o tráfego pela porta NFS 2049.

   > **Note**
   >
   > Como alternativa, é possível criar e anexar os grupos de segurança de forma manual. Para criar e anexar manualmente os grupos de segurança, desmarque Automatically create and attach the required security groups (Criar e anexar automaticamente os grupos de segurança necessários).

e. Para montar automaticamente o sistema de arquivos compartilhado quando a instância for iniciada, selecione Automatically mount shared file system by attaching required user data script (Montar automaticamente o sistema de arquivos compartilhado anexando o script de dados do usuário necessário). Para visualizar os dados do usuário gerados automaticamente, expanda Advanced details (Detalhes avançados) e role para baixo até User data (Dados do usuário).

   > **Note**
   >
   > Se você adicionou dados do usuário antes de selecionar esta caixa de seleção, os dados do usuário originais serão substituídos pelos dados do usuário gerados automaticamente.

9. Defina outras configurações da instância, conforme necessário.
10. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para ter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta.

Testar o sistema de arquivos do EFS

É possível se conectar à instância e verificar se o sistema de arquivos está montado no diretório especificado (por exemplo, /mnt/efs).

Para verificar se o sistema de arquivos está montado

1. Conecte-se à sua instância. Para ter mais informações, consulte Conecte-se à sua instância do Linux.
2. Na janela do terminal da instância, execute o comando df -T para verificar se o sistema de arquivos do EFS está montado.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

O nome do sistema de arquivos, mostrado na saída do exemplo como *efs-dns*, tem a seguinte forma.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Opcional) Crie um arquivo no sistema de arquivos com base na instância e verifique se é possível visualizar o arquivo por outra instância.

   a. Na instância, execute o seguinte comando para criar o arquivo.

   ```
   $ sudo touch /mnt/efs/test-file.txt
   ```

   b. Na outra instância, execute o comando a seguir para visualizar o arquivo.

   ```
   $ ls /mnt/efs
   test-file.txt
   ```

Excluir o sistema de arquivos do EFS

Se não precisar mais do arquivo de sistemas, você poderá excluí-lo.

Para excluir o sistema de arquivos

1. Abra o console do Amazon Elastic File System em https://console.aws.amazon.com/efs/.
2. Selecione o sistema de arquivos a ser excluído.
3. Escolha Actions (Ações), Delete file system (Excluir sistema de arquivos).
4. Quando a confirmação for solicitada, insira o ID do sistema de arquivos e escolha Delete file system (Excluir sistema de arquivos).

Use o Amazon FSx com o Amazon EC2

A família de serviços Amazon FSx facilita a inicialização, a execução e a escala do armazenamento compartilhado alimentado por sistemas de arquivos comerciais e de código aberto populares. É possível usar o novo assistente de inicialização de instância para anexar automaticamente os seguintes tipos de sistemas de arquivos Amazon FSx às suas instâncias do Amazon EC2 na inicialização:

- O Amazon FSx for NetApp ONTAP fornece armazenamento compartilhado totalmente gerenciado na Nuvem AWS com os recursos populares de acesso e gerenciamento de dados do NetApp ONTAP.
- O Amazon FSx for OpenZFS fornece armazenamento compartilhado econômico e totalmente gerenciado, alimentado pelo popular sistema de arquivos OpenZFS.

> **Note**
>
> - Essa funcionalidade está disponível somente no novo assistente de inicialização de instância. Para obter mais informações, consulte Iniciar uma instância usando o novo assistente de inicialização de instância, versão beta
> - Os sistemas de arquivos do Amazon FSx para Windows File Server e Amazon FSx para Lustre não podem ser montados na inicialização. É necessário montar esses sistemas de arquivos manualmente após a inicialização.

É possível escolher montar um sistema de arquivos existente criado anteriormente ou criar um novo sistema de arquivos para montar em uma instância na inicialização.

Tópicos

- Script de dados do usuário e de grupos de segurança
- Montar um sistema de arquivos Amazon FSx na inicialização

Script de dados do usuário e de grupos de segurança

Quando você monta um sistema de arquivos Amazon FSx em uma instância usando o assistente de inicialização de instância, é possível escolher se deseja criar e anexar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos e se deseja incluir automaticamente os scripts de dados do usuário necessários para montar o sistema de arquivos e torná-lo disponível para uso.

Tópicos

- Grupos de segurança
- Script de dados do usuário

Grupos de segurança

Se você optar por criar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos, o assistente de inicialização de instância criará e anexará dois grupos de segurança: um é anexado à instância e o outro é anexado ao sistema de arquivos. Para obter mais informações sobre os requisitos do grupo de segurança, consulte Controle de acesso do sistema de arquivos FSx for ONTAP com Amazon VPC e Controle de acesso do sistema de arquivos FSx for OpenZFS com Amazon VPC.

Adicionamos a etiqueta `Name=instance-sg-1` ao grupo de segurança que é criado e anexado à instância. O valor na etiqueta é incrementado automaticamente toda vez que o assistente de execução de instância cria um grupo de segurança para sistemas de arquivos do Amazon FSx.

O grupo de segurança inclui as regras de saída a seguir, mas nenhuma regra de entrada.

Regras de saída

Tipo de protocolo	Número da porta	Destination (Destino)
UDP	111	*grupo de segurança do sistema de arquivos*
UDP	20001 - 20003	*grupo de segurança do sistema de arquivos*
UDP	4049	*grupo de segurança do sistema de arquivos*
UDP	2049	*grupo de segurança do sistema de arquivos*
UDP	635	*grupo de segurança do sistema de arquivos*
UDP	4045 - 4046	*grupo de segurança do sistema de arquivos*
TCP	4049	*grupo de segurança do sistema de arquivos*
TCP	635	*grupo de segurança do sistema de arquivos*
TCP	2049	*grupo de segurança do sistema de arquivos*
TCP	111	*grupo de segurança do sistema de arquivos*
TCP	4045 - 4046	*grupo de segurança do sistema de arquivos*
TCP	20001 - 20003	*grupo de segurança do sistema de arquivos*

Tipo de protocolo	Número da porta	Destination (Destino)
Todos	Todos	*grupo de segurança do sistema de arquivos*

O grupo de segurança criado e anexado ao sistema de arquivos é marcado com `Name=fsx-sg-`*1*. O valor na etiqueta é incrementado automaticamente toda vez que o assistente de execução de instância cria um grupo de segurança para sistemas de arquivos do Amazon FSx.

O grupo de segurança inclui as regras a seguir.

Regras de entrada

Tipo de protocolo	Número da porta	Origem
UDP	2049	*security group da instância*
UDP	20001 - 20003	*security group da instância*
UDP	4049	*security group da instância*
UDP	111	*security group da instância*
UDP	635	*security group da instância*
UDP	4045 - 4046	*security group da instância*
TCP	4045 - 4046	*security group da instância*
TCP	635	*security group da instância*
TCP	2049	*security group da instância*
TCP	4049	*security group da instância*
TCP	20001 - 20003	*security group da instância*
TCP	111	*security group da instância*

Regras de saída

Tipo de protocolo	Número da porta	Destination (Destino)
Todos	Tudo	0.0.0.0/0

Script de dados do usuário

Se você optar por anexar automaticamente scripts de dados do usuário, o assistente de inicialização de instância adicionará os seguintes dados do usuário à instância. Este script instala os pacotes necessários, monta o sistema de arquivos e atualiza as configurações da instância para que o sistema de arquivos seja remontado automaticamente sempre que a instância for reiniciada.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Montar um sistema de arquivos Amazon FSx na inicialização

Para montar um sistema de arquivos Amazon FSx novo ou existente na inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch instance (Iniciar instância) para abrir o assistente de inicialização de instância.
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a AMI a ser usada.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância.
5. Na seção Key pair (Par de chaves), selecione um par de chaves existente ou crie um novo.
6. Na seção Network settings (Configurações da rede), faça o seguinte:

    a. Selecione a opção Editar.

    b. Se você deseja montar um sistema de arquivos existente, para Subnet (Sub-rede), escolha a sub-rede preferida do sistema de arquivos. Recomendamos que você execute a instância na mesma zona de disponibilidade da sub-rede preferencial do sistema de arquivos para otimizar a performance.

    Se você deseja criar um novo sistema de arquivos para montar em uma instância, para Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância.

    > **Important**
    >
    > É necessário selecionar uma sub-rede para habilitar a funcionalidade do Amazon FSx no novo assistente de inicialização de instância. Se você não selecionar uma sub-rede, não poderá montar um sistema de arquivos existente ou criar um novo.

7. Na seção Storage (Armazenamento), faça o seguinte:

    a. Configure os volumes conforme necessário.

    b. Expanda a seção File systems (Sistemas de arquivos) e selecione FSx.

    c. Selecione Add shared file system (Adicionar sistema de arquivos compartilhado).

    d. Para File system (Sistema de arquivos), selecione o sistema de arquivos a ser montado.

    > **Note**
    >
    > A lista exibe todos os sistemas de arquivos do Amazon FSx para NetApp ONTAP e Amazon FSx para OpenZFS na sua conta na região selecionada.

    e. Para criar e anexar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos, selecione Automatically create and attach security groups

(Criar e anexar grupos de segurança automaticamente). Se você preferir criar os grupos de segurança manualmente, desmarque a caixa de seleção. Para ter mais informações, consulte Grupos de segurança.

f. Para anexar automaticamente os scripts de dados do usuário necessários para montar o sistema de arquivos, selecione Automatically mount shared file system by attaching required user data script (Montar automaticamente o sistema de arquivos compartilhados anexando o script de dados do usuário necessário). Se você preferir fornecer os scripts de dados do usuário manualmente, desmarque a caixa de seleção. Para ter mais informações, consulte Script de dados do usuário.

8. Na seção Advanced (Avançado), defina as configurações de instância adicionais conforme necessário.
9. Escolha Executar.

Usar o Amazon File Cache com o Amazon EC2

O Amazon File Cache é um cache de alta velocidade totalmente gerenciado na AWS, que é usado para processar dados de arquivos, independentemente do local em que os dados estão armazenados. O Amazon File Cache serve como um local temporário e de alto desempenho para armazenamento de dados que ficam em sistemas de arquivos on-premises, sistemas de arquivos da AWS e buckets do Amazon Simple Storage Service (Amazon S3). Você pode usar esse recurso a fim de disponibilizar conjuntos de dados dispersos para aplicações baseadas em arquivos na AWS com uma visão unificada e altas velocidades (latências inferiores a um milissegundo e alto throughput). Para obter mais informações, consulte O que é o Amazon File Cache?.

Você pode acessar seu cache por meio de suas instâncias do Amazon EC2 usando o cliente de código aberto Lustre. As instâncias do Amazon EC2 podem acessar seu cache por meio de outras zonas de disponibilidade na mesma Amazon Virtual Private Cloud (Amazon VPC), desde que sua rede permita o acesso entre sub-redes na VPC. Depois que seu cache estiver montado, você poderá trabalhar com os arquivos e diretórios da mesma forma que trabalha ao usar um sistema local de arquivos.

Para começar, consulte Introdução ao Amazon File Cache.

Limites de volumes de instância

O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Ao considerar quantos volumes adicionar à sua instância, é

necessário avaliar se uma maior largura de banda de E/S ou maior capacidade de armazenamento são necessárias.

Largura de banda x capacidade

Para casos de uso de largura de banda consistentes e previsíveis, use instâncias otimizadas para Amazon EBS com volumes SSD de finalidade geral ou volumes SSD com IOPS provisionadas. Para obter o máximo de performance, faça a correspondência entre as IOPS provisionadas para seus volumes e a largura de banda disponível para o tipo da instância.

Para configurações de RAID, talvez você ache que matrizes com mais de 8 volumes prejudicam a performance devido à maior sobrecarga de E/S. Teste a performance de aplicações individuais e ajuste, se necessário.

Tópicos

- Limites de volume para instâncias criadas no Nitro System
- Limites de volume para instâncias baseadas em Xen

Limites de volume para instâncias criadas no Nitro System

Tópicos

- Limite de volume dedicado do Amazon EBS
- Limite de volume compartilhado do Amazon EBS

Limite de volume dedicado do Amazon EBS

Os tipos de instância do Nitro, apresentados a seguir, têm um limite de volume dedicado do Amazon EBS que varia dependendo do tamanho da instância. O limite não é compartilhado com outros anexos do dispositivo. Em outras palavras, é possível anexar qualquer número de volumes do Amazon EBS até o limite de anexação de volume, independentemente do número de dispositivos conectados, como volumes de armazenamento de instâncias NVMe e interfaces de rede.

- Uso geral: M7a, M7i e M7i-flex
- Otimizada para computação: C7a, C7i
- Otimizadas para memória: R7a, R7i, R7iz

Para esses tipos de instância que oferecem suporte a limites de volume dedicados, os limites de volume dependem do tamanho da instância. A tabela a seguir mostra o limite para cada tamanho de instância.

Tamanho da instância	Limite de volume
`medium | large | xlarge | 2xlarge | 4xlarge | 8xlarge | 12xlarge`	32
`16xlarge`	48
`24xlarge`	64
`32xlarge`	88
`48xlarge`	128
`metal-16xl | metal-24xl`	39
`metal-32xl | metal-48xl`	79

Limite de volume compartilhado do Amazon EBS

Todos os outros tipos de instância do Nitro (não listados em Limite de volume dedicado do Amazon EBS) têm um limite de anexo de volume que é compartilhado entre os volumes do Amazon EBS, as interfaces de rede e os volumes de armazenamento de instância para NVMe. É possível anexar qualquer número de volumes do Amazon EBS até esse limite, menos o número de interfaces de rede conectadas e os volumes de armazenamento de instâncias NVMe. Lembre-se de que cada instância deve ter pelo menos uma interface de rede e que os volumes de armazenamento de instâncias NVMe são anexados automaticamente na inicialização.

A maioria dessas instâncias oferece suporte a um máximo de 28 anexos. Por exemplo, você não tiver anexos de interface de rede adicionais em uma instância `m5.xlarge`, será possível anexar até 27 volumes do EBS (limite de 28 volumes - 1 interface de rede). Se você tiver duas interfaces de rede adicionais em uma instância `m5.xlarge`, será possível anexar até 25 volumes do EBS

(limite de 28 volumes - 3 interfaces de rede). Da mesma forma, se você tiver duas interfaces de rede adicionais em uma instância `m5d.xlarge`, a qual tem 1 volume de armazenamento de instâncias NVMe, será possível anexar até 24 volumes EBS (limite de 28 volumes - 3 interfaces de rede - 1 volume de armazenamento de instância NVMe).

Veja a seguir as exceções para os tipos de instância que têm limites de volume compartilhados:

- As instâncias DL2q comportam até 19 volumes do EBS.
- A maioria das instâncias bare metal oferece suporte a um máximo de 31 volumes do EBS.
- As instâncias virtualizadas de alta memória oferecem suporte a um máximo de 27 volumes do EBS.
- As instâncias bare metal de alta memória oferecem suporte a um máximo de 19 volumes do EBS.
- As instâncias `inf1.xlarge` e `inf1.2xlarge` oferecem suporte a um máximo de 26 volumes do EBS.
- As instâncias `inf1.6xlarge` oferecem suporte a um máximo de 23 volumes do EBS.
- `mac1.metal` As instâncias oferecem suporte a um máximo de 16 volumes do EBS.
- As instâncias `mac2.metal`, `mac2-m2.metal` e `mac2-m2pro.metal` são compatíveis com até 10 volumes do EBS.
- As instâncias `inf1.24xlarge` oferecem suporte a um máximo de 11 volumes do EBS.
- As instâncias `g5.48xlarge` são compatíveis com um máximo de 9 volumes do EBS.
- As instâncias `d3.8xlarge` e `d3en.12xlarge` oferecem suporte a um máximo de 3 volumes do EBS.
- Para instâncias com computação acelerada, os aceleradores conectados são contabilizados para o limite de volume compartilhado. Por exemplo, para instâncias `p4d.24xlarge`, as quais têm um limite de volume compartilhado de 28, 8 GPUs e 8 volumes de armazenamento de instâncias NVMe, é possível anexar até 11 volumes do Amazon EBS (limite de 28 volumes - 1 interface de rede - 8 GPUs - 8 volumes de armazenamento de instâncias NVMe).

Limites de volume para instâncias baseadas em Xen

Instâncias do Linux

Anexar mais de 40 volumes a uma instância do Linux baseada em Xen pode causar falhas na inicialização. Esse número inclui o volume raiz, mais os volumes do Amazon EBS e os volumes de armazenamento de instâncias anexados.

Em caso de problemas de inicialização em uma instância com um grande número de volumes, interrompa a instância, desanexe todos os volumes que não são essenciais ao processo de inicialização, inicie a instância e anexe novamente os volumes depois que a instância estiver em execução.

> **Important**
>
> A anexação de mais de 40 volumes a uma instância do Linux baseada em Xen ocorre somente em uma base de melhor esforço e não é garantida.

Instâncias do Windows

A tabela a seguir mostra os limites de volumes para instâncias do Windows baseadas em Xen em função do driver usado. Esses números incluem o volume raiz, mais quaisquer volumes do Amazon EBS e volumes de armazenamento de instâncias anexados.

> **Important**
>
> A anexação de um número de volumes superior ao a seguir a uma instância do Windows baseada em Xen ocorre somente em uma base de melhor esforço e não é garantida.

Driver	Solicitação de volume
AWS PV	26
Citrix PV	26
Red Hat PV	17

Não recomendamos anexar mais de 26 volumes a uma instância do Windows baseada em Xen com drivers AWS PV ou Citrix PV, pois é provável que isso cause problemas de performance. Para determinar quais drivers PV sua instância está usando ou atualizar sua instância do Windows do Red Hat para drivers Citrix PV, consulte the section called “Atualizar drivers de PV”.

Para obter mais informações sobre como os nomes dos dispositivos estão relacionados a volumes, consulte Mapear discos para volumes na sua instância do Windows.

Volume raiz da instância do Amazon EC2

Quando você inicia uma instância, um volume raiz é criado para ela. O volume raiz contém a imagem usada para inicializar a instância. Cada instância tem um único volume raiz. É possível adicionar volumes de armazenamento às instâncias durante ou após a inicialização.

Reservamos nomes de dispositivos específicos para os volumes raízes. Para ter mais informações, consulte Nomes de dispositivos em instâncias do Amazon EC2.

Conteúdo

- Tipo do volume de raiz
- Escolha de uma AMI do Linux por tipo de volume raiz
- Determinação do tipo de dispositivo raiz da instância do Linux
- Alterar o volume raiz para persistir
- Alterar o tamanho inicial do volume raiz
- Substituir o volume raiz de uma instância do EC2

Tipo do volume de raiz

A AMI usada para iniciar uma instância determina o tipo de volume raiz. É possível iniciar uma instância usando uma AMI baseada no Amazon EBS (instâncias do Linux e do Windows) ou uma AMI baseada no armazenamento de instância (somente para instâncias do Linux). Existem diferenças significativas quanto ao que é possível fazer com cada tipo de AMI. Para obter mais informações sobre essas diferenças, consulte Armazenamento para o dispositivo raiz.

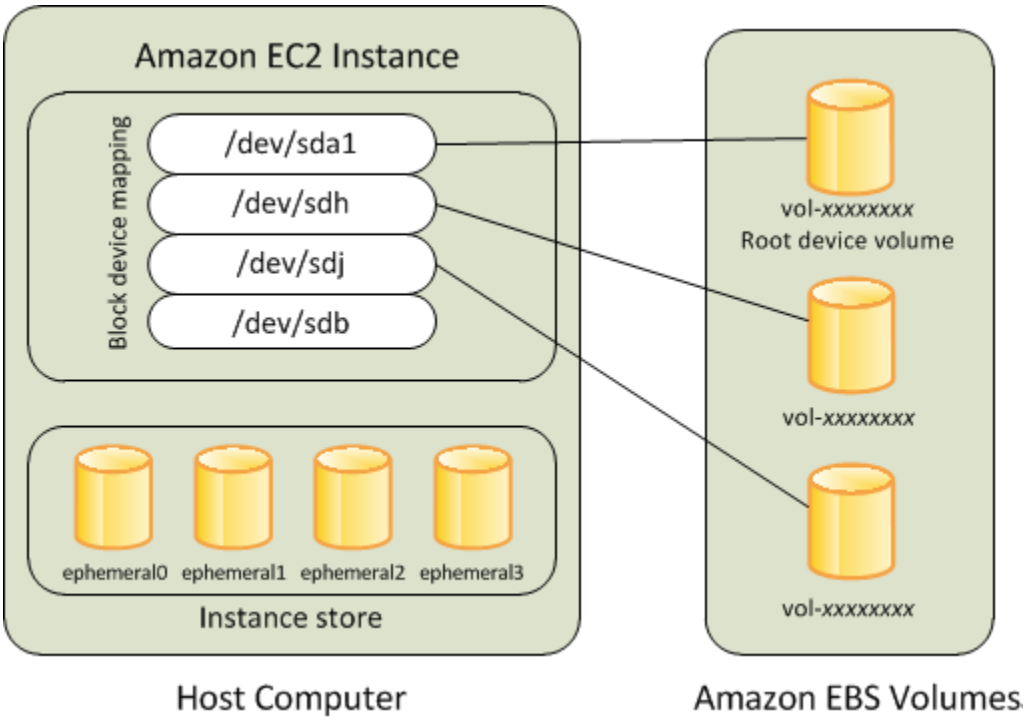
Recomendamos que você use AMIs baseadas no Amazon EBS, pois elas são iniciadas mais rapidamente e usam armazenamento persistente.

Instâncias baseadas no Amazon EBS

As instâncias que usam o Amazon EBS para o volume raiz automaticamente têm um volume do Amazon EBS associado. Quando você executa uma instância baseada no Amazon EBS, criamos um volume do Amazon EBS para cada snapshot do Amazon EBS mencionado pela AMI que você usa. Também é possível usar outros volumes do Amazon EBS ou volumes de armazenamento de instâncias, dependendo do tipo de instância.

Uma instância baseada no Amazon EBS pode ser interrompida e posteriormente reiniciada sem afetar os dados armazenados nos volumes associados. Há várias tarefas relacionadas a instâncias

e volumes que é possível realizar quando uma instância baseada no Amazon EBS estiver em estado interrompido. Por exemplo, é possível modificar as propriedades da instância, alterar seu tamanho ou atualizar o kernel que está usando ou é possível associar o volume o raiz a uma instância em execução diferente para depuração ou qualquer outra finalidade. Para obter mais informações, consulte Volumes do Amazon EBS.



Limitação

Você não pode usar os volumes `st1` ou `sc1` do EBS como volumes raízes.

Falha de instância

Se uma instância baseada no Amazon EBS falhar, será possível restaurar sua sessão seguindo um dos seguintes métodos:

- Pare e reinicie (teste esse método primeiro).
- Faça automaticamente o snapshot de todos os volumes relevantes e crie uma nova AMI. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
- Associe o volume à nova instância seguindo estas etapas:
  1. Crie um snapshot de novo volume raiz.
  2. Registre a nova AMI usando o snapshot.
  3. Execute uma nova instância a partir da nova AMI.

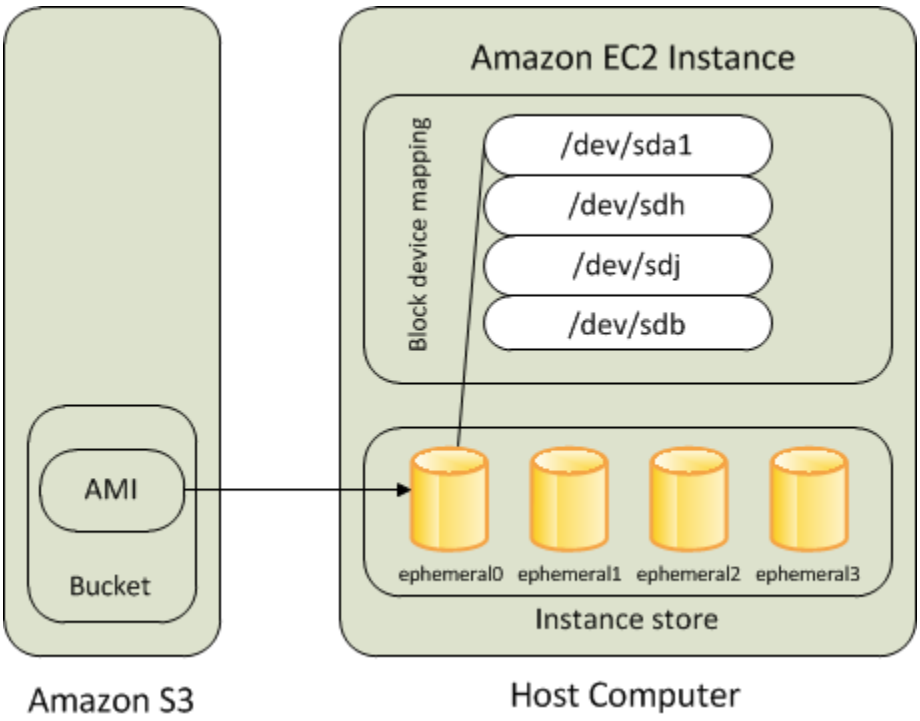
4. Separe os volumes do Amazon EBS restantes da instância antiga.
5. Reassocie os volumes do Amazon EBS à nova instância.

Instâncias baseadas no armazenamento de instância (somente para instâncias do Linux)

> **Note**
>
> As instâncias do Windows não são compatíveis com volumes raiz baseados no armazenamento de instância.

As instâncias que usam armazenamentos de instância para o volume raiz automaticamente têm um ou mais volumes de armazenamento de instância disponíveis, sendo que um volume serve como volume raiz. Quando uma instância é executada, a imagem usada para inicializá-la é copiada para o volume do dispositivo raiz. Observe que você também usar volumes adicionais de armazenamento de instâncias, dependendo do tipo de instância.

Todos os dados nos volumes de armazenamento de instâncias são mantidos desde que a instância esteja em execução, mas esses dados serão excluídos quando a instância for encerrada (instâncias com armazenamento de instâncias não oferecem suporte à ação Stop (Interromper)) ou se ela falhar (por exemplo, se uma unidade subjacente tiver problemas). Para ter mais informações, consulte Armazenamento de instâncias do Amazon EC2.



Requisito

Somente os seguintes tipos de instância são compatíveis com um volume de armazenamento de instância como o volume raiz: C3, D2, I2, M3 e R3.

Falha de instância

Após uma instância com armazenamento de instâncias falhar ou ser encerrada, ela não poderá ser restaurada. Se você planeja usar as instâncias baseadas em armazenamento de instâncias no Amazon EC2, recomendamos enfaticamente que distribua os dados nos seus armazenamentos de instâncias através de várias zonas de disponibilidade. Você também deve fazer backup dos dados críticos dos volumes de armazenamento de instâncias para o armazenamento persistente regularmente.

Escolha de uma AMI do Linux por tipo de volume raiz

> **Note**
>
> Todas as AMIs do Windows são baseadas no EBS.

A AMI que você especifica ao executar a instância determina o tipo de volume de dispositivo raiz que sua instância tem. É possível visualizar AMIs por tipo de dispositivo raiz usando um dos métodos a seguir.

Console

Para selecionar uma AMI baseada no Amazon EBS usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione AMIs.
3. Nas listas de filtros, selecione o tipo de imagem (por exemplo, Public images (Imagens públicas)). Na barra de pesquisa, escolha Plataforma para selecionar o sistema operacional (por exemplo, o Amazon Linux) e Tipo de dispositivo raiz para selecionar o tipo de volume raiz (ebs ou armazenamento de instância).
4. (Opcional) Para obter informações adicionais para ajudar você a fazer sua escolha, selecione o ícone de Preferências, alterne as colunas a serem exibidas e escolha Confirmar.
5. Escolha uma AMI e anote seu ID da AMI.

AWS CLI

Para verificar o tipo de volume do dispositivo raiz de uma AMI usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Determinação do tipo de dispositivo raiz da instância do Linux

> **Note**
>
> Todas as instâncias do Windows são baseadas no EBS.

É possível visualizar o tipo de dispositivo raiz da instância do Linux usando um dos métodos apresentados a seguir.

Console

Para determinar o tipo de dispositivo raiz de uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Na guia Storage (Armazenamento), em Root device details (Detalhes do dispositivo raiz), verifique o valor de Root device type (Tipo de dispositivo raiz), da seguinte maneira:
   - Se o valor for `EBS`, essa será uma instância com Amazon EBS.
   - Se o valor for `INSTANCE-STORE`, essa será uma instância com armazenamento de instâncias.

AWS CLI

Para determinar o tipo de dispositivo raiz de uma instância usando a linha de comando

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Alterar o volume raiz para persistir

Por padrão, o volume raiz de uma AMI com Amazon EBS é excluído quando a instância é encerrada. É possível alterar o comportamento padrão para garantir que o volume persista após a interrupção da instância. Para alterar o comportamento padrão, defina o atributo `DeleteOnTermination` como `false` usando um mapeamento de dispositivos de blocos.

Tarefas

- Configurar o volume raiz para persistir durante a execução da instância
- Configurar o volume raiz para persistir em uma instância existente
- Confirmar que um volume raiz está configurado para persistir

Configurar o volume raiz para persistir durante a execução da instância

É possível configurar o volume raiz para persistir ao executar uma instância usando o console do Amazon EC2 ou as ferramentas da linha de comando.

Console

Como configurar o volume raiz para persistir ao executar uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
3. Escolha uma imagem de máquina da Amazon (AMI), um tipo de instância e um par de chaves e defina suas configurações de rede.
4. Em Configurar armazenamento, escolha Avançado.
5. Expanda o volume raiz.
6. Em Excluir no encerramento, escolha Não.
7. Ao concluir a configuração da instância, escolha Executar instância.

AWS CLI

Como configurar o volume raiz para persistir ao executar uma instância usando o AWS CLI

Use o comando run-instances e inclua um mapeamento de dispositivo de bloco que define o atributo `DeleteOnTermination` como `false`.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

Especifique o seguinte em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
```

```
]
```

Tools for Windows PowerShell

Como configurar o volume raiz para persistir ao executar uma instância usando o Tools for Windows PowerShell

Use o comando New-EC2Instance e inclua um mapeamento de dispositivo de bloco que define o atributo `DeleteOnTermination` como `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
 $bdm ...other parameters...
```

Configurar o volume raiz para persistir em uma instância existente

É possível configurar o volume raiz para persistir em uma instância em execução usando apenas as ferramentas da linha de comando.

AWS CLI

Como configurar o volume raiz para persistir em uma instância existente usando o AWS CLI

Use o comando modify-instance-attribute com um mapeamento de dispositivo de blocos que define o atributo `DeleteOnTermination` como `false`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

Especifique o seguinte em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
```

```
        }
    }
]
```

Tools for Windows PowerShell

Como configurar o volume raiz para persistir em uma instância existente usando o AWS Tools for Windows PowerShell

Use o comando Edit-EC2InstanceAttribute com um mapeamento de dispositivo de blocos que define o atributo `DeleteOnTermination` como `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
 $bdm
```

Confirmar que um volume raiz está configurado para persistir

É possível confirmar que um volume raiz está configurado para persistir usando o console do Amazon EC2 ou as ferramentas da linha de comando.

Console

Como confirmar se um volume raiz está configurado para persistir usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Storage (Armazenamento), em Block devices (Dispositivos de blocos), localize a entrada do volume raiz. Se a opção Delete on termination (Excluir ao encerrar) for No, o volume será configurado para persistir.

AWS CLI

Como confirmar que um volume raiz está configurado para persistir usando o AWS CLI

Use o comando describe-instances e verifique se o atributo `DeleteOnTermination` no elemento de resposta `BlockDeviceMappings` está definido como `false`.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
        }
    }
...
```

Tools for Windows PowerShell

Como confirmar que um volume raiz está configurado para persistir usando o AWS Tools for Windows PowerShell

Use o Get-EC2Instance e verifique se o atributo `DeleteOnTermination` no elemento de resposta `BlockDeviceMappings` está definido como `false`.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Alterar o tamanho inicial do volume raiz

Por padrão, o tamanho do volume raiz é determinado pelo tamanho do snapshot. É possível aumentar o tamanho inicial do volume raiz usando o mapeamento de dispositivos de blocos da instância da seguinte forma.

1. Determine o nome do dispositivo do volume raiz especificado na AMI, conforme descrito em Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI.
2. Confirme o tamanho do snapshot especificado no mapeamento de dispositivos de blocos da AMI.

3. Substitua o tamanho do volume raiz usando o mapeamento de dispositivos de blocos da instância, conforme descrito em Atualizar o mapeamento de dispositivos de blocos ao executar uma instância, especificando um tamanho de volume maior que o tamanho do snapshot.

Por exemplo, a entrada a seguir para o mapeamento de dispositivos de blocos da instância aumenta o tamanho do volume raiz `/dev/xvda` para 100 GiB. É possível omitir o ID do snapshot no mapeamento de dispositivos de blocos da instância porque o ID do snapshot já está especificado no mapeamento do dispositivos de blocos da AMI.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para ter mais informações, consulte Mapeamentos de dispositivos de blocos.

Substituir o volume raiz de uma instância do EC2

O Amazon EC2 permite que você substitua o volume raiz do Amazon EBS por uma instância em execução retendo o seguinte:

- Dados armazenados em volumes de armazenamento de instâncias: os volumes de armazenamento de instâncias permanecem anexados à instância após a restauração do volume raiz.
- Dados armazenados em volumes de dados (não raiz) do Amazon EBS: os volumes não raiz do Amazon EBS permanecem anexados à instância após a restauração do volume raiz.
- Configuração de rede — Todas as interfaces de rede permanecem conectadas à instância e mantêm seus endereços IP, identificadores e IDs de anexo. Quando a instância fica disponível, todo o tráfego de rede pendente é liberado. Além disso, a instância permanece no mesmo host físico, portanto, mantém seus endereços IP públicos e privados e o nome DNS.
- Políticas do IAM — IAM os perfis e as políticas (como políticas baseadas em tags) associados à instância são mantidos e impostos.

Tópicos

- Como funciona?

- Substituir um volume raiz
- Exibir tarefas de substituição do volume raiz

Como funciona?

Quando você substitui o volume raiz de uma instância, um novo volume raiz (substituto) é restaurado de uma das seguintes maneiras:

- Para o estado inicial de execução: o volume é restaurado para seu estado inicial na execução da instância. Para ter mais informações, consulte Restaurar um volume raiz para seu estado de execução.
- Com base em um snapshot da mesma linhagem do volume raiz atual: isso permite corrigir problemas, como corrupção de volume raiz ou erros de configuração de rede do sistema operacional convidado. Para ter mais informações, consulte Substituir um volume raiz usando um snapshot.
- Com base em uma AMI com os mesmos atributos principais da instância: isso permite que você execute patches ou atualizações de sistemas operacionais e aplicativos. Para ter mais informações, consulte Substituir um volume raiz usando uma AMI.

O volume raiz original é desvinculado da instância e o novo volume raiz é anexado à instância em seu lugar. O mapeamento de dispositivos de blocos da instância é atualizado para refletir a ID do volume raiz substituto. Após a conclusão do processo de substituição do volume raiz, você pode escolher se deseja manter ou não o volume raiz original. Se você optar por excluir o volume raiz original após a conclusão do processo de substituição, o volume raiz original será automaticamente excluído e ficará irrecuperável. Se você optar por manter o volume raiz original após a conclusão do processo, o volume permanecerá provisionado em sua conta; você deverá excluí-lo manualmente quando não precisar mais dele.

Se a tarefa de substituição do volume raiz falhar, a instância será reinicializada e o volume raiz original permanecerá anexado à instância.

Considerações sobre a substituição do volume raiz

- A instância deve estar no estado `running`.
- A instância é reinicializada automaticamente durante o processo. O conteúdo da memória (RAM) é apagado durante a reinicialização. Não requer reinicializações manuais.

- Não é possível substituir o volume raiz se ele for um volume de armazenamento de instâncias. Só há compatibilidade com instâncias com volumes raiz do Amazon EBS.
- Você pode substituir o volume raiz de todos os tipos de instâncias virtualizadas e instâncias bare metal do EC2 Mac. Nenhum outro tipo de instância bare metal é compatível.
- Só é possível usar snapshots que pertencem à mesma linhagem que os volumes raiz anteriores da instância.
- Se sua conta estiver habilitada para Criptografia do Amazon EBS por padrão na região atual, o volume raiz de substituição criado pela tarefa de substituição do volume raiz será sempre criptografado, independentemente do status de criptografia do snapshot especificado ou do volume raiz da AMI especificada.
- A tabela a seguir resume os possíveis resultados da criptografia.

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
Restaurar o volume raiz substituto para o estado de execução inicial	Criptografado	Não aplicável	Não considerado	Criptografado	Mesma chave do KMS do volume raiz original
	Não criptografado	Não aplicável	Desabilitado	Não criptografado	Não aplicável
	Não criptografado	Não aplicável	Habilitado	Criptografado	Conta chave KMS padrão para criptografia do Amazon EBS
Restaurar o volume raiz	Criptografado	Não criptografado	Não considerado	Criptografado	Mesma chave do

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
de substituição a partir do snapshot ou da AMI					KMS do volume raiz original
	Criptografado	Criptografado	Não considerado	Criptografado	Mesma chave do KMS do volume raiz original
	Não criptografado	Não criptografado	Desabilitado	Não criptografado	Não aplicável
	Não criptografado	Não criptografado	Habilitado	Criptografado	Contaschave KMS padrão para criptografia do Amazon EBS

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
	Não criptografado	Criptografado	Não considerado	Criptografado	Se a AMI ou o snapshot pertencer à conta, o volume de substituição será criptografado com a chave do KMS da AMI ou do snapshot. Se a AMI ou o snapshot for compartilhados com a conta, o volume de substituição será criptografado com a chave do KMS padrão para criptografia do Amazon EBS da conta.

Tópicos

- Restaurar um volume raiz para seu estado de execução
- Substituir um volume raiz usando um snapshot
- Substituir um volume raiz usando uma AMI

Restaurar um volume raiz para seu estado de execução

Você pode realizar uma substituição do volume raiz que substitui o volume raiz de uma instância por um volume raiz substituto que é restaurado para o estado de execução do volume raiz original. O volume substituto é restaurado automaticamente com base no snapshot que foi usado para criar o volume original durante a execução da instância.

O volume raiz substituto obtém o mesmo tipo, tamanho e exclusão nos atributos de encerramento do volume raiz original.

Substituir um volume raiz usando um snapshot

Você pode realizar uma substituição do volume raiz que substitui o volume raiz de uma instância por um volume substituto que é restaurado com um snapshot específico. Isso permite restaurar o volume raiz de uma instância para um snapshot específico que você criou anteriormente com base nesse volume raiz.

O volume raiz substituto obtém o mesmo tipo, tamanho e exclusão nos atributos de encerramento do volume raiz original.

Considerações sobre o uso de um snapshot

- Só é possível usar snapshots que pertencem à mesma linhagem que o volume raiz atual da instância.
- Não é possível usar cópias de snapshots criadas de snapshots que foram tirados do volume raiz.
- Após restaurar o volume raiz com sucesso, ainda é possível usar os snapshots obtidos com base no volume raiz original para substituir o novo volume raiz (substituto).

Substituir um volume raiz usando uma AMI

Você pode realizar uma substituição do volume raiz usando uma AMI de sua propriedade ou uma AMI compartilhada com você. A AMI deve ter o mesmo código de produto, informações de cobrança, tipo de arquitetura e tipo de virtualização da instância.

Se a instância estiver habilitada para ENA ou sriov-net, você deverá usar uma AMI que ofereça suporte a esses recursos. Se a instância não estiver habilitada para ENA ou sriov-net, você poderá selecionar uma AMI que não inclua suporte para esses recursos ou adicionar suporte automaticamente se selecionar uma AMI compatível com ENA ou sriov-net.

Se a instância estiver habilitada para o NitroTPM, você deverá usar uma AMI que tenha o NitroTPM habilitado. O suporte ao NitroTPM não será habilitado se a instância não tiver sido configurada para ele, independentemente da AMI que você selecionar.

Você pode selecionar uma AMI com um modo de inicialização diferente do modo da instância, desde que a instância seja compatível com o modo de inicialização da AMI. Se a instância não for compatível com o modo de inicialização, a solicitação falhará. Se a instância for compatível com o modo de inicialização, o novo modo de inicialização será propagado para a instância e seus dados UEFI serão atualizados adequadamente. Se você tiver modificado a ordem de inicialização manualmente ou adicionado uma chave UEFI Secure Boot privada para carregar módulos privados do kernel, as alterações serão perdidas durante a substituição do volume raiz.

O volume raiz substituto obtém o mesmo tipo de volume e o mesmo atributo de exclusão ao encerrar do volume raiz original, e obtém o tamanho do mapeamento de dispositivos de blocos do volume raiz AMI.

> **Note**
>
> O tamanho do mapeamento de dispositivos de blocos de volume raiz da AMI deve ser igual ou maior que o tamanho do volume raiz original. Se o tamanho do mapeamento de dispositivos de blocos do volume raiz da AMI for menor que o tamanho do volume raiz original, a solicitação falhará.

Após a conclusão da tarefa de substituição do volume raiz, as seguintes informações novas e atualizadas são refletidas quando você descreve a instância usando o console, a AWS CLI ou AWS SDKs:

- ID da nova AMI
- ID de novo volume para o volume raiz
- Atualização da configuração do modo de inicialização (se alterada pela AMI)
- Atualização da configuração do NitroTPM (se habilitada pela AMI)

- Atualização da configuração do ENA (se habilitada pela AMI)
- Atualização da configuração de sriov-net (se habilitada pela AMI)

A ID da nova AMI também é refletida nos metadados da instância.

Considerações sobre o uso de uma AMI:

- Se você usar uma AMI que tenha vários mapeamentos de dispositivos de blocos, somente o volume raiz da AMI será usado. Os outros volumes (não raiz) serão ignorados.
- Você só poderá usar esse recurso se tiver permissões para a AMI e o respectivo snapshot de volume raiz associado. Não é possível usar esse recurso com AMIs do AWS Marketplace.
- Você só poderá usar uma AMI sem um código de produto se a instância não tiver um código de produto.
- O tamanho do mapeamento de dispositivos de blocos de volume raiz da AMI deve ser igual ou maior que o tamanho do volume raiz original. Se o tamanho do mapeamento de dispositivos de blocos do volume raiz da AMI for menor que o tamanho do volume raiz original, a solicitação falhará.
- Os documentos de identidade da instância são atualizados automaticamente.
- Se a instância for compatível com NitroTPM, os dados do nitroTPM da instância serão redefinidos e novas chaves serão geradas.

Substituir um volume raiz

Quando você substitui o volume raiz de uma instância, uma tarefa de substituição do volume raiz é criada. É possível usar a tarefa de substituição de volume raiz para monitorar o progresso e o resultado do processo de substituição. Para ter mais informações, consulte Exibir tarefas de substituição do volume raiz.

É possível substituir o volume raiz de uma instância usando um dos métodos a seguir.

> **Note**
>
> Se você usar o console do Amazon EC2, a funcionalidade só estará disponível no novo console.

New console

Para substituir o volume raiz

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que será substituída pelo volume raiz e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas) e Replace root volume (Substituir volume raiz).

   > **Note**
   >
   > A ação Replace root volume (Substituir volume raiz) estará desabilitada se a instância selecionada não estiver no estado `running`.

4. Na tela Replace root volume (Substituir volume raiz), siga um destes procedimentos:
   - Para restaurar o volume raiz substituto para seu estado inicial de execução, escolha Create replacement task (Criar tarefa de substituição) sem selecionar um snapshot.
   - Para restaurar o volume raiz substituto em um snapshot específico, em Snapshot, selecione o snapshot a ser usado e escolha Create replacement task (Criar tarefa de substituição).
   - Para restaurar o volume raiz substituto usando uma AMI, em AMI, selecione a AMI a ser usada e escolha Create replacement task (Criar tarefa de substituição).
5. Para excluir o volume raiz original após a conclusão da tarefa de substituição, selecione Delete replaced root volume (Excluir volume raiz substituído).

AWS CLI

Para restaurar o volume raiz substituto para o estado de execução

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Omita os parâmetros `--snapshot-id` e `--image-id`. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
```

```
--delete-replaced-root-volume true
```

Para restaurar o volume raiz em um snapshot específico

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `--snapshot-id`, especifique o ID do snapshot a ser usado. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume true
```

Para restaurar o volume raiz substituto usando uma AMI

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `--image-id`, especifique o ID da AMI a ser usada. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-01234567890abcdef \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume true
```

Tools for Windows PowerShell

Para restaurar o volume raiz substituto para o estado de execução

Use o comando New-EC2ReplaceRootVolumeTask. Em `-InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Omita os parâmetros `-SnapshotId` e `-ImageId`. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
DeleteReplacedRootVolume $true
```

Para restaurar o volume raiz em um snapshot específico

Use o comando New-EC2ReplaceRootVolumeTask. Em `--InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `-SnapshotId`, especifique o ID do snapshot a ser usado. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

Para restaurar o volume raiz substituto usando uma AMI

Use o comando New-EC2ReplaceRootVolumeTask. Em `-InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `-ImageId`, especifique o ID da AMI a ser usada. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Exibir tarefas de substituição do volume raiz

Quando você substitui o volume raiz de uma instância, uma tarefa de substituição do volume raiz é criada. A tarefa de substituição de volume raiz faz transição pelos seguintes estados durante o processo:

- `pending` — o volume de substituição está sendo criado.
- `in-progress` — o volume original está sendo destacado e o volume de substituição está sendo anexado.
- `succeeded` — o volume de substituição foi anexado com êxito à instância e a instância está disponível.
- `failing` — a tarefa de substituição está em processo de falha.
- `failed`: a tarefa de substituição falhou, mas o volume raiz original ainda está anexado.
- `failing-detached`: a tarefa de substituição está em processo de falha e talvez a instância não tenha um volume raiz anexado.
- `failed-detached`: a tarefa de substituição falhou e a instância não tem um volume raiz anexado.

É possível visualizar as tarefas de substituição do volume raiz de uma instância usando um dos seguintes métodos.

> **Note**
>
> Se você usar o console do Amazon EC2, a funcionalidade só estará disponível no novo console.

Console

Para visualizar as tarefas de substituição do volume raiz

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância para a qual deseja visualizar as tarefas de substituição do volume raiz e escolha a guia Storage (Armazenamento).
4. Na guia Storage (Armazenamento), expanda Recent root volume replacement tasks (Tarefas recentes de substituição de volume raiz).

AWS CLI

Para visualizar o status de uma tarefa de substituição de volume raiz

Use o comando describe-replace-root-volume-tasks e especifique os IDs das tarefas de substituição do volume raiz a serem visualizadas.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
```

```
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

Como alternativa, especifique o filtro `instance-id` para filtrar os resultados por instância.

```
$ aws ec2 describe-replace-root-volume-tasks \
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

Para visualizar o status de uma tarefa de substituição de volume raiz

Use o comando Get-EC2ReplaceRootVolumeTask e especifique os IDs das tarefas de substituição do volume raiz a serem visualizadas.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

Como alternativa, especifique o filtro `instance-id` para filtrar os resultados por instância.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nomes de dispositivos em instâncias do Amazon EC2

Quando você anexa um volume à instância, você inclui um nome de dispositivo para o volume. Esse nome de dispositivo é usado pelo Amazon EC2. O driver do dispositivo de blocos da instância atribui o nome real do volume ao montá-lo, e o nome atribuído pode ser diferente do nome usado pelo Amazon EC2.

O número de volumes que a instância pode suportar é determinado pelo sistema operacional. Para obter mais informações, consulte Limites de volumes de instância.

Conteúdo

- Nomes de dispositivos disponíveis

- Considerações sobre nomes de dispositivos

Nomes de dispositivos disponíveis

Instâncias do Linux

Há dois tipos de virtualização disponíveis para instâncias do Linux: paravirtual (PV) e máquina virtual de hardware (HVM). O tipo de virtualização de uma instância é determinado pela AMI usada para executar a instância. Todos os tipos de instância são compatíveis com AMIs HVM. Alguns tipos de instância da geração anterior oferecem suporte a AMIs PV. Observe o tipo de virtualização da AMI, pois os nomes de dispositivos recomendados e disponíveis que é possível usar dependem do tipo de virtualização da instância. Para ter mais informações, consulte Tipos de virtualização de AMI.

A tabela a seguir lista os nomes de dispositivo disponíveis que podem ser especificados em um mapeamento de dispositivo de bloco ou ao associar um volume do EBS.

Tipo de virtualização	Disponível	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd[a-d][a-z] /dev/xvd[e-z]	Difere por AMI /dev/sda1 ou /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd [] BH (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge)

Tipo de virtualização	Disponível	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
				**

* Os nomes de dispositivo que você especifica para volumes NVMe do EBS no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivo de NVMe (`/dev/nvme[0-26]n1`). O driver do dispositivo de blocos pode atribuir nomes de dispositivos NVMe em uma ordem diferente da especificada para os volumes no mapeamento de dispositivos de blocos.

** Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um nome de dispositivo NVMe.

Instâncias do Windows

As AMIs do Windows usam um dos seguintes conjuntos de drivers para permitir acesso ao hardware virtualizado: AWS PV, Citrix PV e RedHat PV. Para ter mais informações, consulte the section called “Drivers PV do Windows”.

A tabela a seguir lista os nomes de dispositivo disponíveis que podem ser especificados em um mapeamento de dispositivo de bloco ou ao associar um volume do EBS.

Tipo de driver	Disponível	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
AWS PV, Citrix PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e] **
Red Hat PV	xvd[a-z] xvd[b-c][a-z] /dev/sda1	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

Tipo de driver	Disponível	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
	/dev/sd[b-e]			

* Para Citrix PV e Red Hat PV, se você mapear um volume do EBS com o nome `xvda`, o Windows não reconhece o volume (o volume é visível para AWS PV ou AWS NVMe).

** Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um letra de unidade do Windows.

Para obter mais informações sobre volumes de armazenamento de instâncias, consulte Armazenamento de instâncias do Amazon EC2. Para obter mais informações sobre volumes do EBS do NVMe (instâncias baseadas em Nitro), incluindo como identificar o dispositivo do EBS, consulte Amazon EBS e NVMe no Guia do usuário do Amazon EBS.

Considerações sobre nomes de dispositivos

Lembre-se do seguinte ao selecionar um nome de dispositivo:

- A parte final dos nomes de dispositivos que você usar não deve se sobrepor, pois isso poderia causar problemas ao iniciar a instância. Por exemplo, evite usar combinações como `/dev/xvdf` e `xvdf` para volumes anexados à mesma instância.
- Embora você possa anexar os volumes do EBS usando nomes de dispositivos usados para volumes de armazenamento da instância, recomendamos enfaticamente que você não o faça porque o comportamento poderá ser imprevisível.
- O número de volumes de armazenamento de instâncias NVMe de uma instância depende do tamanho da instância. Os volumes de armazenamento de instância de NVMe são enumerados automaticamente e recebem um nome de dispositivo de NVMe (instâncias do Linux) ou uma letra de unidade do Windows (instâncias do Windows).
- (Instâncias do Windows) As AMIs do Windows da AWS vêm com um software adicional que prepara uma instância quando ela é inicializada pela primeira vez. Ele é o serviço EC2Config (AMIs do Windows de versões anteriores ao Windows Server 2016) ou EC2Launch (Windows Server 2016 e posterior). Após o mapeamento nas unidades, os dispositivos são inicializados e montados. A unidade raiz é inicializada e montada como `C:\`. Por padrão, quando um volume do EBS é anexado a uma instância do Windows, ele poderá ser mostrado como

qualquer letra de unidade na instância. É possível alterar as configurações para definir as letras dos volumes de acordo com suas especificações. Para volumes de armazenamento de instâncias, o padrão depende do driver AWS. Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A: Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:. Para obter mais informações, consulte Definição das configurações de inicialização para instâncias do Windows do Amazon EC2 e Mapear discos para volumes na sua instância do Windows.

- (Instâncias do Linux) Dependendo do driver de dispositivo de blocos do kernel, o dispositivo pode ser anexado com um nome diferente do especificado. Por exemplo, se você especificar um nome de dispositivo de `/dev/sdh`, o dispositivo poderá ser renomeado como `/dev/xvdh` ou `/dev/hdh`. Na maioria dos casos, a letra à direita permanece a mesma. Em algumas versões do Red Hat Enterprise Linux (e suas variantes, como o CentOS), a letra à direita pode ser alterada (`/dev/sda` pode se tornar `/dev/xvde`). Nesses casos, a letra à direita de cada nome de dispositivo é aumentada no mesmo número de vezes. Por exemplo, se `/dev/sdb` é renomeado `/dev/xvdf`, então `/dev/sdc` é renomeado `/dev/xvdg`. O Amazon Linux cria um link simbólico para o nome que você especificou no dispositivo renomeado. Outros sistemas operacionais podem se comportar de maneira diferente.
- (Instâncias do Linux) As AMIs de HVM não oferecem suporte ao uso de números finais em nomes de dispositivos, exceto `/dev/sda1`, que é reservado para o dispositivo raiz, e `/dev/sda2`. Embora o uso de `/dev/sda2` seja possível, não recomendamos o uso desse mapeamento de dispositivo com instâncias HVM.
- (Instâncias do Linux) Ao usar as AMIs PV, não é possível anexar volumes que compartilhem as mesmas letras de dispositivo com e sem dígitos finais. Por exemplo, se você anexar um volume como `/dev/sdc` e outro volume como `/dev/sdc1`, somente `/dev/sdc` será visível para a instância. Para usar dígitos à direita em nomes de dispositivos, use dígitos à direita em todos os nomes de dispositivos que compartilham as mesmas letras base (como `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Instâncias do Linux) Alguns kernels personalizados podem ter restrições que limitam o uso a `/dev/sd[f-p]` ou a `/dev/sd[f-p][1-6]`. Se estiver tendo problema para usar `/dev/sd[q-z]` ou `/dev/sd[q-z][1-6]`, tente mudar para `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`.

Antes de especificar o nome do dispositivo selecionado, verifique se ele está disponível. Caso contrário, você receberá um erro informando que o nome de dispositivo já está em uso. Para visualizar os dispositivos de disco e seus pontos de montagem, use o comando lsblk (instâncias do Linux), ou o utilitário Gerenciamento de Disco ou o comando diskpart (instâncias do Windows).

Mapeamentos de dispositivos de blocos

Cada instância que você executa tem um volume de dispositivo raiz associado, seja um volume do Amazon EBS ou um volume de armazenamento de instâncias. Use o mapeamento de dispositivos de blocos para especificar mais volumes do EBS ou volumes de armazenamento de instâncias para anexar a uma instância quando ela for executada. É possível associar volumes adicionais do EBS a uma instância em execução. Contudo, a única forma de associar volumes de armazenamento de instâncias a uma instância é usar o mapeamento de dispositivos de blocos para anexá-los à medida que a instância é executada.

Conteúdo

- Conceitos de mapeamento de dispositivos de blocos
- Mapeamento de dispositivos de blocos da AMI
- Mapeamento de dispositivos de blocos de instância

Conceitos de mapeamento de dispositivos de blocos

Um dispositivo de blocos é um dispositivo de armazenamento que move dados em sequências de bytes ou de bits (blocos). Esses dispositivos oferecem suporte ao acesso aleatório e geralmente usam E/S em buffer. Os exemplos incluem discos rígidos, unidades de CD-ROM e pen-drives. Um dispositivo de blocos pode ser fisicamente ligado a um computador ou acessado remotamente, como se estivesse ligado fisicamente ao computador.

O Amazon EC2 oferece suporte a dois tipos de dispositivo de blocos:

- Volumes de armazenamento de instâncias (dispositivos virtuais cujo hardware subjacente é ligado fisicamente ao computador host da instância)
- Volumes EBS (dispositivos de armazenamento remoto)

Um mapeamento de dispositivos de blocos define os dispositivos de blocos (volumes de armazenamento de instâncias e volumes do EBS) para anexar a uma instância. É possível especificar um mapeamento de dispositivos de blocos como parte da criação de um AMI para que o mapeamento seja usado por todas as instâncias executadas pela AMI. Como alternativa, é possível especificar um mapeamento de dispositivos de blocos ao executar uma instância, para que o mapeamento cancele o especificado na AMI do qual você iniciou a instância. Observe que todos os volumes de armazenamento de instâncias de NVMe compatíveis com um tipo de instância

são automaticamente enumerados e atribuídos a um nome de dispositivo durante a execução da instância. Incluí-los no seu mapeamento de dispositivos de blocos não surtirá nenhum efeito.

Tópicos

- Entradas do mapeamento de dispositivos de blocos
- Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos
- Exemplo de mapeamento de dispositivos de blocos
- Como os dispositivos são disponibilizados no sistema operacional

Entradas do mapeamento de dispositivos de blocos

Ao criar um mapeamento de dispositivos de blocos, é preciso especificar as informações a seguir para cada dispositivo de blocos que você precisa associar à instância:

- O nome de dispositivo usado no Amazon EC2. O driver de dispositivo de blocos da instância atribui o nome real do volume ao montar o volume. O nome atribuído pode ser diferente do nome recomendado pelo Amazon EC2. Para obter mais informações, consulte Nomes de dispositivos em instâncias do Amazon EC2.

Para volumes de armazenamento de instâncias, você também especifica as seguintes informações:

- O dispositivo virtual: `ephemeral[0-23]`. Observe que o número e o tamanho de volumes de armazenamento de instâncias disponíveis variam por tipo de instância.

Para volumes de armazenamento de instâncias NVMe, as seguintes informações também se aplicam:

- Esses volumes são automaticamente enumerados e atribuídos a um nome de dispositivo; incluí-los no mapeamento de dispositivos de blocos não surtirá nenhum efeito.

Para volumes do EBS, você também especifica as seguintes informações:

- O ID do snapshot a ser usado para criar o dispositivo de blocos (snap-xxxxxxxx). Esse valor é opcional, desde que você especifique um tamanho do volume. Você não pode especificar a ID de snapshots arquivados.

- O tamanho do volume em GiB. O tamanho especificado deve ser maior que ou igual ao tamanho do snapshot especificado.
- Se o volume deve ser excluído no encerramento da instância (`true` ou `false`). O valor padrão é `true` para o volume do dispositivo raiz e `false` para volumes associados. Quando você cria a AMI, o mapeamento de dispositivos de blocos dele herda essa configuração da instância. Quando você executa uma instância, ela herda essa configuração da AMI.
- O tipo de volume, que pode ser `gp2` e `gp3` para SSD de uso geral, `io1` e `io2` para SSD de IOPS provisionadas, `st1` para HDD otimizado para throughput, `sc1` para HDD a frio ou `standard` para magnético.
- O número de operações de entrada/saída por segundo (IOPS) que o volume é capaz de suportar. (Usado apenas com volumes `io1` e `io2`.)

Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos

Há várias advertências a serem consideradas ao executar instâncias com os AMIs que têm volumes de armazenamento de instâncias em seus mapeamentos de dispositivos de blocos.

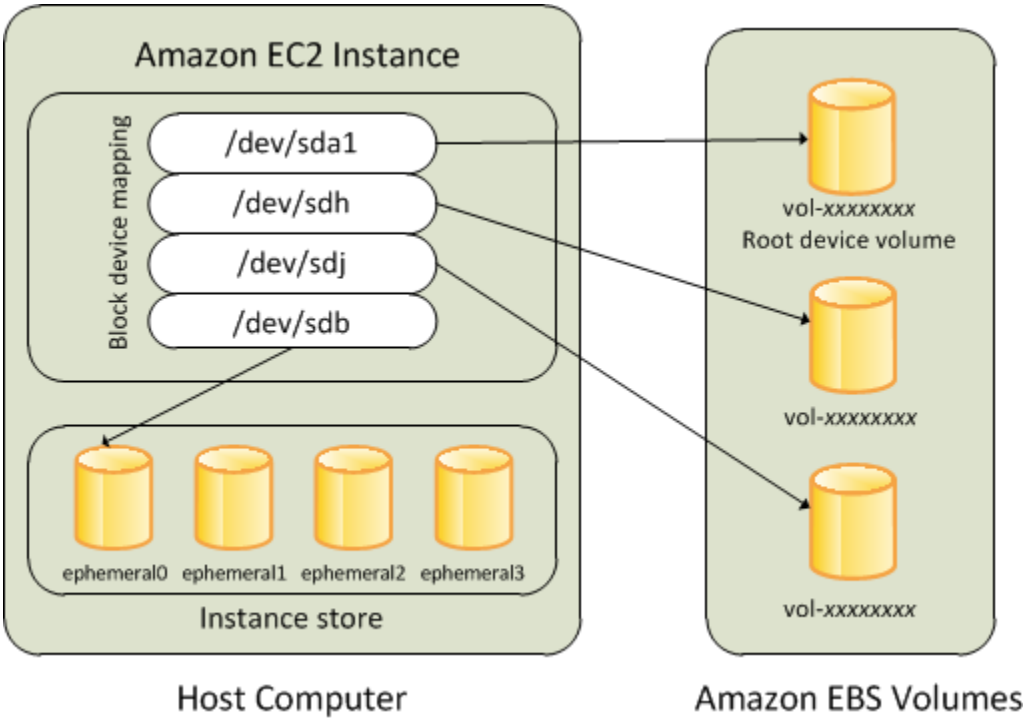
- Alguns tipos de instância incluem mais volumes de armazenamento de instâncias que outros, e alguns tipos de instância não contêm nenhum volume de armazenamento de instâncias. Se seu tipo de instância for compatível com um volume de armazenamento de instâncias e o AMI tiver mapeamentos para dois volumes de armazenamento de instâncias, a instância será executada com um volume de armazenamento de instâncias.
- Volumes de armazenamento de instâncias só podem ser mapeados no momento da execução. Você não pode interromper uma instância sem volumes de armazenamento de instâncias (como `t2.micro`), alterar a instância para um tipo que suporte os volumes de armazenamento de instâncias e reiniciem a instância com volumes de armazenamento de instâncias. No entanto, é possível criar uma AMI com base na instância e executá-la em um tipo de instância que suporte volumes de armazenamento de instâncias e os mapeie para a instância.
- Se você executar uma instância com os volumes de armazenamento de instâncias mapeados e, em seguida, interromper a instância e alterá-la para um tipo de instância com menos volumes de armazenamento de instâncias e reiniciá-la, os mapeamentos do volume de armazenamento de instâncias da execução inicial continuarão a ser exibidos nos metadados da instância. Contudo, somente o número máximo de volumes aceito pelo armazenamento de instâncias para aquele tipo de instância estará disponível.

> **Note**
>
> Quando uma instância for interrompida, todos os dados nos volumes do armazenamento de instâncias serão perdidos.

- Dependendo da capacidade de armazenamento das instâncias no momento da execução, as instâncias M3 poderão ignorar os mapeamentos de dispositivos de blocos do armazenamento de instâncias da AMI na execução, a menos que sejam especificadas na execução. Especifique mapeamentos de dispositivos de blocos no armazenamento de instâncias no momento da inicialização, mesmo que a AMI que você está executando tenha os volumes de armazenamento de instâncias mapeados na AMI, de forma a garantir que os volumes de armazenamento das instâncias estejam disponíveis quando a instância é iniciada.

Exemplo de mapeamento de dispositivos de blocos

Essa figura mostra um exemplo de mapeamento de dispositivos de blocos para uma instância com EBS. Isso mapeia `/dev/sdb` para `ephemeral0` e mapeia dois volumes do EBS: uma para `/dev/sdh` e outro para `/dev/sdj`. Isso também mostra o volume do EBS que é o volume do dispositivo raiz, `/dev/sda1`.



Observe que esse exemplo de mapeamento de dispositivos de blocos é utilizado em exemplos de comandos e APIs neste tópico. É possível encontrar os exemplos de comandos e APIs que criam mapeamentos de dispositivos de blocos em Especificar um mapeamento de dispositivos de blocos para uma AMI e Atualizar o mapeamento de dispositivos de blocos ao executar uma instância.

Como os dispositivos são disponibilizados no sistema operacional

Nomes de dispositivos, como `/dev/sdh` e `xvdh`, são usados pelo Amazon EC2 para descrever dispositivos de blocos. O mapeamento de dispositivos de blocos é usado pelo Amazon EC2 para especificar os dispositivos de blocos para uma instância do EC2. Após um dispositivo de blocos ser associado a uma instância, ele deverá ser montado pelo sistema operacional antes que você possa acessar o dispositivo de armazenamento. Quando um dispositivo de blocos é separado de uma instância, ele será desmontado pelo sistema operacional e você não poderá mais acessar o dispositivo de armazenamento.

Instâncias do Linux: os nomes de dispositivos especificados no mapeamento de dispositivos de blocos são mapeados para os dispositivos de blocos correspondentes quando a instância é inicializada pela primeira vez. O tipo de instância determina quais volumes de armazenamento de instâncias são formatados e montados por padrão. É possível montar volumes de armazenamento de instâncias adicionais na execução, desde que não ultrapasse o número de volumes de armazenamento de instâncias disponível para seu tipo de instância. Para obter mais informações, consulte Armazenamento de instâncias do Amazon EC2. O driver do dispositivo de blocos para a instância determina quais dispositivos são usados quando os volumes são formatados e montados.

Instâncias do Windows: os nomes de dispositivos especificados no mapeamento de dispositivos de blocos são mapeados para os dispositivos de bloco correspondentes quando a instância é inicializada pela primeira vez e, em seguida, o serviço Ec2Config inicializa e monta as unidades. O volume do dispositivo raiz é montado como `C:\`. Os volumes de armazenamento de instâncias são montados como `Z:\`, `Y:\`, etc. Quando um volume do EBS é montado, isso pode acontecer usando qualquer letra de unidade disponível. No entanto, é possível configurar como as letras de unidade são atribuídas aos volumes do EBS. Para obter mais informações, consulte the section called “Definição de agentes de inicialização do Windows”.

Mapeamento de dispositivos de blocos da AMI

Cada AMI tem um mapeamento de dispositivos de blocos que especifica os dispositivos de blocos a serem associados a uma instância quando é executada pela AMI. Para adicionar mais dispositivos de blocos a uma AMI, crie sua própria AMI.

Tópicos

- Especificar um mapeamento de dispositivos de blocos para uma AMI
- Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI

Especificar um mapeamento de dispositivos de blocos para uma AMI

Há duas maneiras de especificar volumes além do volume do dispositivo raiz ao criar uma AMI. Se você já tiver associado volumes a uma instância em execução antes de criar uma AMI pela instância, o mapeamento de dispositivos de blocos para a AMI incluirá os mesmos volumes. Para volumes do EBS, os dados existentes são salvos em um novo snapshot, e é esse novo snapshot que é especificado no mapeamento de dispositivos de blocos. Para volumes de armazenamento de instâncias, os dados não são preservados.

Para AMI baseados em EBS, é possível adicionar volumes do EBS e volumes de armazenamento de instâncias usando um mapeamento de dispositivos de blocos. Para AMIs com armazenamento de instâncias, você só poderá adicionar volumes de armazenamento de instâncias ao modificar as entradas de mapeamento de dispositivos de blocos no arquivo manifesto da imagem ao registrar a imagem.

> **Note**
>
> Para instâncias M3, especifique volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos para a instância ao iniciá-los. Quando você executa uma instância M3, os volumes de armazenamento de instâncias especificados no mapeamento de dispositivos de blocos para a AMI poderão ser ignorados se não forem especificados como parte do mapeamento de dispositivos de blocos da instância.

Console

Para adicionar volumes a uma AMI usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Insira um nome e uma descrição para a imagem.

5. Os volumes de instância aparecem em Volumes de instância (Volumes de instância). Para adicionar outro volume, escolha Add volume (Adicionar volume).
6. Em Volume type (Tipo de volume), escolha o tipo de volume. Para Device (Dispositivo), escolha o nome do dispositivo. Para um volume do EBS, é possível especificar detalhes adicionais, como um snapshot, o tamanho do volume, o tipo de volume, IOPS e estado de criptografia.
7. Escolha Create Image (Criar imagem).

Command line

To add volumes to an AMI using the command line (Para adicionar volumes a uma AMI usando a linha de comando)

Use o comando create-image da AWS CLI para especificar um mapeamento de dispositivos de blocos para uma AMI com EBS. Use o comando register-image da AWS CLI para especificar um mapeamento de dispositivos de blocos para uma AMI com armazenamento de instâncias.

Especifique o mapeamento de dispositivos de blocos usando o parâmetro `--block-device-mappings`. Os argumentos codificados em JSON podem ser fornecidos diretamente na linha de comando ou por referência a um arquivo:

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

Para adicionar um volume de armazenamento de instâncias, use o mapeamento a seguir.

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Para adicionar um volume vazio do gp2 de 100 GiB, use o mapeamento a seguir.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para adicionar um volume do EBS com base em um snapshot, use o mapeamento a seguir.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

Para omitir um mapeamento de um dispositivo, use o mapeamento a seguir:

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

Como alternativa, é possível usar o parâmetro `-BlockDeviceMapping` com os comandos a seguir (AWS Tools for Windows PowerShell):

- New-EC2Image
- Register-EC2Image

Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI

É possível facilmente enumerar volumes do EBS no mapeamento de dispositivos de blocos para AMI.

Console

Para visualizar os volumes do EBS para uma AMI usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione AMIs.
3. Escolha EBS images (Imagens de EBS) da lista Filter (Filtro) para obter uma lista de AMIs com EBS.
4. Selecione a AMI desejada e examine a guia Details (Detalhes). No mínimo, estarão disponíveis as informações a seguir para o dispositivo raiz:

    - Root Device Type (Tipo de dispositivo raiz (`ebs`)

- Root Device Name (Nome do dispositivo raiz) (por exemplo, `/dev/sda1`)
- Block Devices (Dispositivos de blocos) (por exemplo, `/dev/sda1=snap-1234567890abcdef0:8:true`)

Se a AMI tiver sido criada com volumes do EBS adicionais usando um mapeamento de dispositivos de blocos, o campo Block Devices (Dispositivos de blocos) exibirá o mapeamento desses volumes adicionais também. (Essa tela não exibe volumes de armazenamento de instâncias.)

Command line

To view the EBS volumes for an AMI using the command line (Para visualizar os volumes do EBS para uma AMI usando a linha de comando)

Use o comando describe-images (AWS CLI) ou o comando Get-EC2Image (AWS Tools for Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma AMI.

Mapeamento de dispositivos de blocos de instância

Por padrão, uma instância que você inicia inclui todos os dispositivos de armazenamento especificados no mapeamento de dispositivos de blocos da AMI do qual você executou a instância. É possível especificar alterações ao mapeamento de dispositivos de blocos para uma instância quando ela é iniciada, e essas atualizações se sobrescrevem ou se mesclam com o mapeamento de dispositivos de blocos da AMI.

Limitações

- Para o volume raiz, você só pode modificar o seguinte: tamanho do volume, tipo de volume e o sinalizador Delete on Termination (Excluir ao encerrar).
- Quando modificar um volume do EBS, não será possível reduzir o tamanho. Portanto, especifique um snapshot cujo tamanho seja igual ou maior que o tamanho do snapshot especificado no mapeamento de dispositivos de blocos da AMI.

Tópicos

- Atualizar o mapeamento de dispositivos de blocos ao executar uma instância

- Atualizar o mapeamento de dispositivos de blocos de uma instância em execução
- Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância
- Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias

Atualizar o mapeamento de dispositivos de blocos ao executar uma instância

É possível adicionar volumes do EBS e volumes de armazenamento de instâncias a uma instância quando iniciá-la. Observe que atualizar o mapeamento de dispositivos de blocos para uma instância não cria uma alteração permanente no mapeamento de dispositivos de blocos da AMI do qual ela foi executada.

Console

Para adicionar volumes a uma instância usando o console

1. Abra o console do Amazon EC2.
2. No painel, escolha Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolha uma imagem de máquina da Amazon), selecione as AMIs a serem usadas e escolha Select (Selecionar).
4. Siga o assistente para preencher as páginas Choose an Instance Type e Configure Instance Details.
5. Na página Add Storage (Adicionar armazenamento), é possível modificar o volume raiz, os volumes do EBS e os volumes de armazenamento de instâncias da seguinte forma:
   - Para alterar o tamanho do volume raiz, localize o volume Root (Raiz) na coluna Type (Tipo) e altere o campo Size (Tamanho).
   - Para excluir um volume do EBS especificado pelo mapeamento de dispositivos de blocos das AMIs usadas para executar a instância, localize o volume e clique no ícone Delete (Excluir).
   - Para adicionar um volume do EBS, escolha Add New Volume (Adicionar novo volume), escolha EBS na lista Type (Tipo) e preencha os campos (Device [Dispositivo], Snapshot [Snapshot] etc.).
   - Para excluir um volume de armazenamento de instâncias especificado pelo mapeamento de dispositivos de blocos da AMI usada para executar a instância, localize o volume e clique no ícone Delete (Excluir).

- Para adicionar um volume de armazenamento de instâncias, selecione Add New Volume (Adicionar novo volume), Instance Store (Armazenamento de instância) na lista Type (Tipo) e selecione um nome de dispositivo em Device (Dispositivo).

6. Preencha as páginas restantes do assistente e escolha Launch (Executar).

Command line

Como adicionar volumes a uma instância usando a AWS CLI

Use o comando run-instances da AWS CLI com a opção `--block-device-mappings` para especificar um mapeamento de dispositivos de blocos para uma instância no lançamento.

Por exemplo, suponha que uma AMI baseada no EBS especifique o seguinte mapeamento de dispositivos de blocos para uma instância do Linux:

- `/dev/sdb` = `ephemeral0`
- `/dev/sdh` = `snap-1234567890abcdef0`
- `/dev/sdj` = `100`

Para evitar que o `/dev/sdj` seja anexado a uma instância em execução nesta AMI, use o mapeamento a seguir.

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

Para aumentar o tamanho de `/dev/sdh` para `300 GiB`, especifique o mapeamento apresentado a seguir. Observe que você não precisa especificar o ID do snapshot para `/dev/sdh`, pois especificar o nome do dispositivo basta para identificar o volume.

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

Para aumentar o tamanho do volume raiz ao iniciar a instância, primeiro chame describe-images com o ID da AMI para verificar o nome de dispositivo do volume raiz. Por exemplo, `"RootDeviceName": "/dev/xvda"`. Para substituir o tamanho do volume raiz, especifique o nome do dispositivo raiz usado pela AMI e o novo tamanho do volume.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para associar um volume adicional de armazenamento de instâncias, `/dev/sdc`, especifique o mapeamento a seguir. Se o tipo de instância não oferecer volumes de armazenamento de múltiplas instâncias, esse mapeamento não surtirá efeito. Se a instância for compatível com os volumes de armazenamento de instâncias NVMe, eles serão automaticamente enumerados e receberão um nome de dispositivo NVMe.

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

Como adicionar volumes a uma instância usando a AWS Tools for Windows PowerShell

Use o parâmetro `-BlockDeviceMapping` com o comando New-EC2Instance (AWS Tools for Windows PowerShell)

Atualizar o mapeamento de dispositivos de blocos de uma instância em execução

É possível usar o comando modify-instance-attribute da AWS CLI para atualizar o mapeamento de dispositivos de blocos de uma instância em execução. Você não precisa parar a instância para alterar esse atributo.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
 file://mapping.json
```

Por exemplo: para preservar o volume raiz no encerramento da instância, especifique o seguinte no `mapping.json`.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Como alternativa, é possível usar o parâmetro `-BlockDeviceMapping` com o comando Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell).

Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância

É possível facilmente enumerar volumes do EBS para a instância.

> **Note**
>
> Para instâncias executadas antes do lançamento da API de 31/10/2009, a AWS não pode exibir o mapeamento de dispositivos de blocos. É necessário separar e reassociar volumes de modo que a AWS possa exibir o mapeamento de dispositivos de blocos.

Console

Para visualizar os volumes do EBS para uma instância usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na caixa de pesquisa, insira Root device type (Tipo de dispositivo raiz) e selecione EBS. Isso exibe uma lista de instâncias baseadas no EBS.
4. Selecione a instância desejada e examine os detalhes exibidos na guia Storage (Armazenamento). No mínimo, estarão disponíveis as informações a seguir para o dispositivo raiz:
   - Root device type (Tipo de dispositivo raiz) (por exemplo, EBS)
   - Root Device Name (Nome do dispositivo raiz) (por exemplo, `/dev/xvda`)

- Block devices (Dispositivos de blocos) (por exemplo `/dev/xvda`, `/dev/sdf` e `/dev/sdj`)

Se a instância tiver sido executada com volumes adicionais do EBS usando um mapeamento de dispositivo de bloco, eles aparecerão em Block devices (Dispositivos de bloco). Nenhum dos volumes de armazenamento de instâncias aparece nesta guia.

5. Para exibir informações adicionais sobre um volume do EBS, escolha seu ID de volume para ir para a página de volume.

Command line

To view the EBS volumes for an instance using the command line (Para visualizar os volumes do EBS para uma instância usando a linha de comando)

Use o comando describe-instances (AWS CLI) ou o comando de Get-EC2Instance (AWS Tools for Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma instância.

Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias

O tipo de instância determina o número e o tipo de volumes de armazenamento de instância que estão disponíveis para a instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número de volumes de armazenamento de instâncias disponível para uma instância, os volumes adicionais serão ignorados. Para visualizar os volumes de armazenamento de instância da instância, execute o comando lsblk (instâncias do Linux) ou abra o Gerenciamento de Disco do Windows (instâncias do Windows). Para saber a quantidade de volumes de armazenamento de instância que são compatíveis com cada tipo de instância, consulte Amazon EC2 instance type specifications.

Quando você vir o mapeamento de dispositivos de blocos para sua instância, verá somente os volumes do EBS, não os volumes de armazenamento de instâncias. O método a ser usado para visualizar os volumes de armazenamento de instâncias para a instância depende do tipo de volume.

Volumes de armazenamento de instâncias do NVMe

Instâncias do Linux

É possível usar o pacote de linha de comando do NVMe, nvme-cli, para consultar os volumes de armazenamento de instâncias do NVMe no mapeamento de dispositivos de blocos. Faça download e instale o pacote de sua instância e execute o seguinte comando.

```
[ec2-user ~]$ sudo nvme list
```

Este é um exemplo de saída de uma instância. O texto na coluna Modelo indica se o volume é um volume do EBS ou um volume do armazenamento de instâncias. Neste exemplo, tanto `/dev/nvme1n1` como `/dev/nvme2n1` são volumes de armazenamento de instâncias.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

Instâncias do Windows

É possível utilizar o Gerenciamento de disco ou o PowerShell para listar volumes NVMe do EBS e do armazenamento de instâncias. Para ter mais informações, consulte the section called “Listar volumes do NVMe”.

Volumes de armazenamento de instâncias HDD ou SSD

É possível usar os metadados da instância para consultar os volumes de armazenamento de instâncias HDD ou SSD no mapeamento de dispositivos de blocos. Os volumes de armazenamento de instâncias NVMe não estão incluídos.

O URI de base de todas as solicitações de metadados da instância é `http://169.254.169.254/latest/`. Para ter mais informações, consulte Trabalhar com metadados de instância.

Instâncias do Linux

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

A resposta inclui o nome dos dispositivo de blocos para a instância. Por exemplo, a saída de uma instância `m1.small` com armazenamento de instância é semelhante a esta:

```
ami
ephemeral0
root
swap
```

O dispositivo `ami` é o dispositivo raiz como visto pela instância. Os volumes de armazenamento de instâncias têm o nome `ephemeral[0-23]`. O dispositivo `swap` é para o arquivo da página. Se você também tiver mapeado os volumes do EBS, eles serão exibidos como `ebs1`, `ebs2`, etc.

Para obter detalhes sobre um dispositivo de blocos individual no mapeamento de dispositivos de blocos, coloque o nome dele na consulta anterior, como mostrado aqui.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
ephemeral0
```

Instâncias do Windows

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/
```

A resposta inclui o nome dos dispositivo de blocos para a instância. Por exemplo, a saída de uma instância `m1.small` com armazenamento de instância é semelhante a esta:

```
ami
ephemeral0
root
swap
```

O dispositivo `ami` é o dispositivo raiz como visto pela instância. Os volumes de armazenamento de instâncias têm o nome `ephemeral[0-23]`. O dispositivo `swap` é para o arquivo da página. Se você também tiver mapeado os volumes do EBS, eles serão exibidos como `ebs1`, `ebs2`, etc.

Para obter detalhes sobre um dispositivo de blocos individual no mapeamento de dispositivos de blocos, coloque o nome dele na consulta anterior, como mostrado aqui.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/ephemeral0
```

Mapear discos para volumes na sua instância do Windows

> **Note**
>
> Este tópico se aplica somente a instâncias do Windows.

Sua instância do Windows vem com um volume do EBS que serve como o volume raiz. Se sua instância do Windows usar os drivers AWS PV ou Citrix PV, é possível adicionar até 25 volumes, contabilizando um total de 26 volumes. Para obter mais informações, consulte Limites de volumes de instância.

Dependendo do tipo de sua instância, você terá de 0 a 24 volumes de armazenamento de instâncias possíveis disponíveis para a instância. Para usar qualquer um dos volumes de armazenamento de instâncias que estão disponíveis para a instância, você deverá especificá-los ao criar sua AMI ou executar a instância. Também é possível adicionar volumes do EBS ao criar sua AMI ou executar a instância ou anexá-los enquanto a instância estiver em execução.

Quando você adicionar um volume à sua instância, especifique o nome do dispositivo que o Amazon EC2 usa. Para ter mais informações, consulte Nomes de dispositivos em instâncias do Amazon EC2. AWS As imagens de máquina da Amazon (AMIs) do Windows contêm um conjunto de drivers que são usados pelo Amazon EC2 para mapear o armazenamento de instância e os volumes do EBS aos discos e a letras de unidade do Windows. Se você executar uma instância a partir de uma AMI do Windows que use drivers AWS PV ou Citrix PV, será possível usar as relações descritas nesta página para mapear os discos do Windows ao seu armazenamento de instâncias e volumes do EBS. Se a AMI da Windows usar drivers Red Hat PV, é possível atualizar sua instância para usar os drivers Citrix. Para ter mais informações, consulte the section called “Atualizar drivers de PV”.

Sumário

- Listar volumes do NVMe
  - Listar discos de NVMe usando o Gerenciamento de disco
  - Listar discos do NVMe usando PowerShell
  - Mapear volumes do EBS de NVMe
- Listar volumes
  - Listar discos usando o Gerenciamento de disco
  - Mapear dispositivos de disco para nomes de dispositivos
    - Volumes de armazenamento de instâncias
    - Volumes do EBS
  - Listar discos usando PowerShell

Listar volumes do NVMe

É possível encontrar os discos na instância do Windows usando Gerenciamento de disco ou Powershell.

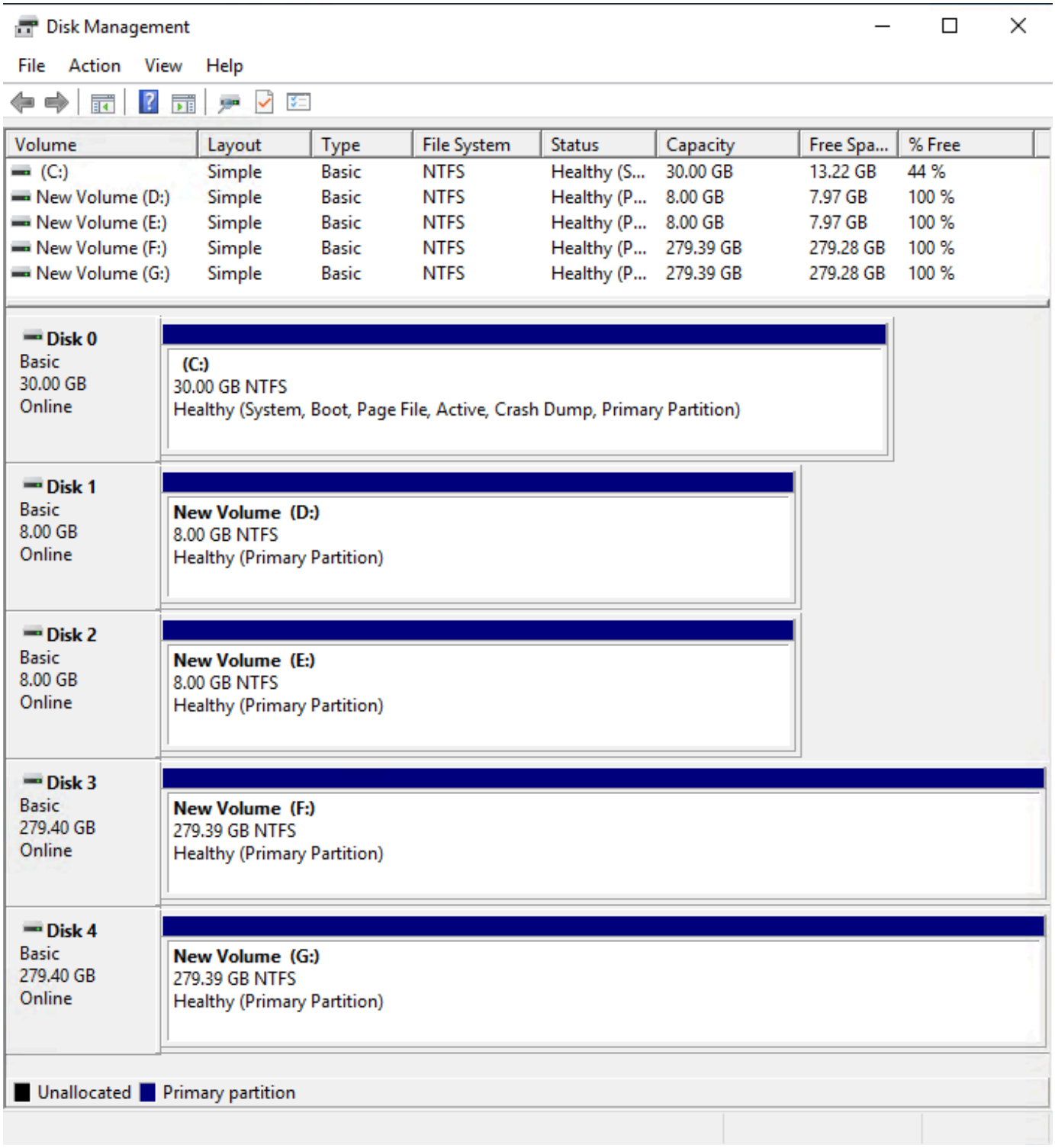
Listar discos de NVMe usando o Gerenciamento de disco

É possível encontrar os discos na sua instância do Windows usando o Gerenciamento de disco do Windows.

Para localizar os discos em sua instância do Windows

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à sua instância do Windows do .
2. Inicie o utilitário de Gerenciamento de Disco.
3. Revise os discos. O volume raiz é um volume do EBS montado como `C:\`. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

   Veja a seguir um exemplo que mostra os discos disponíveis se você executar uma instância `r5d.4xlarge` com dois volumes adicionais do EBS.


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (S... 30.00 GB 13.22 GB 44 %
New Volume (D:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (E:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (F:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
New Volume (G:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
Disk 0
Basic
30.00 GB
Online
(C:)
30.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)
Disk 1
Basic
8.00 GB
Online
New Volume (D:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
8.00 GB
Online
New Volume (E:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 3
Basic
279.40 GB
Online
New Volume (F:)
279.39 GB NTFS
Healthy (Primary Partition)
Disk 4
Basic
279.40 GB
Online
New Volume (G:)
279.39 GB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition

Listar discos do NVMe usando PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes. Ele se destina ao uso com instâncias desenvolvidas no AWS Nitro System, que usam volumes do EBS com especificação NVMe e volumes de armazenamento de instância.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o script a seguir e salve-o como `mapping.ps1` na instância do Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
```

```
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
```

```
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

Veja a seguir um exemplo de saída para uma instância com um volume raiz, dois volumes do EBS e dois volumes de armazenamento de instâncias.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Se você não tiver fornecido suas credenciais do Tools for Windows PowerShell na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna `EbsVolumeId`.

Mapear volumes do EBS de NVMe

Com as instâncias desenvolvidas no AWS Nitro System, os volumes do EBS são expostos como dispositivos NVMe. É possível usar o comando Get-Disk para mapear os números de disco do Windows para IDs de volume do EBS.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                     Style
------ ------------- -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
             279.4 GB MBR
```

```
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy            Online
             279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy            Online
               8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy            Online
              30 GB MBR
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy            Online
               8 GB MBR
```

Também é possível executar o comando ebsnvme-id para mapear números de disco do NVMe para IDs de volume do EBS e nomes de dispositivos.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Listar volumes

É possível encontrar os discos na instância do Windows usando Gerenciamento de disco ou Powershell.

Listar discos usando o Gerenciamento de disco

É possível encontrar os discos na sua instância do Windows usando o Gerenciamento de disco do Windows.

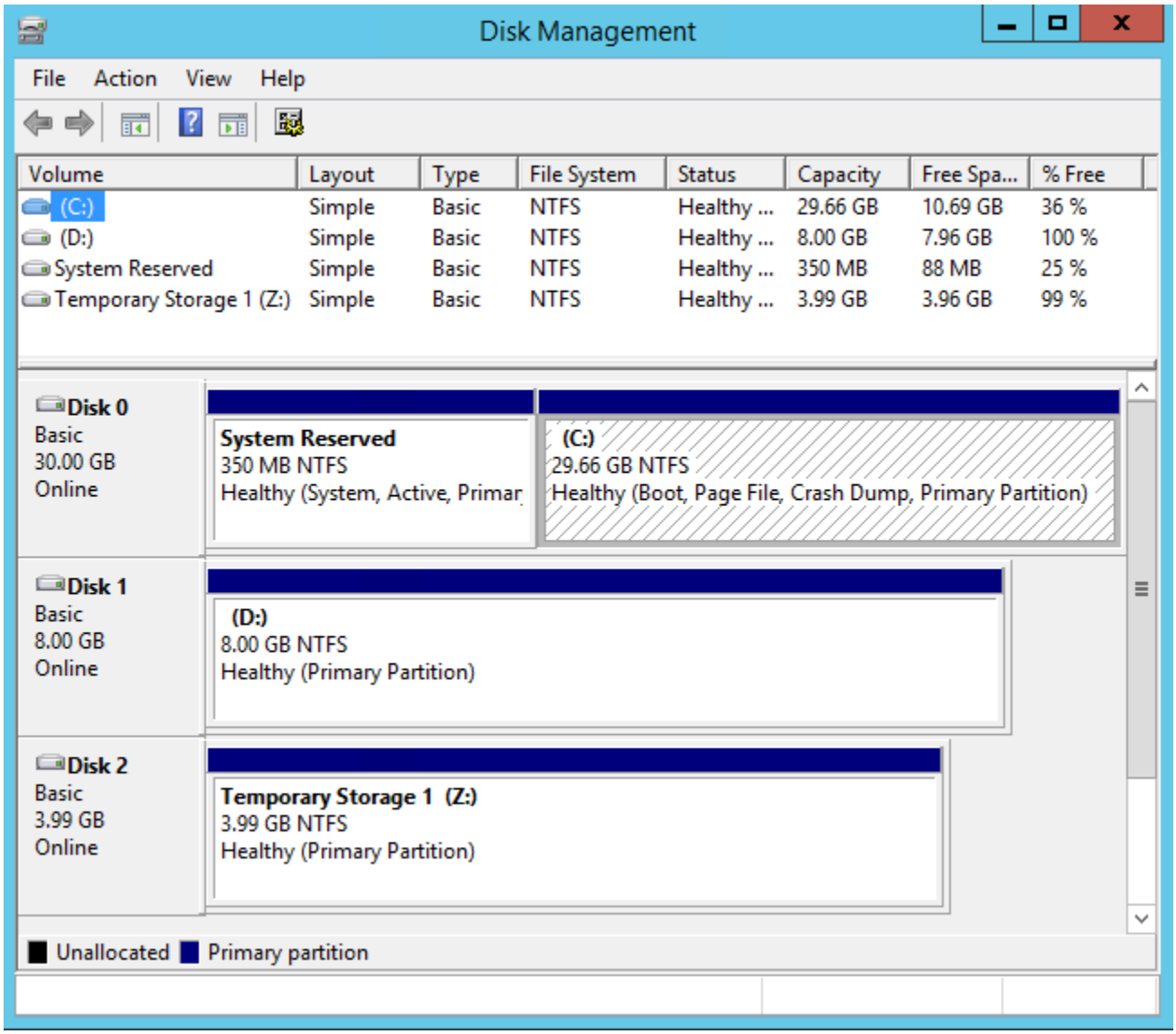
Para localizar os discos em sua instância do Windows

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à sua instância do Windows do .
2. Inicie o utilitário de Gerenciamento de Disco.

Na barra de tarefas, clique com o botão direito do mouse no logotipo do Windows e escolha Gerenciamento de disco.

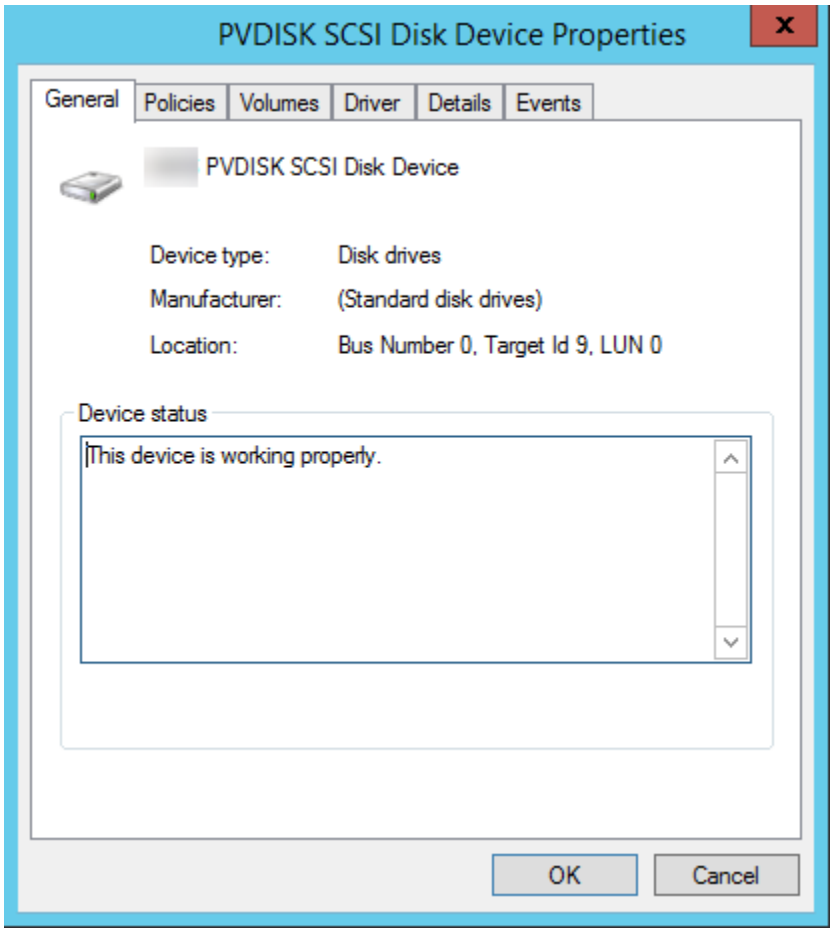
3. Revise os discos. O volume raiz é um volume do EBS montado como `C:\`. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

   Veja a seguir um exemplo que mostra os discos que estão disponíveis se você executar uma instância `m3.medium` com um volume de armazenamento de instâncias (disco 2) e um volume do EBS adicional (disco 1).



4. Clique com o botão direito no painel cinza identificado como Disco 1 e selecione Properties (Propriedades). Observe o valor de Location (Local) e procure-o nas tabelas em Mapear dispositivos de disco para nomes de dispositivos. Por exemplo, o seguinte disco tem o Número

de barramento de local 0, ID de destino 9, LUN 0. De acordo com a tabela de volumes do EBS, o nome do dispositivo para esse local é `xvdj`.



Mapear dispositivos de disco para nomes de dispositivos

O driver de dispositivo de blocos da instância distribui os nomes de volume reais ao montar volumes.

Mapeamentos

- Volumes de armazenamento de instâncias
- Volumes do EBS

Volumes de armazenamento de instâncias

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes de armazenamento de instâncias não NVMe a volumes do Windows. O número de volumes de armazenamento de instâncias disponíveis é determinado pelo tipo de instância. Para obter mais informações, consulte Volumes de armazenamento de instâncias.

Local	Nome do dispositivo
Barramento número 0, ID de destino 78, LUN 0	xvdca
Barramento número 0, ID de destino 79, LUN 0	xvdcb
Barramento número 0, ID de destino 80, LUN 0	xvdcc
Barramento número 0, ID de destino 81, LUN 0	xvdcd
Barramento número 0, ID de destino 82, LUN 0	xvdce
Barramento número 0, ID de destino 83, LUN 0	xvdcf
Barramento número 0, ID de destino 84, LUN 0	xvdcg
Barramento número 0, ID de destino 85, LUN 0	xvdch
Barramento número 0, ID de destino 86, LUN 0	xvdci
Barramento número 0, ID de destino 87, LUN 0	xvdcj
Barramento número 0, ID de destino 88, LUN 0	xvdck
Barramento número 0, ID de destino 89, LUN 0	xvdcl

Volumes do EBS

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes do EBS não NVME a volumes do Windows.

Local	Nome do dispositivo
Barramento número 0, ID de destino 0, LUN 0	/dev/sda1
Barramento número 0, ID de destino 1, LUN 0	xvdb
Barramento número 0, ID de destino 2, LUN 0	xvdc
Barramento número 0, ID de destino 3, LUN 0	xvdd

Local	Nome do dispositivo
Barramento número 0, ID de destino 4, LUN 0	xvde
Barramento número 0, ID de destino 5, LUN 0	xvdf
Barramento número 0, ID de destino 6, LUN 0	xvdg
Barramento número 0, ID de destino 7, LUN 0	xvdh
Barramento número 0, ID de destino 8, LUN 0	xvdi
Barramento número 0, ID de destino 9, LUN 0	xvdj
Barramento número 0, ID de destino 10, LUN 0	xvdk
Barramento número 0, ID de destino 11, LUN 0	xvdl
Barramento número 0, ID de destino 12, LUN 0	xvdm
Barramento número 0, ID de destino 13, LUN 0	xvdn
Barramento número 0, ID de destino 14, LUN 0	xvdo
Barramento número 0, ID de destino 15, LUN 0	xvdp
Barramento número 0, ID de destino 16, LUN 0	xvdq
Barramento número 0, ID de destino 17, LUN 0	xvdr
Barramento número 0, ID de destino 18, LUN 0	xvds
Barramento número 0, ID de destino 19, LUN 0	xvdt
Barramento número 0, ID de destino 20, LUN 0	xvdu
Barramento número 0, ID de destino 21, LUN 0	xvdv
Barramento número 0, ID de destino 22, LUN 0	xvdw
Barramento número 0, ID de destino 23, LUN 0	xvdx

Local	Nome do dispositivo
Barramento número 0, ID de destino 24, LUN 0	xvdy
Barramento número 0, ID de destino 25, LUN 0	xvdz

Listar discos usando PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes.

Requisitos e limitações

- Requer o Windows Server 2012 ou posterior.
- Requer credenciais para obter o ID de volume do EBS. É possível configurar um perfil usando o Tools for PowerShell, ou anexar uma função do IAM à instância.
- Não suporta volumes NVMe.
- Não suporta discos dinâmicos.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o script a seguir e salve-o como `mapping.ps1` na instância do Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}
```

```
[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).SerialNumber) -
replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -ExpandProperty
 SystemName
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-EC2InstanceMetadata
 CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and Metadata
 is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}
```

```
Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*" +
 $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").ephemeral((Get-WmiObject -Class Win32_Diskdrive | Where-Object
 { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
```

```
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
   }
   Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
   }
   New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
   }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
 EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

A seguir está um exemplo de saída.

```
Disk  Partitions  DriveLetter   EbsVolumeId            Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------            ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Se você não tiver fornecido suas credenciais na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna `EbsVolumeId`.

Snapshots do Amazon EBS baseados no Windows VSS consistentes com a aplicação

> **Note**
>
> Os snapshots baseados em VSS do Windows e consistentes com a aplicação são compatíveis somente com as instâncias do Windows.

Você pode obter snapshots consistentes com a aplicação de todos os volumes do Amazon EBS anexados às instâncias do Windows do Amazon EC2 usando o Run Command do AWS Systems Manager. O processo de snapshot usa o Serviço de Cópias de Snapshot de Volume (VSS) do Windows para fazer backups no nível do volume do EBS de aplicações habilitadas para VSS. Os snapshots incluem dados das transações pendentes entre essas aplicações e o disco. Além disso, você não precisa desligar as instâncias ou desconectá-las quando precisar fazer backup de todos os volumes anexados.

Não há custos adicionais pelo uso de snapshots do EBS baseados no VSS. Você paga apenas pelos snapshots do EBS criados pelo processo de backup. Para obter mais informações, consulte Como é a cobrança pelos snapshots do Amazon EBS?

Conteúdo

- O que é o VSS?
- Pré-requisitos
- Criar snapshots do EBS habilitados para VSS
- Solucionar problemas de snapshots do EBS baseados no Windows VSS
- Restaurar volumes do EBS por meio de snapshots do EBS habilitados para VSS
- Histórico de versões da solução AWS VSS

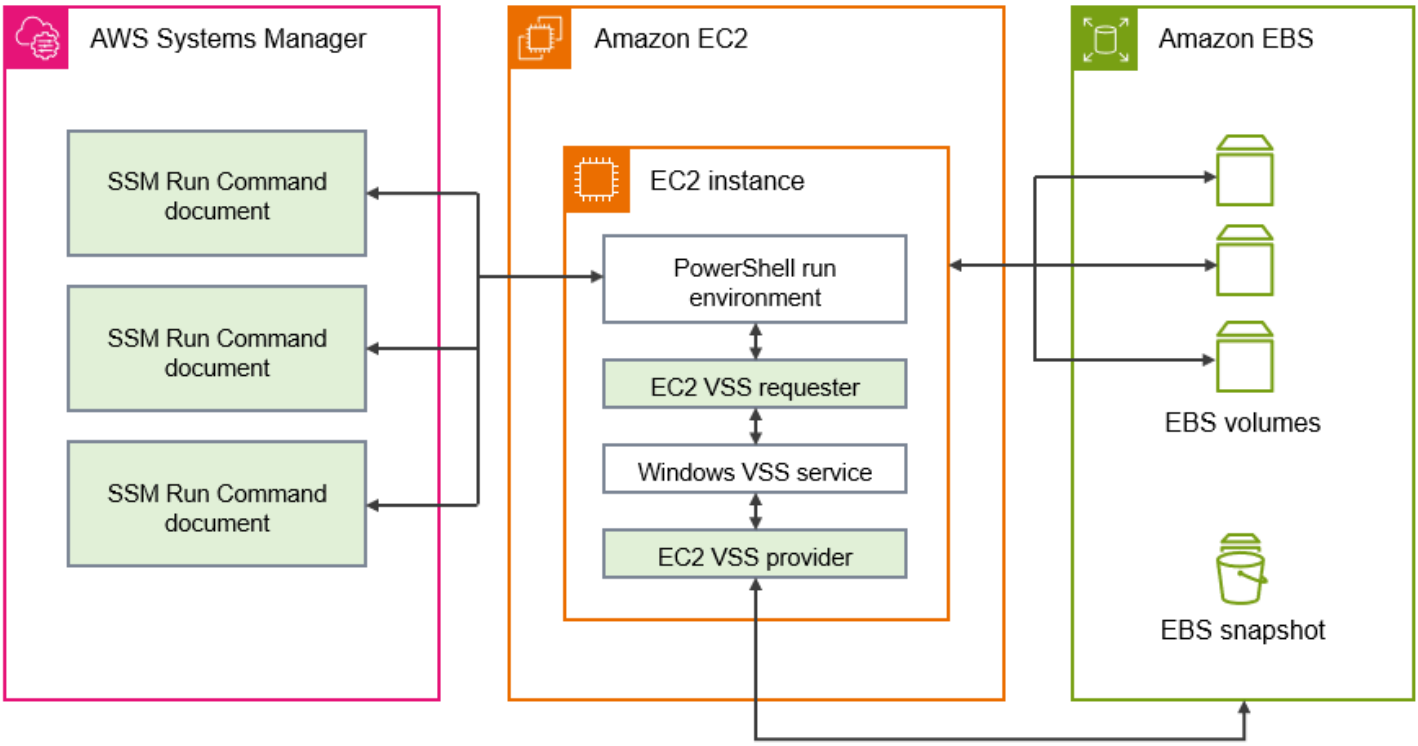
O que é o VSS?

O Serviço de Cópias de Snapshot de Volume (VSS) é uma tecnologia de backup e recuperação incluída no Microsoft Windows. Ele poderá criar cópias de backup, ou snapshots, de arquivos ou volumes do computador enquanto estiverem em uso. Para obter mais informações, consulte Serviço de Cópias de Snapshot de Volume.

Para criar um snapshot consistente com aplicações, os componentes do software a seguir são necessários.

- Serviço de VSS: parte do sistema operacional Windows
- Solicitante de VSS: o software que solicita a criação de cópias de sombra
- Gravador de VSS: normalmente fornecido como parte de uma aplicação, como o SQL Server, para garantir um conjunto de dados consistente para backup
- Provedor de VSS: o componente que cria as cópias de sombra dos volumes subjacentes

A solução de snapshots do Amazon EBS baseados no Windows VSS consiste em vários documentos do Run Command do Systems Manager (SSM) que facilitam a criação de backup e um pacote do Systems Manager Distributor, denominado `AwsVssComponents` que inclui um solicitante de VSS do EC2 e um provedor de VSS do EC2. O pacote `AwsVssComponents` deve ser instalado em instâncias do Windows do EC2 para obter snapshots dos volumes do EBS de maneira consistente com as aplicações. O diagrama a seguir ilustra a relação entre esses componentes de software.



Como funciona a solução de snapshots do Amazon EBS baseada no VSS

O processo para gerar scripts de snapshots do EBS baseados no VSS consistentes com a aplicação consiste nas etapas a seguir.

1. Preencha Pré-requisitos.
2. Insira os parâmetros para o documento do SSM `AWSEC2-VssInstallAndSnapshot` e execute esse documento usando o Run Command. Para ter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).
3. O serviço VSS do Windows na sua instância coordena todas as operações de E/S em andamento para a execução de aplicações.
4. O sistema libera todos os buffers de E/S e temporariamente todas as operações de E/S. A pausa dura no máximo dez segundos.
5. Durante essa pausa, o sistema cria snapshots de todos os volumes anexados à instância.
6. A pausa é suspensa e as operações de E/S são retomadas.
7. O sistema adiciona todos os snapshots recém-criados à lista de snapshots do EBS. O sistema marca todos os snapshots do EBS habilitados para VSS que foram criados com êxito por esse processo com AppConsistent:true.

8. Se for necessário restaurar usando um snapshot, será possível usar o processo padrão do EBS de criação de um volume por meio de um snapshot ou restaurar todos os volumes para uma instância usando um script de exemplo, conforme descrito em Restaurar volumes do EBS por meio de snapshots do EBS habilitados para VSS.

Pré-requisitos

Você pode criar snapshots do EBS baseados no VSS com o Run Command do Systems Manager, o AWS Backup ou o Amazon Data Lifecycle Manager. Os pré-requisitos a seguir se aplicam a todas as soluções.

Pré-requisitos

- Requisitos do sistema
- Permissões do IAM
- Componentes do VSS

Requisitos do sistema

Instalar o agente do Systems Manager

O VSS é orquestrado pelo AWS Systems Manager (Systems Manager) usando o PowerShell. Verifique se a versão `3.0.502.0` ou posterior do SSM Agent está instalada em sua instância do EC2. Se você já estiver usando uma versão mais antiga do SSM Agent, poderá atualizá-la usando o Run Command. Para obter mais informações, consulte Configuração do Systems Manager para instâncias do Amazon EC2 e Trabalhar com o SSM Agent em instâncias do Amazon EC2 para Windows Server no Guia do usuário do AWS Systems Manager.

Amazon EC2 Requisitos de instância do Windows

Os snapshots do EBS baseados no VSS são compatíveis com instâncias que executam o Windows Server 2012 ou posterior. Para versões mais antigas do Windows, consulte a tabela de suporte à versão do Windows em Histórico de versões da solução AWS VSS.

Versão do .NET Framework

O pacote `AwsVssComponents` requer o .NET Framework versão `4.6` ou posterior. As versões do sistema operacional Windows anteriores ao Windows Server 2016 usam como padrão uma versão anterior do .NET Framework. Se a sua instância usar uma versão anterior do .NET Framework, você deverá instalar a versão `4.6` ou posterior usando o Windows Update.

Versão do AWS Tools for Windows PowerShell

Verifique se sua instância está executando a versão `3.3.48.0` ou posterior do AWS Tools for Windows PowerShell. Para verificar a versão, execute o comando a seguir na instância em um terminal do PowerShell.

```
C:\> Get-AWSPowerShellVersion
```

Para atualizar o AWS Tools for Windows PowerShell na sua instância, consulte Instalar o AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.

Versão Windows Powershell

Verifique se sua instância está executando o Windows PowerShell, versão principal `3`, `4` ou `5`. Para verificar a versão, execute o comando a seguir na instância em um terminal do PowerShell.

```
C:\> $PSVersionTable.PSVersion
```

Modo de linguagem do PowerShell

Certifique-se de que sua instância tenha o modo de idioma da PowerShell definido como `FullLanguage`. Para obter mais informações, consulte about_Language_Modes na documentação da Microsoft.

Permissões do IAM

O perfil do IAM anexado à instância do Windows do Amazon EC2 deve ter permissão para criar snapshots consistentes com aplicações ao usar o VSS. Para conceder as permissões necessárias, é possível anexar a política `AWSEC2VssSnapshotPolicy` ao seu perfil de instância.

A política possibilita que o Systems Manager execute as seguintes ações:

- Criar e realizar a marcação de snapshots do EBS;
- Criar e realizar a marcação de imagens de máquina da Amazon (AMIs);
- Anexar metadados, como o ID do dispositivo, às etiquetas de snapshot padrão criadas pelo VSS.

Tópicos

- Anexar a política de snapshot habilitada para o VSS ao perfil de instância
- Política gerenciada para a criação de snapshots do VSS

- Política legada (não é mais compatível)

Anexar a política de snapshot habilitada para o VSS ao perfil de instância

Para conceder permissões para snapshots habilitados para o VSS para a instância, anexe a política gerenciada AWSEC2VssSnapshotPolicy à função do perfil de instância conforme apresentado a seguir. É importante garantir que a instância atenda a todos os Requisitos do sistema.

> **Note**
>
> Para usar a política gerenciada, a instância deve ter o pacote `AwsVssComponents` na versão `2.3.1` ou em versões posteriores instalado. Para obter o histórico de versões, consulte Versões do pacote AwsVssComponents.
> Se você tiver uma versão anterior do pacote `AwsVssComponents` instalada na instância, consulte Política legada.

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis para visualizar uma lista de perfis do IAM aos quais você tem acesso.
3. Selecione o link Nome do perfil para o perfil anexado à instância. Isso abre a página de detalhes do perfil.
4. Para anexar a política gerenciada, escolha a opção Adicionar permissões, localizada no canto superior direito do painel da lista. Em seguida, selecione Anexar políticas na lista suspensa.
5. Para agilizar os resultados, insira o nome da política na barra de pesquisa (`AWSEC2VssSnapshotPolicy`).
6. Marque a caixa de seleção ao lado do nome da política a ser anexada e escolha Adicionar permissões.

Política gerenciada para a criação de snapshots do VSS

Uma política gerenciada pela AWS é uma política autônoma que a Amazon fornece aos clientes da AWS. As políticas gerenciadas pela AWS são projetadas para conceder permissões para casos de uso conhecidos. Não é possível alterar as permissões definidas nas políticas gerenciadas pela AWS. No entanto, você pode copiar a política e usá-la como referência para o desenvolvimento de uma política gerenciada pelo cliente específica ao seu caso de uso.

Para ter mais informações sobre as políticas gerenciadas da AWS, consulte Políticas gerenciadas da AWS no Guia do usuário do IAM.

Para usar a política AWSEC2VssSnapshotPolicy, que é uma política gerenciada, você pode anexá-la ao perfil do IAM vinculado às instâncias do Windows do EC2. Essa política possibilita que a solução VSS do EC2 crie e adicione etiquetas a imagens de máquina da Amazon (AMIs) e a snapshots do EBS. Para anexar a política, consulte Anexar a política de snapshot habilitada para o VSS ao perfil de instância.

Permissões concedidas pelo AWSEC2VssSnapshotPolicy

A política AWSEC2VssSnapshotPolicy inclui as seguintes permissões do Amazon EC2:

- ec2:CreateTags: adicione etiquetas a snapshots e a AMIs do EBS para ajudar na identificação e na categorização dos recursos.
- ec2:DescribeInstanceAttribute: recupere os volumes do EBS e os mapeamentos de dispositivos de bloco correspondentes que estão anexados à instância de destino.
- ec2:CreateSnapshots: crie snapshots de volumes do EBS.
- ec2:CreateImage: crie uma AMI usando uma instância do EC2 em execução.
- ec2:DescribeImages: recupere as informações para AMIs e snapshots do EC2.
- ec2:DescribeSnapshots: defina o horário de criação e o status dos snapshots para verificar a consistência da aplicação.

Exemplo de política

A seguir há um exemplo da política do AWSEC2VssSnapshotPolicy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DescribeInstanceInfo",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceAttribute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
```

```
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessVolume",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ]
```

```
        },
        {
            "Sid": "CreateImageWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateImageAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateTagsOnResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateImage",
```

```
                        "CreateSnapshots"
                    ]
                }
            }
        },
        {
            "Sid": "CreateTagsAfterResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/AwsVssConfig": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AppConsistent",
                        "Device"
                    ]
                }
            }
        },
        {
            "Sid": "DescribeImagesAndSnapshots",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Simplificação das permissões para casos de uso específicos (avançado)

A política gerenciada `AWSEC2VssSnapshotPolicy` inclui permissões para todas as maneiras pelas quais é possível criar snapshots habilitados para o VSS. É possível criar uma política personalizada que inclua somente as permissões de que você precisa.

Caso de uso: criar uma AMI | Caso de uso: usar o serviço AWS Backup

Caso use exclusivamente a opção `CreateAmi` ou crie snapshots habilitados para o VSS somente por meio do serviço AWS Backup, você poderá simplificar as declarações de política conforme apresentado a seguir.

- Omissão das declarações de política identificadas pelos seguintes IDs de declaração (SIDs):
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Ajuste da instrução `CreateTagsOnResourceCreation` da seguinte maneira:
  - Remova `arn:aws:ec2:*:*:snapshot/*` dos recursos.
  - Remova `CreateSnapshots` da condição `ec2:CreateAction`.
- Ajuste da instrução `CreateTagsAfterResourceCreation` para remover `arn:aws:ec2:*:*:snapshot/*` dos recursos.
- Ajuste da instrução `DescribeImagesAndSnapshots` para remover `ec2:DescribeSnapshots` da ação da instrução.

Caso de uso: somente snapshots

Se você não usar a opção `CreateAmi`, poderá simplificar as declarações de política conforme apresentado a seguir.

- Omissão das declarações de política identificadas pelos seguintes IDs de declaração (SIDs):
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Ajuste da instrução `CreateTagsOnResourceCreation` da seguinte maneira:
  - Remova `arn:aws:ec2:*:*:image/*` dos recursos.
  - Remova `CreateImage` da condição `ec2:CreateAction`.
- Ajuste da instrução `CreateTagsAfterResourceCreation` para remover `arn:aws:ec2:*:*:image/*` dos recursos.
- Ajuste da instrução `DescribeImagesAndSnapshots` para remover `ec2:DescribeImages` da ação da instrução.

> **Note**
>
> Para garantir que a política personalizada funcione conforme o esperado, recomendamos analisar e incorporar atualizações regularmente à política gerenciada.

Política legada (não é mais compatível)

A política legada que concede permissão para snapshots habilitados para o VSS inclui as permissões do IAM recomendadas antes do lançamento da política gerenciada `AWSEC2VssSnapshotPolicy`.

Se você configurou um perfil de instância com a política legada, poderá continuar a usá-lo. No entanto, para garantir que a política permaneça atualizada com as práticas recomendadas mais recentes do IAM e que defina as declarações de política de acordo, recomendamos substituir a política legada pela política gerenciada `AWSEC2VssSnapshotPolicy`.

Exemplo de política

O exemplo de política apresentado a seguir usa o atributo `ec2:DescribeInstanceAttribute`, que tem suporte nas versões 2.2.1 e em versões posteriores do pacote `AwsVssComponents`. Se você tiver uma versão mais antiga do pacote `AwsVssComponents` instalada, deverá substituí-la pela ação `ec2:DescribeInstances`.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": [
    "arn:aws:ec2:*::snapshot/*",
    "arn:aws:ec2:*::image/*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstanceAttribute",
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots",
```

```
    "ec2:CreateImage",
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  }
 ]
}
```

Para obter mais informações sobre as políticas gerenciadas pelo IAM, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Componentes do VSS

Para criar snapshots consistentes com a aplicação nos sistemas operacionais Windows, o pacote `AwsVssComponents` deve estar instalado na instância. O pacote contém um VSS Agent do EC2 na instância que funciona como solicitante do VSS e um provedor do VSS do EC2 para volumes do EBS.

Existem várias maneiras de instalar o componente em uma instância existente:

- (Recomendado) Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado). Se necessário, isso faz a instalação ou a atualização automaticamente toda vez que for executado.
- Instalar manualmente os componentes do VSS em uma instância.
- Atualizar os componentes do VSS nas instâncias segundo agendado.

Você também pode criar uma AMI com o EC2 Image Builder que usa o componente gerenciado `aws-vss-components-windows` para instalar o pacote `AwsVssComponents` da imagem. O componente gerenciado usa o AWS Systems Manager Distributor para instalar o pacote. Depois que o Image Builder criar a imagem, toda instância que você executar na AMI associada terá o pacote VSS instalado nela. Para obter mais informações sobre como criar uma AMI com o pacote VSS instalado, consulte Componentes gerenciados do pacote do Distributor para Windows no Guia do usuário do EC2 Image Builder.

Conteúdo

- Instalar manualmente os componentes do VSS em uma instância
- Atualizar os componentes do VSS nas instâncias segundo agendado

Instalar manualmente os componentes do VSS em uma instância

Sua instância do EC2 para Windows deve ter componentes VSS instalados antes de criar snapshots consistentes com aplicações usando o Systems Manager. Se você não executar o documento do comando `AWSEC2-VssInstallAndSnapshot` para instalar ou atualizar automaticamente o pacote toda vez que criar snapshots consistentes com aplicações, deverá instalar o pacote manualmente.

Você também deve fazer a instalação manualmente se planeja usar um dos métodos a seguir para criar snapshots consistentes com aplicações usando a instância do EC2.

- Criar snapshots do VSS usando o AWS Backup
- Criar snapshots do VSS usando o Amazon Data Lifecycle Manager

Se precisar fazer uma instalação manual, recomendamos usar o pacote de componentes do AWS VSS mais recente para melhorar a confiabilidade e o desempenho de snapshots consistentes com aplicações nas suas instâncias do EC2 para Windows.

> **Note**
>
> Para instalar ou atualizar automaticamente o pacote `AwsVssComponents` sempre que você criar snapshots consistentes com a aplicação, recomendamos que use o Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`. Para ter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).

Para instalar os componentes do VSS em uma instância do Windows do Amazon EC2, siga as etapas para o ambiente de sua preferência.

Console

Instalar os componentes do VSS usando o SSM Distributor

1. Abra o console do AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, selecione Executar comando.
3. Selecione Run command (Executar comando).

4. Em Command document (Documento do comando), selecione o botão ao lado de AWS-ConfigureAWSPackage.
5. Em Command parameters (Parâmetros do comando), faça o seguinte:
   a. Verifique se Action (Ação) está definida como Install (Instalar).
   b. Em Name (Nome), insira `AwsVssComponents`.
   c. Em Versão, insira uma versão ou deixe o campo vazio para que o Systems Manager instale a versão mais recente.
6. Em Targets (Destinos), identifique as instâncias nas quais você deseja executar essa operação especificando tags ou selecionando instâncias manualmente.

   > **Note**
   >
   > Se você optar por selecionar manualmente as instâncias e uma instância que você espera visualizar não estiver incluída na lista, consulte Algumas das minhas instâncias estão ausentes no Manual do usuário do AWS Systems Manager para obter dicas para solução de problemas.

7. Para Other parameters (Outros parâmetros):
   - (Opcional) Em Comment (Comentário), digite informações sobre esse comando.
   - Em Timeout (seconds) (Tempo limite [segundos]), especifique o número de segundos para o sistema aguardar até a falha de execução do comando total.
8. (Opcional) Em Rate control (Controle de taxa):
   - Em Concurrency (Concorrência), especifique um número ou uma porcentagem de instâncias nas quais executar o comando ao mesmo tempo.

     > **Note**
     >
     > Se tiver selecionado destinos escolhendo tags do Amazon EC2 e não tiver certeza de quantas instâncias usam tags selecionadas, limite o número de instâncias que podem executar o documento ao mesmo tempo especificando uma porcentagem.

   - Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outras instâncias depois de falhar em alguns ou em uma porcentagem de instâncias. Por exemplo, se você especificar três erros, o Systems Manager deixará de enviar o comando

quando o 4° erro for recebido. As instâncias que continuam processando o comando também podem enviar erros.

9. (Opcional) Na seção Output options (Opções de saída), se você quiser salvar a saída de comando em um arquivo, selecione a caixa ao lado de Enable writing to an S3 bucket (Habilitar a gravação em um bucket do S3). Especifique o bucket e os nomes (de pastas) de prefixo (opcional).

   > **Note**
   >
   > As permissões do S3 que concedem a possibilidade de gravar os dados em um bucket do S3 são as do perfil de instância atribuído à instância, e não as do usuário que realiza essa tarefa. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager no Manual do usuário do AWS Systems Manager.

10. (Opcional) Especifique opções para SNS notifications (Notificações do SNS).

    Para obter informações sobre como configurar notificações do Amazon SNS para o Run Command, consulte Configuração das notificações do Amazon SNS para o AWS Systems Manager.

11. Escolha Run.

AWS CLI

Use o procedimento a seguir para baixar e instalar o pacote `AwsVssComponents` em suas instâncias usando o Run Command por meio da AWS CLI. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS por meio da AWS CLI

- Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
aws ssm send-command \
  --document-name "AWS-ConfigureAWSPackage" \
  --instance-ids "i-01234567890abcdef" \
  --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Use o procedimento a seguir para fazer baixar e instalar o pacote `AwsVssComponents` em suas instâncias usando o Run Command por meio do Tools for Windows PowerShell. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS usando o AWS Tools for Windows PowerShell

- Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'action'='Install';'name'='AwsVssComponents'}
```

Verifique a assinatura nos componentes do AWS VSS

Use o procedimento a seguir para verificar a assinatura no pacote `AwsVssComponents`.

1. Conecte-se à sua instância do Windows. Para ter mais informações, consulte Conectar-se à sua instância do Windows do .
2. Navegue até C:\Program Files\Amazon\AwsVssComponents.
3. Abra o menu de contexto de `ec2-vss-agent.exe` (clique com o botão direito do mouse) e escolha Propriedades.
4. Navegue até a guia Assinaturas digitais e verifique se o nome do signatário é Amazon Web Services Inc.
5. Use as etapas anteriores para verificar a assinatura em `Ec2VssInstaller` e `Ec2VssProvider.dll`.

Atualizar os componentes do VSS nas instâncias segundo agendado

Recomendamos que você sempre mantenha os componentes do VSS atualizados com a versão mais recente recomendada. Existem diversas maneiras diferentes de atualizar componentes quando uma nova versão do pacote `AwsVssComponents` é lançada.

Métodos de atualização

- Você pode repetir as etapas descritas em Instalar manualmente os componentes do VSS em uma instância quando uma nova versão dos componentes do AWS VSS é lançada.
- Você pode configurar uma associação do State Manager do Systems Manager para baixar e instalar automaticamente os componentes novos ou atualizados do VSS quando o pacote `AwsVssComponents` ficar disponível.
- Para instalar ou atualizar automaticamente o pacote `AwsVssComponents` sempre que você criar snapshots consistentes com a aplicação, ao usar o Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`.

> **Note**
>
> Recomendamos que você use o Systems Manager para executar o documento de comando `AWSEC2-VssInstallAndSnapshot`, que instala ou atualiza automaticamente o pacote `AwsVssComponents` antes de criar snapshots consistentes com a aplicação. Para ter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).

Para criar uma associação do State Manager do Systems Manager, siga as etapas do ambiente de sua preferência.

Console

Criar uma associação do Gerenciador de Estados usando o console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha State Manager.

   Ou, se a página inicial do Systems Manager abrir primeiro, abra o painel de navegação e escolha Gerenciador de Estados.
3. Escolha Create association (Criar associação).
4. No campo Association Name (Nome da associação), insira um nome descritivo.
5. Na lista Documento, escolha AWS-ConfigureAWSPackage.

6. Na seção Parameters Parâmetros), escolha Install (Instalar) na lista Action (Ação).
7. Para Installation type (Tipo de instalação), escolha Uninstall and reinstall (Desinstalar e reinstalar).
8. No campo Name (Nome), insira `AwsVssComponents`. Você pode manter os campos Version (Versão) e Additional Arguments (Argumentos adicionais) vazios.
9. Na seção Select Targets by, escolha uma opção.

   > **Note**
   >
   > Se você optar por especificar instâncias de destino usando tags e especificar tags que são mapeadas para instâncias do Linux, a associação será bem-sucedida na instância do Windows, mas falhará nas instâncias do Linux. O status geral da associação mostra Failed.

10. Na seção Specify schedule, escolha uma opção.
11. Na seção Advanced options (Opções avançadas), em Compliance severity (Severidade de conformidade), escolha um nível de gravidade para a associação. Para obter mais informações, consulte Sobre a conformidade de associações do Gerenciador de Estados. Em Calendários de alteração, selecione um calendário de alterações pré-configurado. Para obter mais informações, consulte Calendário de alterações do AWS Systems Manager.
12. Em Controle de taxa, faça o seguinte:

    - Em Concurrency (Concorrência), especifique um número ou uma porcentagem de nós gerenciados nos quais executar o comando ao mesmo tempo.
    - Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outros nós depois de falhar em alguns ou em uma porcentagem de nós.

13. (Opcional) Em Opções de saída, para salvar a saída de comando em um arquivo, selecione a caixa Habilitar gravação da saída no S3. Digite os nomes de bucket e prefixo (pastas) nas caixas de texto.
14. Escolha Create Association (Criar associação) e, em seguida, Close (Fechar). O sistema tenta criar a associação nas instâncias e aplicar imediatamente o estado.

    > **Note**
    >
    > Se as instâncias do EC2 para o Windows Server mostrarem o status Com falha, verifique se o SSM Agent está sendo executado na instância e se a instância está

configurada com um perfil do AWS Identity and Access Management (IAM) para o Systems Manager. Para obter mais informações, consulte Configurar o AWS Systems Manager.

AWS CLI

Você pode executar o comando create-association da AWS CLI para atualizar um pacote do Distributor segundo agendado sem deixar a aplicação associada offline. Somente arquivos novos ou atualizados no pacote são substituídos.

Criar uma associação do Gerenciador de Estados usando a AWS CLI

1. Instale e configure o AWS CLI, caso ainda não o tenha feito. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI.
2. Execute o comando a seguir para criar uma associação. O valor de `--name`, o nome do documento, é sempre `AWS-ConfigureAWSPackage`. O comando a seguir usa a chave `InstanceIds` para especificar as instâncias de destino.

```
aws ssm create-association \
 --name "AWS-ConfigureAWSPackage" \
 --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["AwsVssComponents"]}' \
 --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-01234567890abcdef\",
\"i-000011112222abcde\"]}]
```

Para obter mais informações sobre outras opções que podem ser usadas com o comando `create-association`, consulte create-association na seção AWS Systems Manager da AWS CLI Command Reference.

Criar snapshots do EBS habilitados para VSS

Esta seção inclui as etapas para criar snapshots do EBS habilitados para VSS.

Você pode criar snapshots do EBS habilitados para VSS dos volumes do EBS anexados às suas instâncias do EC2. Antes de tentar criar um snapshot habilitado para VSS, verifique se os Pré-requisitos foram atendidos.

Tópicos

- Criação de snapshots do VSS com documentos de comando do AWS Systems Manager
- Criar snapshots do VSS usando o AWS Backup
- Criar snapshots do VSS usando o Amazon Data Lifecycle Manager

Criação de snapshots do VSS com documentos de comando do AWS Systems Manager

Você pode usar documentos de comando do AWS Systems Manager para criar snapshots habilitados para VSS. O conteúdo a seguir apresenta os documentos de comando disponíveis e os parâmetros de runtime que os documentos usam para criar seus snapshots.

Antes de usar qualquer um dos documentos de comando do Systems Manager, verifique se você atendeu a todos os Pré-requisitos.

Tópicos

- Parâmetros para documentos de snapshot de VSS do Systems Manager
- Execução de documentos de comando de snapshot de VSS do Systems Manager

Parâmetros para documentos de snapshot de VSS do Systems Manager

Todos os documentos do Systems Manager que criam snapshots de VSS usam os seguintes parâmetros, exceto onde indicado:

ExcludeBootVolume (string, opcional)

Se você criar snapshots, essa configuração excluirá os volumes de inicialização do processo de backups. Para excluir os volumes de inicialização dos snapshots, defina ExcludeBootVolume como **`True`** e CreateAmi como `False`.

Se você criar uma AMI para o backup, esse parâmetro deverá ser definido como `False`. O valor padrão desse parâmetro é `False`.

NoWriters (string, opcional)

Para excluir os gravadores do VSS do processo de snapshots, defina esse parâmetro como `True`. Excluir gravadores do VSS pode ajudar você a resolver conflitos com componentes de backup de VSS de terceiros. O valor padrão desse parâmetro é `False`.

CopyOnly (string, opcional)

Se você estiver usando o backup nativo do SQL Server além do AWS VSS, fazer um backup somente cópia evitará que o AWS VSS rompa a cadeia nativa de backup diferencial. Para realizar uma operação de backup somente cópia, defina esse parâmetro como `True`.

O valor padrão desse parâmetro é `False`, que faz com que o AWS VSS faça uma operação de backup total.

CreateAmi (string, opcional)

Para criar uma imagem de máquina da Amazon (AMI) habilitada para VSS para fazer backup da instância, defina esse parâmetro como `True`. O valor padrão desse parâmetro é `False`, que faz backup da instância com um snapshot do EBS.

Para obter mais informações sobre como criar uma AMI de uma instância, consulte Criação de uma AMI baseada no Amazon EBS.

AmiName (string, opcional)

Se a opção CreateAmi for definida como `True`, especifique o nome da AMI que o backup criará.

description (string, opcional)

Especifique uma descrição para os snapshots ou para a imagem que esse processo vai criar.

tags (string, opcional)

Recomendamos marcar seus snapshots e imagens com tags para facilitar a localização e o gerenciamento dos seus recursos, por exemplo, para restaurar volumes de uma lista de snapshots. O sistema adiciona a chave `Name` com um valor em branco em que você pode especificar o nome que deseja aplicar aos snapshots ou imagens de saída.

Se desejar especificar tags adicionais, separe-as com ponto e vírgulas. Por exemplo, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

Por padrão, o sistema adiciona as seguintes tags reservadas para snapshots e imagens habilitados para VSS.

- Dispositivo: para snapshots habilitados para VSS, esse é o nome do dispositivo do volume do EBS capturado pelo snapshot.
- AppConsistent: essa tag indica a criação bem-sucedida de um snapshot ou AMI habilitado para VSS.

- AwsVSSConfig: identifica snapshots e AMIs criados com o VSS habilitado. A tag inclui meta-informações, como a versão de `AwsVssComponents`.

> **Warning**
>
> Especificar qualquer uma dessas tags reservadas na sua lista de parâmetros causará um erro.

executionTimeout (string, opcional)

Especifique o tempo máximo em segundos para executar o processo de criação de snapshots na instância ou para criar uma AMI da instância. Aumentar esse tempo limite permite que o comando aguarde mais tempo até o VSS iniciar seu congelamento e concluir a marcação dos recursos criados. Esse tempo limite só se aplica às etapas de criação de snapshot ou AMI. A etapa inicial para instalar ou atualizar o pacote `AwsVssComponents` não está incluída no tempo limite.

CollectDiagnosticLogs (string, opcional)

Para coletar mais informações durante as etapas de criação de snapshots e AMIs, defina esse parâmetro como "`True`". O valor padrão desse parâmetro é "`False`". Os logs de diagnóstico consolidados são salvos como um arquivo no formato `.zip` no seguinte local em sua instância:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

VssVersion (string, opcional)

Somente para o documento `AWSEC2-VssInstallAndSnapshot`, você pode especificar o parâmetro `VssVersion` para instalar uma versão específica do pacote `AwsVssComponents` na instância. Deixe esse parâmetro em branco para instalar a versão padrão recomendada.

Se a versão especificada do pacote `AwsVssComponents` já estiver instalada, o script pulará a etapa de instalação e passará para a etapa de backup. Para obter uma lista das versões do pacote `AwsVssComponents` e suporte operacional, consulte Histórico de versões da solução AWS VSS.

Execução de documentos de comando de snapshot de VSS do Systems Manager

Você pode criar snapshots do EBS habilitados para VSS com documentos de comando do AWS Systems Manager da maneira a seguir.

Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado)

Quando você usa o AWS Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`, o script executa as etapas a seguir.

1. O script primeiro instala ou atualiza o pacote `AwsVssComponents` na instância, dependendo de ele já estar ou não instalado.
2. O script cria os snapshots consistentes com a aplicação após a conclusão da primeira etapa.

Para executar o documento `AWSEC2-VssInstallAndSnapshot`, siga as etapas para o ambiente de sua preferência.

Console

Criar snapshots do EBS habilitados para VSS usando o console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. Selecione Run Command no painel de navegação. Isso mostra uma lista dos comandos que estão sendo executados atualmente na conta, se aplicável.
3. Selecione Run command. Isso abre uma lista dos documentos de comando a que você tem acesso.
4. Selecione `AWSEC2-VssInstallAndSnapshot` na lista de documentos de comando. Para otimizar os resultados, você pode inserir todo ou parte do nome do documento. Você também pode filtrar pelo proprietário, por tipos de plataforma ou por tags.

   Quando você seleciona um documento de comando, os detalhes são preenchidos abaixo da lista.
5. Selecione `Default version at runtime` na lista Versão do documento.
6. Configure os parâmetros de comando para definir como `AWSEC2-VssInstallAndSnapshot` instalará o pacote `AwsVssComponents` e fará backup com snapshots ou com uma AMI do VSS. Para obter detalhes dos parâmetros, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.
7. Em Seleção de alvos, especifique as tags ou selecione manualmente as instâncias em que a operação deve ser executada.

> **Note**
>
> Se selecionar manualmente as instâncias e uma instância que você espera ver não estiver incluída na lista, consulte Onde estão minhas instâncias? para obter dicas de solução de problemas.

8. Para obter parâmetros adicionais para definir o comportamento do Run Command do Systems Manager, como, Controle da taxa, insira os valores como descrito em Executar comandos no console.
9. Escolha Run.

   Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando do Systems Manager para obter detalhes do motivo da falha. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de volumes do EBS.

AWS CLI

Você pode executar os comandos a seguir na AWS CLI para criar snapshots do EBS habilitados para VSS e obter o status de criação do snapshot.

Criar snapshots do EBS habilitados para VSS

Execute o comando a seguir para criar snapshots do EBS habilitados para VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `--instance-ids`. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Se bem-sucedido, o documento de comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando

as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

Obter status do comando

Para obter o status atual dos snapshots, execute o comando a seguir usando o ID de comando retornado de send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Execute os comandos a seguir com o AWS Tools for Windows PowerShell para criar snapshots do EBS habilitados para VSS e obter o status atual do runtime da criação da saída. Especifique os parâmetros descritos na lista anterior para modificar o comportamento do processo de snapshots.

Criar snapshots do EBS habilitados para VSS usando o Tools for Windows PowerShell

Execute o comando a seguir para criar snapshots ou AMIs do EBS habilitados para VSS.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Obter status do comando

Para obter o status atual dos snapshots, execute o comando a seguir usando o ID de comando retornado de Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

Execução do documento de comandos AWSEC2-CreateVssSnapshot

Para executar o documento `AWSEC2-CreateVssSnapshot`, siga as etapas para o ambiente de sua preferência.

Console

Criar snapshots do EBS habilitados para VSS usando o console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. Selecione Run Command no painel de navegação. Isso mostra uma lista dos comandos que estão sendo executados atualmente na conta, se aplicável.
3. Selecione Run command. Isso abre uma lista dos documentos de comando a que você tem acesso.
4. Selecione `AWSEC2-CreateVssSnapshot` na lista de documentos de comando. Para otimizar os resultados, você pode inserir todo ou parte do nome do documento. Você também pode filtrar pelo proprietário, por tipos de plataforma ou por tags.

   Quando você seleciona um documento de comando, os detalhes são preenchidos abaixo da lista.
5. Selecione `Default version at runtime` na lista Versão do documento.
6. Configure os Parâmetros de comando para definir como `AWSEC2-CreateVssSnapshot` fará backup com snapshots ou com uma AMI do VSS. Para obter detalhes dos parâmetros, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.
7. Em Seleção de alvos, especifique as tags ou selecione manualmente as instâncias em que a operação deve ser executada.

   > **Note**
   >
   > Se selecionar manualmente as instâncias e uma instância que você espera ver não estiver incluída na lista, consulte Onde estão minhas instâncias? para obter dicas de solução de problemas.
8. Para obter parâmetros adicionais para definir o comportamento do Run Command do Systems Manager, como, Controle da taxa, insira os valores como descrito em Executar comandos no console.

9. Escolha Run.

   Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando do Systems Manager para obter detalhes do motivo da falha. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de volumes do EBS.

AWS CLI

Você pode executar o comando a seguir na AWS CLI para criar snapshots do EBS habilitados para VSS.

Criar snapshots do EBS habilitados para VSS

Execute o comando a seguir para criar snapshots do EBS habilitados para VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `--instance-ids`. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Se bem-sucedido, o documento de comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

PowerShell

Execute o comando a seguir com o AWS Tools for Windows PowerShell para criar snapshots do EBS habilitados para VSS.

Criar snapshots do EBS habilitados para VSS usando o Tools for Windows PowerShell

Execute o comando a seguir para criar snapshots do EBS habilitados para VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `InstanceId`. Você pode

especificar mais de uma instância para a qual criar snapshots. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de snapshots do EBS.

Execução de documentos de comando para um cluster de failover do Windows com armazenamento compartilhado do EBS

Você pode usar qualquer um dos procedimentos de linha de comando descritos na seção anterior para criar um snapshot habilitado para VSS. O documento de comando (`AWSEC2-VssInstallAndSnapshot` ou `AWSEC2-CreateVssSnapshot`) deve ser executado no nó primário do cluster. O documento falhará nos nós secundários, pois eles não têm acesso aos discos compartilhados. Se o primário e o secundário mudarem dinamicamente, você poderá executar o documento AWS Systems Manager Executar comando em vários nós com a expectativa de que o comando seja bem-sucedido no nó primário e falhe nos nós secundários.

Execução do documento de comando do SSM AWSEC2-ManageVssIO

É possível usar o script a seguir e o documento predefinido `AWSEC2-ManageVssIO` do SSM para pausar temporariamente as operações de E/S, criar snapshots do EBS habilitados para VSS e reiniciar as operações de E/S. Esse processo é executado no contexto do usuário que executa o comando. Se o usuário tiver permissão suficiente para criar e marcar snapshots, o AWS Systems Manager poderá criar e marcar snapshots do EBS habilitados para VSS sem precisar de outra função de snapshot do IAM na instância.

Ao contrário, o documento de comando (`AWSEC2-VssInstallAndSnapshot` ou `AWSEC2-CreateVssSnapshot`) exige que você atribua um perfil de snapshot do IAM a cada instância para

a qual deseja criar snapshots do EBS. Se não desejar fornecer mais permissões do IAM às suas instâncias por motivo de política ou conformidade, poderá usar o script a seguir.

Antes de começar

Observe os detalhes essenciais a seguir sobre esse processo:

- Esse processo usa um script do PowerShell (`CreateVssSnapshotAdvancedScript.ps1`) para fazer snapshots de todos os volumes das instâncias que você especificar, com exceção dos volumes raiz. Se você precisar fazer snapshots dos volumes raiz, use o documento SSM do `AWSEC2-CreateVssSnapshot`.
- O script chama o documento `AWSEC2-ManageVssIO` duas vezes. A primeira vez com o parâmetro `Action` definido como `Freeze`, que pausa todas as operações de E/S nas instâncias. Na segunda vez, o parâmetro `Action` é definido como `Thaw`, que força a retomada das operações de E/S.
- Não tente usar o documento `AWSEC2-ManageVssIO` sem usar o script CreateVssSnapshotAdvancedScript.ps1. A estrutura de VSS da Microsoft requer que as ações `Freeze` e `Thaw` sejam chamadas a não mais de dez segundos de distância entre uma e outra, e chamar manualmente essas ações sem o script pode resultar em erros.

Para criar snapshots do EBS habilitados para VSS usando o documento **`AWSEC2-ManageVssIO`** do SSM

1. Faça download do arquivo CreateVssSnapshotAdvancedScript.zip e extraia os conteúdos do arquivo.
2. Abra `CreateVssSnapshotAdvancedScript.ps1` em um editor de texto, edite a chamada de amostra, na parte inferior do script, com um ID válido da instância do EC2, a descrição do snapshot e os valores de tag desejados e execute o script a partir do PowerShell.

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução. Se o comando tiver sido concluído com êxito, mas tiver havido falha no backup de um volume específico, será possível solucionar essa falha na lista de volumes do EBS.

> **Note**
>
> Para automatizar os backups, você pode criar uma tarefa da janela de manutenção do AWS Systems Manager que use o documento `AWSEC2-VssInstallAndSnapshot`. Para obter mais informações, consulte Trabalhar com janelas de manutenção (console) no Manual do usuário do AWS Systems Manager.

Criar snapshots do VSS usando o AWS Backup

Você pode criar um backup do VSS usando o AWS Backup ao habilitar o VSS no console ou na CLI. Verifique se os pré-requisitos foram atendidos antes de criar o plano de backup habilitado para VSS. Para obter mais informações, consulte Creating Windows VSS backups no Guia do desenvolvedor do AWS Backup.

> **Note**
>
> O AWS Backup não instala automaticamente o pacote `AwsVssComponents` na instância. Você deve realizar uma instalação manual na instância. Para ter mais informações, consulte Instalar manualmente os componentes do VSS em uma instância.

Criar snapshots do VSS usando o Amazon Data Lifecycle Manager

Você pode criar snapshots do VSS usando o Amazon Data Lifecycle Manager habilitando scripts prévios e posteriores nas políticas de ciclo de vida de snapshots. Para ter mais informações, consulte https://docs.aws.amazon.com/ebs/latest/userguide/automate-app-consistent-backups.html.

> **Note**
>
> O Amazon Data Lifecycle Manager não instala automaticamente o pacote `AwsVssComponents` na instância. Você deve realizar uma instalação manual na instância. Para ter mais informações, consulte Instalar manualmente os componentes do VSS em uma instância.

Solucionar problemas de snapshots do EBS baseados no Windows VSS

Antes de tentar qualquer outra etapa de solução de problemas, recomendamos verificar os detalhes a seguir.

- Certifique-se de que você atendeu a todos os Pré-requisitos.
- Verifique se está usando o Suporte para a versão do SO Windows mais recente do pacote `AwsVssComponents` para o sistema operacional. O problema observado pode ter sido resolvido em versões mais recentes.

Tópicos

- Verificar arquivos de log
- Coletar logs de diagnóstico adicionais
- Usar o VSS em instâncias com proxy configurado
- Erro: A conexão do tubo de descongelamento expirou, erro no descongelamento, tempo limite aguardando o VSS Freeze, ou outros erros de tempo limite
- Erro: não é possível invocar o método. A invocação de métodos é compatível somente em tipos principais nesse modo de linguagem.

Verificar arquivos de log

Se tiver problemas ou receber mensagens de erro ao criar snapshots do EBS habilitados para o VSS, você poderá visualizar a saída do comando no console do Systems Manager.

Para documentos do Systems Manager que criam snapshots do VSS, você pode definir o parâmetro `CollectDiagnosticLogs` como "`True`" no runtime. Quando o parâmetro `CollectDiagnosticLogs` é definido como "`True`", o VSS coleta logs adicionais para ajudar na depuração. Para ter mais informações, consulte Coletar logs de diagnóstico adicionais.

Se você coletar logs de diagnóstico, o documento do Systems Manager os armazena em sua instância no seguinte local: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. O padrão do parâmetro `CollectDiagnosticLogs` é "`False`".

> **Note**
>
> Para obter ajuda adicional com a depuração, você pode enviar o arquivo `.zip` para o AWS Support.

Os seguintes logs adicionais estarão disponíveis, se você coletar ou não logs de diagnóstico:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Também é possível abrir a aplicação do Windows Event Viewer (Visualizador de Eventos) e escolher Windows Logs (Logs do Windows), Application (Aplicação) para visualizar registros adicionais. Para ver eventos especificamente do provedor VSS do EC2 do Windows e do Volume Shadow Copy Service (Serviço de Cópia de Sombra de Volume), filtre por Source (Origem) nos termos **`Ec2VssSoftwareProvider`** **`VSS`**e.

Se estiver usando o Systems Manager com endpoints da VPC e houver falha na ação da API SendCommand *do Systems Manager (**Run Command** no console), verifique se configurou corretamente o seguinte endpoint:* com.amazonaws.region.ec2.

Sem o endpoint do Amazon EC2 definido, ocorre falha na chamada para enumerar os volumes anexados do EBS, o que causa a falha do comando do Systems Manager. Para obter mais informações sobre como configurar endpoints da VPC com o Systems Manager, consulte Criar um endpoint da nuvem privada virtual no Manual do usuário do AWS Systems Manager.

Coletar logs de diagnóstico adicionais

Para coletar logs de diagnóstico adicionais ao usar o comando send do Systems Manager para executar o documento de snapshot do VSS, defina o parâmetro de entrada `CollectDiagnosticLogs` como "`True`" no runtime. Recomendamos que você defina esse parâmetro como "`True`" ao solucionar problemas.

Para ver um exemplo da linha de comando, selecione uma das guias a seguir.

AWS CLI

O exemplo a seguir executa o documento `AWSEC2-CreateVssSnapshot` do Systems Manager na AWS CLI:

```
aws ssm send-command \
--document-name "AWSEC2-CreateVssSnapshot" \
--instance-ids "i-1234567890abcdef0" \
--parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

O exemplo a seguir executa o documento `AWSEC2-CreateVssSnapshot` do Systems Manager no PowerShell:

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs
 at runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Usar o VSS em instâncias com proxy configurado

Se você tiver problemas ao criar snapshots do EBS habilitados para VSS em instâncias que usam um proxy para alcançar endpoints do EC2, certifique-se do seguinte:

- O proxy está configurado de modo que os endpoints de serviço do EC2 na região e no IMDS da instância possam ser alcançados pelo AWS Tools for Windows PowerShell sendo executado como SYSTEM.
- `AwsVssComponents` versão 2.0.1 ou posterior instalados. A partir dos `AwsVssComponents` versão 2.0.1, o provedor de VSS do EC2 é compatível com o uso do proxy WinHTTP configurado do sistema. Para obter mais informações sobre a configuração do proxy WinHTTP, consulte Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) no site da Microsoft.

Erro: A conexão do tubo de descongelamento expirou, erro no descongelamento, tempo limite aguardando o VSS Freeze, ou outros erros de tempo limite

O provedor de VSS do Windows EC2 pode acabar devido a atividades ou serviços na instância, impedindo que snapshots habilitados para VSS prossigam em tempo hábil. O Windows VSS

Framework fornece uma janela de 10 segundos não configurável durante a qual a comunicação com o sistema de arquivos é pausada. Durante esse tempo, o `AWSEC2-CreateVssSnapshot` captura seus volumes.

Os seguintes problemas podem fazer com que o provedor VSS do EC2 para Windows seja executado em limites de tempo durante um snapshot:

- E/S excessiva para um volume
- Capacidade de resposta lenta da API do EC2 na instância
- Volumes fragmentados
- Incompatibilidade com algum software antivírus
- Problemas com um gravador de aplicação de VSS
- Quando o Registro de Módulos estiver habilitado para um grande número de módulos do PowerShell, os scripts do PowerShell poderão ser executados com lentidão

A maioria dos problemas de tempo limite que ocorrem ao executar o documento de comando `AWSEC2-CreateVssSnapshot` está relacionada à workload na instância ser muito alta no momento do backup. As ações a seguir podem ajudá-lo a obter um snapshot bem-sucedido:

- Tente novamente o comando `AWSEC2-CreateVssSnapshot` para ver se a tentativa do snapshot é bem-sucedida. Se a nova tentativa for bem-sucedida em alguns casos, reduzir a carga da instância poderá tornar os snapshots mais bem-sucedidos.
- Aguarde um pouco até que a workload na instância diminua e tente novamente o comando `AWSEC2-CreateVssSnapshot`. Como alternativa, é possível tentar capturar snapshots quando a instância é conhecida por estar sob baixa tensão.
- Tente snapshots do VSS quando o software antivírus no sistema estiver desativado. Se isso resolver o problema, consulte as instruções do software antivírus e configure-o para permitir snapshots do VSS.
- Se houver um grande volume de chamadas de API do Amazon EC2 na sua conta na mesma região em que estiver executando um snapshot, o controle de utilização da API pode atrasar as operações de snapshot. Para reduzir o impacto do controle de utilização, use o pacote `AwsVssComponents` mais recente (versão 2.1.0 e superior, com as permissões de pré-requisito). Esse pacote utiliza a ação da API `CreateSnapshots` do EC2 para reduzir o número de ações mutantes, como a criação e a marcação de snapshots por volume.

- Se você tiver vários scripts de comando `AWSEC2-CreateVssSnapshot` em execução ao mesmo tempo, siga as etapas a seguir para reduzir os problemas de simultaneidade.
  - Considere agendar snapshots durante períodos de menor atividade da API.
  - Se você usar o Run Command no console do Systems Manager (ou o SendCommand na API) para executar o script de comando, poderá usar os controles de taxa do Systems Manager para reduzir a simultaneidade.

    Você também pode usar os controles de taxa do Systems Manager para reduzir a simultaneidade em serviços como o AWS Backup, que usam o Systems Manager para executar o script de comando.
- Execute o comando `vssadmin list writers` em um shell e veja se ele relata quaisquer erros no campo Last error (Último erro) para qualquer gravador no sistema. Se algum gravador relatar um erro de tempo esgotado, tente novamente capturar snapshots quando a instância estiver com menos carga.
- Ao usar tipos de instância menores, como *t2 | t3 | t3a*.nano ou *t2 | t3 | t3a*.micro, podem ocorrer tempos limite devido a restrições de memória e CPU. As ações a seguir podem ajudar a reduzir os problemas de tempo limite.
  - Tente fechar aplicações que consomem muita memória ou CPU antes de tirar snapshots.
  - Tente tirar snapshots durante períodos de menor atividade das instâncias.

Erro: não é possível invocar o método. A invocação de métodos é compatível somente em tipos principais nesse modo de linguagem.

Você receberá esse erro quando o modo de idioma da PowerShell não estiver definido como `FullLanguage`. Os documentos do SSM `AWSEC2-CreateVssSnapshot` e `AWSEC2-ManageVssIo` exigem que a PowerShell seja configurada no modo `FullLanguage`.

Para verificar o modo de idioma, execute o comando a seguir na instância em um console da PowerShell:

```
$ExecutionContext.SessionState.LanguageMode
```

Para obter mais informações sobre os modos de idioma, consulte about_Language_Modes na documentação da Microsoft.

Restaurar volumes do EBS por meio de snapshots do EBS habilitados para VSS

É possível usar o script `RestoreVssSnapshotSampleScript.ps1` para restaurar volumes em uma instância por meio de snapshots do EBS habilitados para VSS. Esse script executa as seguintes tarefas:

- Interrompe uma instância
- Remove todos os discos existentes da instância (exceto o volume de inicialização, se ele tiver sido excluído)
- Cria novos volumes por meio dos snapshots
- Anexa os volumes à instância usando a tag do ID do dispositivo no snapshot
- Reinicia a instância

> **Important**
>
> O script a seguir separa todos os volumes anexados a uma instância e, em seguida, cria novos volumes por meio de um snapshot. É essencial fazer um backup correto da instância. Os volumes antigos não são excluídos. Se desejar, é possível editar o script para excluir os volumes antigos.

Para restaurar volumes por meio de snapshots do EBS habilitados para VSS

1. Faça download do arquivo RestoreVssSnapshotSampleScript.zip e extraia o conteúdo dele.
2. Abra `RestoreVssSnapshotSampleScript.ps1` em um editor de texto e edite a chamada de amostra na parte inferior do script com um ID válido de instância do EC2 e o ID do snapshot do EBS. Depois, execute o script pelo PowerShell.

Histórico de versões da solução AWS VSS

Tópicos

- Versões do pacote AwsVssComponents
- Suporte para a versão do SO Windows

Versões do pacote AwsVssComponents

A tabela a seguir descreve as versões lançadas do pacote de componentes do AWS VSS.

Versão	Detalhes	Data de lançamento
2.3.3	O agente do VSS foi atualizado para garantir que o `Ec2VssProvider` seja usado durante a criação do snapshot.	25 de junho de 2024
2.3.2	Corrigido um caso em que o registro do provedor do VSS não era removido na desinstalação.	9 de maio de 2024
2.3.1	Adição de uma nova tag padrão `AwsVssConfig` para identificar snapshots e AMIs criados pelo AWS VSS.	7 de março de 2024
2.2.1	• Adição de compatibilidade com o uso da API `DescribeInstanceAttribute` . • Correções de bugs e aprimoramentos em confiabilidade. • Suporte obsoleto para Windows Server 2012 e 2012 R2. AWS A instalação dos componentes do VSS versão 2.2.1 no Windows Server 2012 e 2012 R2 falhará. AWS A versão 2.1.0 dos componentes do VSS é a última versão compatível com o Windows Server 2012 e 2012 R2.	18 de janeiro de 2024
2.1.0	Adição de compatibilidade com o uso da API `CreateSnapshots` .	6 de novembro de 2023
2.0.1	Adicionada compatibilidade com o uso das configurações do proxy WinHTTP.	26 de outubro de 2023

Versão	Detalhes	Data de lançamento
2.0.0	Capacidade adicionada ao componente AWS VSS para criar snapshots e AMIs, o que permite a compatibilidade com os recursos de registro em log do módulo PowerShell, registro em log de blocos de scripts e transcrição.	28 de abril de 2023
1.3.2.0	Corrigido um caso em que a falha de instalação não é relatada corretamente.	10 de maio de 2022
1.3.1.0	• Correção de snapshots com falha em controladores de domínio em relação a um erro de registro de gravador NTDS VSS. • Correção do erro do agente VSS ao desinstalar o provedor VSS versão 1.0.	6 de fevereiro de 2020
1.3.00	• Registro aprimorado reduzindo a verbosidade indesejada. • Correção de problemas de regionalização durante a instalaçã o. • Correção de códigos de retorno para algumas condições de erro de registro do provedor. • Correção de vários problemas de instalação.	19 de março de 2019
1.2.00	• Adição de parâmetros de linha de comando `-nw` (sem gravadores) e `-copy` (somente cópia) ao agente. • Correção de erros de log de eventos causados por chamadas inadequadas de alocação de memória.	15 de novembro de 2018

Versão	Detalhes	Data de lançamento
1.1	Correção de componentes do AWS VSS que estavam sendo usados incorretamente como o provedor padrão de Backup e Restauração do Windows.	12 de dezembro de 2017
1,0	Versão inicial.	20 de novembro de 2017

Suporte para a versão do SO Windows

A tabela a seguir mostra as versões da solução AWS VSS que devem ser executadas em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão do AwsVssComponents	Nome da versão do AWSEC2-VssInstallAndSnapshot	Nome da versão do AWSEC2-CreateVssSnapshot	Nome da versão do AWSEC2-ManageVssIO
Windows Server 2022	padrão	padrão	padrão	padrão
Windows Server 2019	padrão	padrão	padrão	padrão
Windows Server 2016	padrão	padrão	padrão	padrão

Versão Windows Server	Versão do AwsVssComponents	Nome da versão do AWSEC2-VssInstallAndSnapshot	Nome da versão do AWSEC2-CreateVssSnapshot	Nome da versão do AWSEC2-ManageVssIO
Windows Server 2012 R2	2.1.0	não compatível	2012R2	2012R2
Windows Server 2012	2.1.0	não compatível	2012R2	2012R2
Windows Server 2008 R2	1.3.1.0	não compatível	2008R2	2008R2

Prevenção de gravação interrompida para instâncias do Linux

> **Note**
>
> A prevenção de gravação interrompida é compatível somente com as instâncias do Linux.

A prevenção de gravação interrompida é um recurso de armazenamento em blocos desenvolvido pela AWS para melhorar a performance das workloads de banco de dados relacional com uso intenso de E/S e reduzir a latência sem afetar negativamente a resiliência dos dados. Bancos de dados relacionais que usam InnoDB ou XtraDB como mecanismo de banco de dados, como MySQL e MariaDB, se beneficiarão da prevenção de gravações interrompidas.

Normalmente, bancos de dados relacionais que usam páginas maiores do que a atomicidade de falha de energia do dispositivo de armazenamento usam mecanismos de log de dados para proteger contra gravações interrompidas. O MariaDB e o MySQL usam um arquivo buffer de gravação

dupla para registrar dados em log antes de gravá-los nas tabelas de dados. No caso de gravações incompletas ou interrompidas, como resultado de falhas no sistema operacional ou perda de energia durante transações de gravação, o banco de dados pode recuperar os dados do buffer de gravação dupla. A sobrecarga adicional de E/S associada à gravação no buffer de gravação dupla afeta a performance do banco de dados e a latência da aplicação, além de reduzir o número de transações que podem ser processadas por segundo. Para obter mais informações sobre o buffer de gravação dupla, consulte a documentação do MariaDB e do MySQL.

Com a prevenção de gravações interrompidas, os dados são gravados no armazenamento em transações de gravação do tipo tudo ou nada, o que elimina a necessidade de usar o buffer de gravação dupla. Isso evita que dados parciais ou interrompidos sejam gravados no armazenamento em caso de falhas no sistema operacional ou perda de energia durante transações de gravação. O número de transações processadas por segundo pode ser aumentado em até 30%, e a latência de gravação pode ser reduzida em até 50%, sem comprometer a resiliência das workloads.

Definição de preço

Não há custos adicionais para o uso da prevenção de gravação interrompida.

Tamanhos de blocos e alinhamentos de limites de blocos compatíveis

A prevenção de gravação interrompida é compatível com operações de gravação para blocos de dados de 4 KiB, 8 KiB e 16 KiB. O endereço do bloco lógico inicial (LBA) do bloco de dados deve estar alinhado ao respectivo tamanho do limite do bloco de 4 KiB, 8 KiB ou 16 KiB. Por exemplo, para operações de gravação de 16 KiB, o LBA inicial do bloco de dados deve estar alinhado a um tamanho limite de bloco de 16 KiB.

A tabela a seguir mostra a compatibilidade de tipos de armazenamento e instância.

	Blocos de 4 KiB	Blocos de 8 KiB	Blocos de 16 KiB
Volumes de armazenamento de instâncias	Todos os volumes de armazenamento de instância NVMe vinculados às instâncias da família I da geração atual.	Instâncias i4i, Im4Gn e IS4gen compatíveis com SSD AWS Nitro.	

	Blocos de 4 KiB	Blocos de 8 KiB	Blocos de 16 KiB
Volumes do Amazon EBS	Todos os volumes do Amazon EBS anexados a instâncias desenvolvidas no AWS Nitro System.		

Para confirmar se sua instância e seu volume são compatíveis com prevenção de gravação interrompida, consulte se a instância é compatível com prevenção de gravação interrompida e outros detalhes, como tamanhos de blocos e limites compatíveis. Para ter mais informações, consulte Verifique o suporte e a configuração de prevenção de gravação interrompida.

Requisitos

Para que a prevenção de gravação interrompida funcione adequadamente, uma operação de E/S deve atender aos requisitos de tamanho, alinhamento e limite, conforme especificado nos campos `NTWPU`, `NTWGU` e `NTWBU`. Você deve configurar seu sistema operacional para garantir que o subsistema de armazenamento específico (sistema de arquivos, LVM, RAID etc.) não modifique as propriedades de E/S na pilha de armazenamento, incluindo mesclagens de blocos, divisões ou realocação de endereços de blocos, antes de ser enviada ao dispositivo.

A prevenção de gravação interrompida foi testada com a seguinte configuração:

- Um tipo de instância e tipo de armazenamento que são compatíveis com o tamanho de bloco necessário.
- Amazon Linux 2 com a versão de kernel 5.10 ou posterior.
- ext4 com `bigalloc` habilitado e um tamanho de cluster de 16 KiB, e os utilitários ext4 mais recentes (e2fsprogs 1.46.5 ou posterior).
- Modo de acesso a arquivos `O_DIRECT` para ignorar o cache do buffer do kernel Linux.

> **Note**
>
> Você não precisa desativar a mesclagem de E/S para workloads do MySQL e do MariaDB.

Verifique o suporte e a configuração de prevenção de gravação interrompida

Para confirmar se sua instância e volume são compatíveis com prevenção de gravação interrompida e para visualizar os dados específicos do fornecedor do namespace NVMe que contém informações de prevenção de gravação interrompida, use o comando a seguir.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> O comando retorna as informações específicas do fornecedor em hexadecimal com interpretação ASCII. Talvez seja necessário criar uma ferramenta, semelhante à `ebsnvme-id`, nas aplicações, que possa ler e analisar a saída.

Por exemplo, o comando a seguir retorna os dados específicos do fornecedor do namespace NVMe que contêm informações de prevenção de gravação interrompida para `/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Se sua instância e seu volume oferecerem suporte à prevenção de gravação interrompida, eles retornarão as seguintes informações de prevenção de gravação interrompida da AWS nos dados específicos do fornecedor do namespace NVMe.

> **Note**
>
> Os bytes na tabela a seguir representam a diferença em bytes do início dos dados específicos do fornecedor do namespace NVMe.

Bytes	Descrição
`0:31`	O nome do ponto de montagem da conexão do dispositivo, por exemplo `/dev/xvda` . Você fornece isso durante a solicitação de anexo de volume e ele pode ser usado pela instância do Amazon EC2 para criar um link simbólico para o dispositivo de blocos NVMe (`nvmeXn1`).

Bytes	Descrição
32:63	O ID do volume. Por exemplo, vol01234567890abcdef . Esse campo pode ser usado para mapear o dispositivo NVMe para o volume anexado.
64:255	Reservado para uso futuro.
256:257	Tamanho da unidade de prevenção de gravação interrompida do namespace (NTWPU). Esse campo indica o tamanho específico do namespace da operação de gravação garantida para ser gravada atomicamente no NVM durante uma falha de energia ou condição de erro. Esse campo é especificado em blocos lógicos representados em valores baseados em zero.
258:259	Tamanho da granularidade de prevenção de gravação interrompida do namespace (NTWPG). Esse campo indica os incrementos de tamanho específico do namespace abaixo de NTWPU da operação de gravação garantida para ser gravada atomicamente no NVM durante uma falha de energia ou condição de erro. Ou seja, o tamanho deve ser NTWPG * n <= NTWPU onde n é um número inteiro positivo. O deslocamento do LBA da operação de gravação também deve estar alinhado com esse campo. Esse campo é especificado em blocos lógicos representados em valores baseados em zero.
260:263	Tamanho do limite de prevenção de gravação interrompida do namespace (NTWPU). Esse campo indica o tamanho do limite atômico desse namespace para o valor de NTWPU. Gravações nesse namespace que cruzam os limites atômicos não teê garantia de serem gravadas atomicamente no NVM durante uma falha de energia ou condição de erro. Um valor de 0h indica que não há limites atômicos para condições de falha ou erro de energia. Todos os outros valores especificam um tamanho em termos de blocos lógicos usando a mesma codificação do campo NTWPU.

Configure sua pilha de software para evitar gravações interrompidas

A prevenção de gravações interrompidas é habilitada por padrão em tipos de instância compatíveis com volumes compatíveis. Você não precisa habilitar nenhuma configuração adicional para habilitar seu volume ou instância para evitar gravações interrompidas.

> **Note**
>
> Não há impacto no performance em workloads que não são compatíveis com a prevenção de gravações interrompidas. Você não precisa fazer nenhuma alteração nessas workloads
> As workloads que são compatíveis com prevenção de gravação interrompida, mas não estão configuradas para usá-la, continuam usando o buffer de gravação dupla e não recebem nenhum benefício de performance.

Para configurar sua pilha de software MySQL ou MariaDB para desativar o buffer de gravação dupla e usar a prevenção de gravação interrompida, conclua as seguintes etapas:

1. Configure seu volume para usar o sistema de arquivos ext4 com a opção BigAlloc e defina o tamanho do cluster como 4 KiB, 8 KiB ou 16 KiB. O uso do BigAlloc com um tamanho de cluster de 4 KiB, 8 KiB ou 16 KiB garante que o sistema de arquivos aloque arquivos alinhados com o respectivo limite.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Para MySQL e MariaDB, você deve usar `-C 16384` para corresponder ao tamanho da página do banco de dados. Definir a granularidade da alocação para um valor diferente de um múltiplo do tamanho da página pode resultar em alocações que podem ser incompatíveis com os limites de prevenção de gravação interrompida do dispositivo de armazenamento.

   Por exemplo:

   ```
   $  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
   ```

2. Configure o InnoDB para usar o método `0_DIRECT` de descarga e desative a gravação dupla do InnoDB. Use seu editor de texto preferido para abrir `/etc/my.cnf` e atualize os parâmetros `innodb_flush_method` e `innodb_doublewrite` da seguinte forma:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

> **Important**
>
> Se você estiver usando o Logical Volume Manager (LVM) ou outra camada de virtualização de armazenamento, certifique-se de que os deslocamentos iniciais dos volumes estejam alinhados em múltiplos de 16 KiB. Isso é relativo ao armazenamento NVMe subjacente para contabilizar os cabeçalhos de metadados e superblocos usados pela camada de virtualização de armazenamento. Se você adicionar um deslocamento ao volume físico do LVM, isso poderá causar desalinhamento entre as alocações do sistema de arquivos e os deslocamentos do dispositivo NVMe, o que invalidaria a prevenção de gravação interrompida. Para obter mais informações, consulte `--dataalignmentoffset` na página do manual do Linux.

Recursos e tags

O Amazon EC2 fornece recursos diferentes que é possível criar e usar. Alguns desses recursos incluem imagens, instâncias, volumes e snapshots. Ao criar um recurso, atribuímos a ele um ID de recurso exclusivo.

Alguns recursos podem ser marcados com valores que você define, para ajudá-lo a organizá-los e identificá-los.

Os seguintes tópicos descrevem recursos e tags e como é possível trabalhar com eles.

Conteúdo

- Lixeira
- Localizações de recursos
- IDs de recursos
- Listar e filtrar seus recursos
- Amazon EC2 Global View
- Marcar com tag os recursos do Amazon EC2
- Service Quotas do Amazon EC2

Lixeira

A Recycle Bin (Lixeira) é um recurso de recuperação de dados que permite restaurar snapshots do Amazon EBS e AMIs apoiadas pelo EBS excluídos acidentalmente. Ao usar a Recycle Bin (Lixeira), se seus recursos forem excluídos, eles serão retidos na Recycle Bin (Lixeira) por um período de tempo que você especifica antes de serem excluídos permanentemente.

É possível restaurar um recurso da Recycle Bin (Lixeira) a qualquer momento antes que o período de retenção expire. Depois que um recurso é restaurado da Recycle Bin (Lixeira), ele é removido da Recycle Bin (Lixeira) e é possível usá-lo como usa qualquer outro recurso do mesmo tipo em sua conta. Se o período de retenção expirar e o recurso não for restaurado, ele será excluído permanentemente da Recycle Bin (Lixeira) e não estará mais disponível para recuperação.

O uso da Recycle Bin (Lixeira) garante a continuidade dos negócios, protegendo os backups de dados críticos de negócios contra exclusão acidental.

Tópicos

- Como funciona?
- Atributos suportados
- Considerações
- Cotas
- Serviços relacionados
- Definição de preço
- Permissões obrigatórias do IAM
- Trabalhar com regras de retenção
- Trabalhar com recursos na Lixeira
- Monitorar a Lixeira

Como funciona?

Para habilitar e usar a Recycle Bin (Lixeira), crie regras de retenção nas regiões da AWS nas quais deseja proteger recursos. As regras de retenção especificam o seguinte:

- Escolha o tipo de recurso que deseja proteger.
- Os recursos que você deseja reter na Recycle Bin (Lixeira) quando forem excluídos.
- O período de retenção para o qual os recursos serão retidos na Recycle Bin (Lixeira) antes de serem excluídos permanentemente.

Com a lixeira, é possível criar dois tipos de regras de retenção:

- Regras de retenção no nível de etiqueta: uma regra de retenção no nível de etiqueta usa etiquetas de recursos para identificar os recursos que devem ser retidos na Recycle Bin (Lixeira). Para cada regra de retenção, você especifica um ou mais pares de chave e valor de tag. Recursos do tipo especificado que são marcados com ao menos um dos pares de chave e valor de etiqueta especificados na regra de retenção são automaticamente retidos na Recycle Bin (Lixeira) após a exclusão. Use esse tipo de regra de retenção se desejar proteger recursos específicos em sua conta com base em suas etiquetas.
- Regras de retenção no nível da região: uma regra de retenção no nível da região não tem nenhuma etiqueta de recurso especificada. Ela se aplica a todos os recursos do tipo especificado na região em que a regra é criada, mesmo que os recursos não tenham sido etiquetados. Use

esse tipo de regra de retenção se desejar proteger todos os recursos de um tipo especifico em uma determinada região.

Enquanto um recurso está na Recycle Bin (Lixeira), é possível restaurá-lo para uso a qualquer momento.

O recurso permanece na Recycle Bin (Lixeira) até que um dos seguintes eventos ocorra:

- Você o restaura manualmente para uso. Quando você restaura um recurso da Recycle Bin (Lixeira), ele é removido da Recycle Bin (Lixeira) e fica imediatamente disponível para uso. É possível usar recursos restaurados da mesma forma que qualquer outro recurso desse tipo em sua conta.
- O período de retenção expira. Se o período de retenção expirar e o recurso não tiver sido restaurado da Recycle Bin (Lixeira), ele será excluído permanentemente e não poderá mais ser exibido nem restaurado.

Atributos suportados

A Recycle Bin (Lixeira) é compatível com os seguintes tipos de recurso:

- Snapshots do Amazon EBS

> **Important**
>
> As regras de retenção da Lixeira também se aplicam aos snapshots arquivados na camada de armazenamento de arquivamento. Se você excluir um snapshot arquivado que corresponda a uma regra de retenção, esse snapshot será retido na Lixeira pelo período de retenção definido na regra. Os snapshots arquivados são cobrados conforme a taxa para snapshots arquivados enquanto estão na lixeira.

- Imagens de máquina da Amazon (AMIs) apoiadas pelo Amazon EBS

> **Note**
>
> As regras de retenção também se aplicam às AMIs desabilitadas.

Considerações

As considerações a seguir se aplicam ao trabalhar com Recycle Bin (Lixeira) e regras de retenção.

Considerações gerais

- **Important**

  Quando você cria sua primeira regra de retenção, pode demorar até 30 minutos para que ela se torne ativa e comece a reter recursos. Depois de criar a primeira regra de retenção, as subsequentes se tornam ativas e começam a reter recursos quase que imediatamente.

- Se um snapshot corresponder a mais de uma regra de retenção no momento da exclusão, a regra de retenção com o período de retenção mais longo terá precedência.
- Não é possível excluir manualmente um recurso da Recycle Bin (Lixeira). O recurso será excluído automaticamente quando o período de retenção expirar.
- Enquanto um recurso está na Lixeira, só é possível exibi-lo, restaurá-lo ou modificar suas etiquetas. Para usar o recurso de qualquer outro modo, primeiro é necessário restaurá-lo.
- Se algum AWS service (Serviço da AWS), como o AWS Backup ou o Amazon Data Lifecycle Manager, excluir um recurso que corresponda a uma regra de retenção, esse recurso será automaticamente retido pela Lixeira.
- Quando um recurso é enviado para a Lixeira, a seguinte etiqueta gerada pelo sistema é atribuída a ele:
  - Chave de etiqueta: `aws:recycle-bin:resource-in-bin`
  - Valor da etiqueta: `true`

  Você não pode editar ou excluir essa etiqueta manualmente. Quando o recurso é restaurado da Lixeira, a etiqueta é removida automaticamente.

Considerações para snapshots

- **Important**

  Se você tiver regras de retenção para AMIs e para snapshots associados a elas, torne o período de retenção para os snapshots igual ou maior que o das AMIs. Isso garante que a

Lixeira não exclua os snapshots associados a uma AMI antes de excluir a AMI em si, pois isso tornaria a AMI irrecuperável.

- Se um snapshot estiver habilitado para restauração rápida de snapshots quando for excluído, a restauração rápida de snapshots será desabilitada automaticamente logo após o snapshot ser enviado para a lixeira.
  - Se você restaurar o snapshot antes que a restauração rápida de snapshots seja desabilitada para o snapshot, ela permanecerá habilitada.
  - Se você restaurar o snapshot após a restauração rápida de snapshots ser desabilitada, ela permanecerá desabilitada. Se necessário, é necessário reabilitar manualmente a restauração rápida de snapshot.
- Se um snapshot for compartilhado quando for excluído, o compartilhamento será automaticamente cancelado quando ele for enviado para a Lixeira. Se você restaurar o snapshot, todas as permissões de compartilhamento anteriores serão restauradas automaticamente.
- Se um snapshot criado por outro produto da AWS, como o AWS Backup, tiver sido enviado à lixeira e, posteriormente, restaurado da lixeira, ele não será mais gerenciado pelo produto da AWS que o criou. Exclua manualmente o snapshot caso ele não seja mais necessário.

Considerações para AMIs

- Somente AMIs apoiadas pelo Amazon EBS são compatíveis.
- **Important**

  Se você tiver regras de retenção para AMIs e para snapshots associados a elas, torne o período de retenção para os snapshots igual ou maior que o das AMIs. Isso garante que a Lixeira não exclua os snapshots associados a uma AMI antes de excluir a AMI em si, pois isso tornaria a AMI irrecuperável.
- Se uma AMI for compartilhada quando for excluída, o compartilhamento será automaticamente cancelado quando ela for enviada para a Lixeira. Se você restaurar a AMI, todas as permissões de compartilhamento anteriores serão restauradas automaticamente.
- Antes de restaurar uma AMI da Lixeira, é necessário primeiro restaurar todos os snapshots associados a ela da Lixeira e garantir que eles estejam no estado `available`.
- Se os snapshots associados à AMI forem excluídos da Lixeira, a AMI não será mais recuperável. A AMI será excluída quando o período de retenção expirar.

- Se uma AMI criada por outro serviço da AWS, como AWS Backup, for enviada para a Lixeira e, posteriormente, restaurada da Lixeira, ela não será mais gerenciada pelo serviço da AWS que a criou. Exclua manualmente a AMI caso ela não seja mais necessária.

Considerações sobre as políticas de snapshot do Amazon Data Lifecycle Manager

- Se o Amazon Data Lifecycle Manager excluir um snapshot que corresponda a uma regra de retenção, esse snapshot será automaticamente retido pela Lixeira.
- Se o Amazon Data Lifecycle Manager excluir um snapshot e enviá-lo para a lixeira quando o limite de retenção da política for atingido e você restaurar manualmente o snapshot da lixeira, você deverá excluir manualmente esse snapshot quando ele não for mais necessário. O Amazon Data Lifecycle Manager não poderá mais gerenciar o snapshot.
- Se você excluir manualmente um snapshot criado por uma política e esse snapshot estiver na lixeira quando o limite de retenção da política for atingido, o Amazon Data Lifecycle Manager não excluirá o snapshot. O Amazon Data Lifecycle Manager não gerencia snapshots enquanto eles estão armazenados no nível de arquivamento.

  Se o snapshot for restaurado da lixeira antes que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager excluirá o snapshot quando o limite de retenção da política for atingido.

  Se o snapshot for restaurado da lixeira depois que o limite de retenção da política seja atingido, o Amazon Data Lifecycle Manager não excluirá mais o snapshot. Exclua manualmente o snapshot quando ele não for mais necessário.

Considerações sobre o AWS Backup

- Se o AWS Backup excluir um snapshot que corresponda a uma regra de retenção, esse snapshot será automaticamente retido pela Lixeira.

Considerações sobre snapshots arquivados

- As regras de retenção da Lixeira também se aplicam aos snapshots arquivados na camada de armazenamento de arquivamento. Se você excluir um snapshot arquivado que corresponda a uma regra de retenção, esse snapshot será retido na Lixeira pelo período de retenção definido na regra.

Os snapshots arquivados são cobrados conforme a taxa para snapshots arquivados enquanto estão na lixeira.

Em outras palavras, se uma regra de retenção excluir um snapshot arquivado da Lixeira antes do período mínimo de 90 dias, os dias restantes serão cobrados. Para obter mais informações, consulte Preços e cobrança de snapshots arquivados no Guia do usuário do Amazon EBS.

Para usar um snapshot arquivado que esteja na Lixeira, primeiro é necessário recuperá-lo da Lixeira e depois restaurá-lo da camada de arquivamento para a camada padrão.

Cotas

As cotas a seguir se aplicam à lixeira.

Cota	Cota padrão			
Regras de retenção por região	250			
Aplicar tags em pares de chave e valor por regra de retenção	50			

Serviços relacionados

A lixeira funciona com os seguintes serviços:

- AWS CloudTrail: habilita o registro de eventos que ocorrem na lixeira. Para ter mais informações, consulte Monitorar a Lixeira usando o AWS CloudTrail.

Definição de preço

Os recursos na Lixeira são cobrados de acordo com as taxas padrão. Não há encargos adicionais pelo uso da lixeira e de regras de retenção. Para obter mais informações, consulte Definição de preço do Amazon EBS.

> **Note**
>
> Alguns recursos ainda podem aparecer no console da Lixeira ou na saída da AWS CLI e da API por um curto período após a expiração dos períodos de retenção e de sua exclusão permanente. Você não será cobrado por esses recursos. O faturamento é interrompido assim que o período de retenção expira.

É possível usar as tags de alocação de custos geradas pela AWS a seguir para rastreamento e alocação de custos ao usar o AWS Billing and Cost Management.

- Chave: `aws:recycle-bin:resource-in-bin`
- Valor: `true`

Para obter mais informações, consulte Tags de alocação de custos geradas pela AWS no Guia do usuário do AWS Billing and Cost Management.

Permissões obrigatórias do IAM

Por padrão, os usuários não têm permissão para trabalhar com a Lixeira, com as regras de retenção nem com os recursos que estão na Lixeira. Para permitir que os usuários trabalhem com esses recursos, você deve criar políticas do IAM que concedam permissão para o uso de recursos e ações de API específicos. Depois que as políticas forem criadas, você deverá adicionar permissões para os usuários, grupos ou perfis.

Tópicos

- Permissões para trabalhar com a Lixeira e com regras de retenção
- Permissões para trabalhar com recursos na Lixeira
- Chaves de condição para a Recycle Bin (Lixeira)

Permissões para trabalhar com a Lixeira e com regras de retenção

Para trabalhar com a Lixeira e com regras de retenção, os usuários precisam das permissões a seguir.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Para usar o console da Lixeira, os usuários precisam ter a permissão `tag:GetResources`.

A seguir está um exemplo de política do IAM que inclui a permissão `tag:GetResources` para usuários do console. Se algumas permissões não forem necessárias, você poderá removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
```

```
        ],
        "Resource": "*"
    }]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Permissões para trabalhar com recursos na Lixeira

Para obter mais informações sobre as permissões do IAM necessárias para trabalhar com recursos na Lixeira, veja as seguintes orientações:

- Permissões para trabalhar com snapshots na lixeira
- Permissões para trabalhar com AMIs na Lixeira

Chaves de condição para a Recycle Bin (Lixeira)

A Recycle Bin (Lixeira) define as seguintes chaves de condição que você pode usar no elemento `Condition` de uma política do IAM para controlar as condições segundo as quais a declaração de política se aplica. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.

Tópicos

- Chave da condição rbin:Request/ResourceType
- Chave da condição rbin:Attribute/ResourceType

Chave da condição **`rbin:Request/ResourceType`**

A chave de condição `rbin:Request/ResourceType` pode ser usada para filtrar o acesso das solicitações CreateRule e ListRules com base no valor especificado para o parâmetro de solicitação `ResourceType`.

Exemplo 1: CreateRule

O exemplo de política do IAM a seguir permite que as entidades principais do IAM façam solicitações CreateRule somente se o valor especificado para parâmetro de solicitação `ResourceType` for `EBS_SNAPSHOT` ou `EC2_IMAGE`. Isso permite que a entidade principal crie novas regras de retenção apenas para snapshots e AMIs.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Exemplo 2: ListRules

O exemplo de política do IAM a seguir permite que as entidades principais do IAM façam solicitações ListRules somente se o valor especificado para o parâmetro de solicitação `ResourceType` for `EBS_SNAPSHOT`. Isso permite que a entidade principal liste regras de retenção somente para snapshots e impede que listem regras de retenção para qualquer outro tipo de recurso.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Chave da condição **`rbin:Attribute/ResourceType`**

A chave de condição `rbin:Attribute/ResourceType` pode ser usada para filtrar o acesso de solicitações DeleteRule, GetRule, UpdateRule, LockRule, UnlockRule, TagResource, UntagResource e ListTagsForResource com base no valor do atributo `ResourceType` da regra de retenção.

Exemplo 1: UpdateRule

O exemplo de política do IAM a seguir permite que as entidades principais do IAM façam solicitações UpdateRule somente se o atributo `ResourceType` da regra de retenção solicitada for `EBS_SNAPSHOT` ou `EC2_IMAGE`. Isso permite que a entidade principal atualize regras de retenção apenas para snapshots e AMIs.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
```

```
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Exemplo 2: DeleteRule

O exemplo de política do IAM a seguir permite que as entidades principais do IAM façam solicitações DeleteRule somente se o atributo `ResourceType` da regra de retenção solicitada for `EBS_SNAPSHOT`. Isso permite que a entidade principal exclua regras de retenção apenas para snapshots.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Trabalhar com regras de retenção

Para habilitar e usar a Recycle Bin (Lixeira), crie regras de retenção nas regiões da AWS nas quais deseja proteger recursos. As regras de retenção especificam o seguinte:

- Escolha o tipo de recurso que deseja proteger.
- Os recursos que você deseja reter na Recycle Bin (Lixeira) quando forem excluídos.
- O período de retenção para o qual os recursos serão retidos na Recycle Bin (Lixeira) antes de serem excluídos permanentemente.

Com a lixeira, é possível criar dois tipos de regras de retenção:

- Regras de retenção no nível de etiqueta: uma regra de retenção no nível de etiqueta usa etiquetas de recursos para identificar os recursos que devem ser retidos na Recycle Bin (Lixeira). Para cada regra de retenção, você especifica um ou mais pares de chave e valor de tag. Recursos do tipo especificado que são marcados com ao menos um dos pares de chave e valor de etiqueta especificados na regra de retenção são automaticamente retidos na Recycle Bin (Lixeira) após a exclusão. Use esse tipo de regra de retenção se desejar proteger recursos específicos em sua conta com base em suas etiquetas.
- Regras de retenção no nível da região: uma regra de retenção no nível da região não tem nenhuma etiqueta de recurso especificada. Ela se aplica a todos os recursos do tipo especificado na região em que a regra é criada, mesmo que os recursos não tenham sido etiquetados. Use esse tipo de regra de retenção se desejar proteger todos os recursos de um tipo especifico em uma determinada região.

Depois de criar uma regra de retenção, os recursos que correspondam aos critérios serão automaticamente retidos na Lixeira pelo período especificado ao serem excluídos.

Tópicos

- Criar uma regra de retenção
- Exibir as regras de retenção da lixeira
- Atualizar regras de retenção
- Regras de retenção de bloqueio
- Desbloquear regras de retenção
- Regras de retenção de tags
- Exibir etiquetas de regras de retenção
- Remover etiquetas de uma regra de retenção
- Excluir regras de retenção da lixeira

Criar uma regra de retenção

Ao criar uma regra de retenção, você deve especificar os seguintes parâmetros obrigatórios:

- O tipo de recurso que deve ser protegido pela regra de retenção.

- Os recursos que devem ser protegidos pela regra de retenção. Você pode criar regras de retenção no nível da tag e no nível da região.
  - Para criar uma regra de retenção no nível da tag, especifique as tags de recurso que identificam os recursos a serem protegidos. Você pode especificar até 50 tags para cada regra e adicionar o mesmo par de chave e valor de tag a até 5 regras de retenção.
  - Para criar uma regra de retenção no nível da região, não especifique nenhum par de chave e valor de tag. Nesse caso, todos os recursos do tipo especificado são protegidos.
- O período durante o qual os recursos devem ser retidos na Lixeira após serem excluídos. O período pode ser de até 1 ano (365 dias).

Você também pode, opcionalmente, especificar os seguintes parâmetros:

- Um nome opcional para a regra de retenção. O nome pode ter até 255 caracteres.
- Uma descrição opcional para a regra de retenção. A descrição pode ter até 255 caracteres.

> **Note**
>
> Recomendamos não incluir informações pessoais, confidenciais ou sigilosas na descrição da regra de retenção.

- Tags de regra de retenção opcionais para ajudar a identificar e organizar as regras de retenção. É possível atribuir até 50 tags a cada regra.

Você também pode, opcionalmente, bloquear as regras de retenção ao criá-las. Se você bloquear uma regra de retenção ao criá-la, também deverá especificar o período de espera para o desbloqueio, que pode ser de 7 a 30 dias. As regras de retenção permanecem desbloqueadas, por padrão, a menos que você as bloqueie explicitamente.

As regras de retenção só funcionam nas regiões em que são criadas. Se você pretender usar a lixeira em outras regiões, deverá criar regras de retenção adicionais nessas regiões.

É possível criar uma regra de retenção da lixeira usando um dos métodos a seguir.

Recycle Bin console

Para criar uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/

2. No painel de navegação, escolha Retention rules (Regras de retenção) e depois escolha Create retention rule (Criar regra de retenção).
3. Na seção Basic details (Detalhes básicos), faça o seguinte:
   a. (Opcional) Em Retention rule name (Nome da regra de retenção), insira um nome descritivo para a regra de retenção.
   b. (Opcional) Em Retention rule description (Descrição da regra de retenção), insira uma breve descrição para a regra de retenção.
4. Na seção Rule settings (Configurações da regra), faça o seguinte:
   a. Para oResource type (Tipo de recurso), selecione o tipo de recurso para a regra de retenção a ser protegida. A regra de retenção reterá somente recursos desse tipo na Lixeira.
   b. Execute um destes procedimentos:
      - Para criar uma regra de retenção no nível da região que corresponda a todos os recursos do tipo especificado excluídos na região, selecione Apply to all resources (Aplicar a todos os recursos). A regra de retenção reterá todos os recursos do tipo especificado excluídos na Lixeira durante a exclusão, mesmo que os recursos não tenham nenhuma etiqueta.
      - Para criar uma regra de retenção no nível da etiqueta, para Resource tags to match (Etiquetas de recurso a corresponder), insira os pares de valor e chave de etiqueta a serem usados para identificar os recursos do tipo especificado que devem ser retidos na Lixeira. Somente recursos do tipo especificado com, pelo menos, um dos pares de valor e chave de etiqueta especificados serão retidos pela regra de retenção.
   c. Em Retention period (Período de retenção), insira o número de dias pelos quais a regra de retenção deve reter recursos na Lixeira.
5. (Opcional) Para bloquear a regra de retenção, em Rule lock settings (Configurações de bloqueio da regra), selecione Lock (Bloquear) e, em seguida, para Unlock delay period (Período de espera para desbloqueio), especifique o período de espera para o desbloqueio em dias. Uma regra de retenção bloqueada não pode ser modificada nem excluída. Para modificar ou excluir a regra, você deve primeiro desbloqueá-la e depois aguardar que o período de espera para o desbloqueio expire. Para ter mais informações, consulte Regras de retenção de bloqueio.

Para deixar a regra de retenção desbloqueada, em Rule lock settings (Configurações de bloqueio da regra), mantenha a opção Unlock (Desbloquear) selecionada. Uma regra de retenção desbloqueada pode ser modificada ou excluída a qualquer momento. Para ter mais informações, consulte Desbloquear regras de retenção.

6. (Opcional) Na seção Tags faça o seguinte:

   - Para marcar a regra com tags personalizadas, escolha Add Tag (Adicionar tag) e insira o par de chave e valor de tag.

7. Selecione Create retention rule (Criar regra de retenção).

AWS CLI

Para criar uma regra de retenção

Use o comando create-rule da AWS CLI. Em `--retention-period`, especifique o número de dias de retenção dos snapshots excluídos na lixeira. Para o `--resource-type`, especifique `EBS_SNAPSHOT` para snapshots ou `EC2_IMAGE` para AMIs. Para criar uma regra de retenção no nível da tag, para `--resource-tags`, especifique as tags a serem usadas para identificar os snapshots que devem ser retidos. Para criar uma regra de retenção no nível da região, omita `--resource-tags`.. Para bloquear uma regra de retenção`--lock-configuration`, inclua e especifique o período de espera para o desbloqueio em dias.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Exemplo 1

O exemplo de comando a seguir cria uma regra de retenção desbloqueada no nível da região que retém todos os snapshots excluídos por um período de 7 dias.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
```

```
--description "Match all snapshots"
```

Exemplo 2

O exemplo de comando a seguir cria uma regra de retenção, no nível da tag, que retém todos os snapshots com tag de `purpose=production` aplicada por um período de 7 dias.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Exemplo 3

O exemplo de comando a seguir cria uma regra de retenção bloqueada no nível da região que retém todos os snapshots excluídos por um período de 7 dias. A regra de retenção é bloqueada com um período de espera para o desbloqueio de 7 dias.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Exibir as regras de retenção da lixeira

É possível visualizar uma regra de retenção da lixeira usando um dos métodos a seguir.

Recycle Bin console

Para visualizar as regras de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. A grade lista todas as regras de retenção para a região selecionada. Para visualizar mais informações sobre uma regra de retenção específica, selecione-a na grade.

AWS CLI

Para visualizar todas as regras de retenção

Use o comando da AWS CLI list-rules e, para `--resource-type`, especifique `EBS_SNAPSHOT`para snapshots ou `EC2_IMAGE` para AMIs.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

Exemplo

O comando de exemplo a seguir fornece a lista todas as regras de retenção que retêm snapshots.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT
```

Para visualizar informações de uma regra de retenção específica

Use o comando get-rule da AWS CLI.

```
aws rbin get-rule --identifier rule_ID
```

Exemplo

O exemplo de comando a seguir fornece informações sobre a regra de retenção `pwxIkFcvge4`.

```
aws rbin get-rule --identifier pwxIkFcvge4
```

Atualizar regras de retenção

Você pode atualizar a descrição, as etiquetas de recursos e o período de retenção de uma regra de retenção desbloqueada a qualquer momento após a criação. Você não pode atualizar o tipo de recurso nem o período de espera para o desbloqueio de uma regra de retenção, mesmo que a regra de retenção esteja desbloqueada.

Você não pode atualizar uma regra de retenção bloqueada de nenhuma maneira. Se precisar modificar uma regra de retenção bloqueada, deverá primeiro desbloqueá-la e aguardar até que o período de espera para o desbloqueio expire.

Se você precisar modificar o período espera para o desbloqueio de uma regra de retenção bloqueada, desbloqueie a regra de retenção e aguarde até que o período atual de espera para o desbloqueio expire. Quando o período de espera para o desbloqueio expirar, você deve bloquear a regra de retenção novamente e especificar o novo período de espera para o desbloqueio.

> **Note**
>
> Recomendamos não incluir informações pessoais, confidenciais ou sigilosas na descrição da regra de retenção.

Depois que você atualiza uma regra de retenção, as alterações só se aplicam aos novos recursos que ela retém. As alterações não afetam os recursos enviados anteriormente para a Lixeira. Por exemplo, se você atualizar o período de retenção de uma regra de retenção, apenas os snapshots excluídos após a atualização serão retidos pelo novo período de retenção. Os snapshots enviados para a lixeira antes da atualização ainda serão retidos pelo período de retenção anterior (antigo).

É possível atualizar uma regra de retenção usando um dos seguintes métodos.

Recycle Bin console

Para atualizar uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Na grade, selecione a regra de retenção a ser atualizada e escolha Actions (Ações), Edit retention rule (Editar regra de retenção).
4. Na seção Rule details (Detalhes da regra), atualize Retention rule name (Nome da regra de retenção) e Retention rule description (Descrição da regra de retenção) conforme necessário.
5. Na seção Rule settings (Configurações de regra), atualize Resource type (Tipo de recurso) Resource tags to match (Etiquetas de recurso a corresponder) e Retention period (Período de retenção) conforme necessário.
6. Na seção Tags, adicione ou remova tags da regra de retenção conforme necessário.
7. Selecione Save retention rule (Salvar regra de retenção).

AWS CLI

Para atualizar uma regra de retenção

Use o comando update-rule da AWS CLI. Para `--identifier`, especifique o ID da regra de retenção a ser atualizada. Para `--resource-types`, especifique `EBS_SNAPSHOT` para snapshots ou `EC2_IMAGE` para AMIs.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Exemplo

O exemplo a seguir atualiza a regra de retenção `6lsJ2Fa9nh9` para reter todos os snapshots por 7 dias e atualiza sua descrição.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Regras de retenção de bloqueio

A Lixeira permite que você bloqueie as regras de retenção no nível regional a qualquer momento.

> **Note**
>
> Você não pode bloquear as regras de retenção no nível da tag.

Uma regra de retenção bloqueada não pode ser modificada nem excluída, mesmo por usuários que tenham as permissões necessárias do IAM. Bloqueie as regras de retenção para ajudar a protegê-las contra modificações e exclusões acidentais ou maliciosas.

Quando você bloqueia uma regra de retenção, deve especificar um período de espera para o desbloqueio. Esse é o período de tempo que você deve esperar após desbloquear a regra de

retenção para poder modificá-la ou excluí-la. Você não pode modificar nem excluir a regra de retenção durante o período de espera para o desbloqueio. Você só pode modificar ou excluir a regra de retenção após o período de espera para o desbloqueio.

Você não pode alterar o período de espera após o bloqueio da regra de retenção. Se as permissões da sua conta tiverem sido comprometidas, o período de espera para o desbloqueio dará a você mais tempo para detectar e responder às ameaças à segurança. A duração desse período deve ser maior do que o tempo necessário para identificar e responder às violações de segurança. Para definir a duração certa, você pode revisar os incidentes de segurança anteriores e o tempo necessário para identificar e solucionar uma violação de conta.

Recomendamos o uso das regras do Amazon EventBridge para notificar você sobre mudanças no estado de bloqueio da regra de retenção. Para ter mais informações, consulte Monitorar a Lixeira usando o Amazon EventBridge.

Considerações

- Você só pode bloquear as regras de retenção no nível regional.
- Você pode bloquear uma regra de retenção desbloqueada a qualquer momento.
- O período de espera para o desbloqueio deve ser de 7 a 30 dias.
- Você pode bloquear novamente uma regra de retenção durante o período de espera para o desbloqueio. Bloquear a regra de retenção novamente redefine o período de espera para o desbloqueio.

Você pode bloquear uma regra de retenção no nível regional usando um dos métodos a seguir.

Recycle Bin console

Para bloquear uma regra de retenção

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Na grade, selecione a regra de retenção desbloqueada a ser bloqueada e escolha Actions (Ações), Edit retention rule (Editar regra de retenção).
4. Na tela Edit retention rule lock (Editar bloqueio da regra de retenção), escolha Lock (Bloquear) e, em Unlock delay period (Período de espera para o desbloqueio), especifique o período de espera para o desbloqueio em dias.

5. Marque a caixa de seleção I acknowledge that locking the retention rule will prevent it from being modified or deleted (Eu reconheço que bloquear a regra de retenção impedirá que ela seja modificada ou excluída) e escolha Save (Salvar).

AWS CLI

Para bloquear uma regra de retenção desbloqueada

Use o comando da AWS CLI lock-rule. Em `--identifier`, especifique o ID da regra de retenção a ser bloqueada. Em `--lock-configuration`, especifique o período de espera para o desbloqueio em dias.

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Exemplo

O exemplo de comando a seguir bloqueia a regra de retenção `6lsJ2Fa9nh9` e define o período de espera para o desbloqueio como 15 dias.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Desbloquear regras de retenção

Você não pode modificar nem excluir uma regra de retenção bloqueada. Se você precisar modificar uma regra de retenção bloqueada, deverá primeiro desbloqueá-la. Depois de desbloquear a regra de retenção, aguarde até que o período de espera para o desbloqueio expire antes de modificá-la ou excluí-la. Você não pode modificar nem excluir uma regra de retenção durante o período de espera para o desbloqueio.

Uma regra de retenção desbloqueada pode ser modificada e excluída a qualquer momento por um usuário que tenha as permissões necessárias do IAM. Deixar as regras de retenção desbloqueadas poderia expô-las a modificações e exclusões acidentais ou maliciosas.

Considerações

- Você pode bloquear novamente uma regra de retenção durante o período de espera para o desbloqueio.
- Você pode bloquear novamente uma regra de retenção após o período de espera para o desbloqueio expirar.
- Você não pode ignorar o período de espera para o desbloqueio.
- Você não pode alterar o período de espera para o desbloqueio após o bloqueio inicial.

Recomendamos o uso das regras do Amazon EventBridge para notificar você sobre mudanças no estado de bloqueio da regra de retenção. Para ter mais informações, consulte Monitorar a Lixeira usando o Amazon EventBridge.

Você pode desbloquear uma regra de retenção bloqueada no nível regional usando um dos métodos a seguir.

Recycle Bin console

Para desbloquear uma regra de retenção

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Na grade, selecione a regra de retenção bloqueada a ser desbloqueada e escolha Actions (Ações), Edit retention rule (Editar regra de retenção).
4. Na tela Edit retention rule lock (Editar bloqueio da regra de retenção), escolha Unlock (Desbloquear) e depois escolha Save (Salvar).

AWS CLI

Para desbloquear uma regra de retenção bloqueada

Use o comando unock-rule da AWS CLI. Em `--identifier`, especifique o ID da regra de retenção a ser desbloqueada.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Exemplo

O exemplo de comando a seguir desbloqueia a regra de retenção `6lsJ2Fa9nh9`

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Regras de retenção de tags

É possível atribuir tags personalizadas às regras de retenção para categorizá-las de diferentes maneiras, por exemplo, por objetivo, proprietário ou ambiente. Isso ajuda a localizar de forma eficiente uma regra de retenção específica com base nas etiquetas personalizadas que foram atribuídas.

É possível atribuir uma tag a uma regra de retenção usando um dos métodos a seguir.

Recycle Bin console

Para aplicar tag em uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Selecione a regra de retenção para aplicar tag, escolha a guia Tags, e depois, escolha Manage tags (Gerenciar tags).
4. Escolha Adicionar Tag. Em Key (Chave), insira o nome da chave. Em Value (Valor), insira o valor da tag.
5. Escolha Save (Salvar).

AWS CLI

Para aplicar tag em uma regra de retenção

Use o comando tag-resource da AWS CLI Em `--resource-arn`, especifique o nome do recurso da Amazon (ARN) da regra de retenção a aplicar tag e, para `--tags`, especifique o par de chave e valor da tag.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Exemplo

O exemplo de comando a seguir narca a regra de retenção `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` com a tag `purpose=production`.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tags key=purpose,value=production
```

Exibir etiquetas de regras de retenção

É possível visualizar as tags atribuídas a uma regra de retenção usando um dos métodos a seguir.

Recycle Bin console

Para visualizar as tags para uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Selecione a regra de retenção para a qual deseja visualizar as etiquetas e escolha a guia Tags (Etiquetas).

AWS CLI

Para visualizar as tags atribuídas a uma regra de retenção

Use o comando list-tags-for-resource AWS CLI. Em `--resource-arn`, especifique o ARN da regra de retenção.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Exemplo

O exemplo de comando a seguir lista as tags da regra de retenção `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

Remover etiquetas de uma regra de retenção

É possível remover tags de uma regra de retenção usando um dos métodos a seguir.

Recycle Bin console

Para remover uma tag de uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Selecione a regra de retenção da qual deseja remover a tag , escolha a guia Tags e, em seguida, escolha Manage tags (Gerenciar tags).
4. Escolha Remove (Remover) ao lado da tag a ser removida.
5. Escolha Save (Salvar).

AWS CLI

Para remover uma tag de uma regra de retenção

Use o comando untag-resource da AWS CLI. Em `--resource-arn`, especifique o ARN da regra de retenção. Em `--tagkeys`, especifique as chaves de tag das tags a serem removidas.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Exemplo

O exemplo de comando a seguir remove as tags que têm uma chave de tag de `purpose` da regra de retenção `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Excluir regras de retenção da lixeira

É possível excluir uma regra de retenção a qualquer momento. Quando você exclui uma regra de retenção, ela não retém mais os novos recursos na Recycle Bin (Lixeira) após serem excluídos. Os

recursos enviados para a Lixeira antes da regra de retenção ser excluída continuam a ser retidos na Lixeira de acordo com o período de retenção definido na regra. Quando o período expira, o recurso é excluído permanentemente da Lixeira.

É possível excluir uma regra de retenção usando um dos seguintes métodos.

Recycle Bin console

Para excluir uma regra de retenção

1. Abra o console da lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Retention rules (Regras de retenção).
3. Na grade, selecione a regra de retenção a ser excluída e escolha Actions (Ações), Delete retention rule (Excluir regra de retenção).
4. Quando solicitado, insira a mensagem de confirmação e escolha Delete retention rule (Excluir regra de retenção).

AWS CLI

Para excluir uma regra de retenção

Use o comando delete-rule da AWS CLI. Em `--identifier`, especifique o ID da regra de retenção a ser excluída.

```
aws rbin delete-rule --identifier rule_ID
```

Exemplo

O exemplo de comando a seguir exclui a regra de retenção `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Trabalhar com recursos na Lixeira

A Recycle Bin (Lixeira) é compatível com os seguintes tipos de recurso:

- Snapshots do Amazon EBS
- Imagens de máquina da Amazon (AMIs) apoiadas pelo Amazon EBS

Tarefas

- Recuperar snapshots da lixeira
- Recuperar AMIs da Lixeira

Recuperar snapshots da lixeira

A Recycle Bin (Lixeira) é um recurso de recuperação de dados que permite restaurar snapshots do Amazon EBS e AMIs apoiadas pelo EBS excluídos acidentalmente. Ao usar a Recycle Bin (Lixeira), se seus recursos forem excluídos, eles serão retidos na Recycle Bin (Lixeira) por um período de tempo que você especifica antes de serem excluídos permanentemente.

É possível restaurar um recurso da Recycle Bin (Lixeira) a qualquer momento antes que o período de retenção expire. Depois que um recurso é restaurado da Recycle Bin (Lixeira), ele é removido da Recycle Bin (Lixeira) e é possível usá-lo como usa qualquer outro recurso do mesmo tipo em sua conta. Se o período de retenção expirar e o recurso não for restaurado, ele será excluído permanentemente da Recycle Bin (Lixeira) e não estará mais disponível para recuperação.

Os snapshots na lixeira são cobrados à mesma taxa que os snapshots comuns em sua conta. Não há encargos adicionais pelo uso da lixeira e de regras de retenção. Para obter mais informações, consulte Definição de preço do Amazon EBS.

Para ter mais informações, consulte Lixeira.

Tópicos

- Permissões para trabalhar com snapshots na lixeira
- Exibir snapshots na lixeira
- Restaurar os snapshots da lixeira

Permissões para trabalhar com snapshots na lixeira

Por padrão, os usuários do IAM não têm permissão para trabalhar com os snapshots que estão na Lixeira. Para permitir que os usuários trabalhem com esses recursos, você deve criar políticas do IAM que concedam permissão para o uso de recursos e ações de API específicos. Depois que as políticas forem criadas, você deverá adicionar permissões para os usuários, grupos ou perfis.

Para visualizar e recuperar snapshots que estão na Lixeira, os usuários precisam ter as seguintes permissões:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Para gerenciar etiquetas para snapshots na Lixeira, os usuários precisam das permissões adicionais a seguir.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para usar o console da Lixeira, os usuários precisam ter a permissão `ec2:DescribeTags`.

A seguir está um exemplo de política do IAM. Ela inclui a permissão `ec2:DescribeTags` para usuários do console e inclui as permissões `ec2:CreateTags` e `ec2:DeleteTags` para gerenciar etiquetas. Se não forem necessárias permissões, será possível removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para obter mais informações sobre permissões necessárias para usar a Lixeira, consulte Permissões para trabalhar com a Lixeira e com regras de retenção.

Exibir snapshots na lixeira

Enquanto um snapshot estiver na lixeira, é possível visualizar informações limitadas sobre ele, incluindo:

- O ID do snapshot.
- A descrição do snapshot.
- O ID do volume do qual o snapshot foi criado.
- A data e a hora em que o snapshot foi excluído e entrou na lixeira.
- A data e a hora em que o período de retenção expira. O snapshot será excluído permanentemente da lixeira nessa hora.

É possível visualizar os snapshots na lixeira usando um dos métodos a seguir.

Recycle Bin console

Para visualizar os snapshots na lixeira usando o console

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/

2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade lista todos os snapshots que estão atualmente na lixeira. Para visualizar os detalhes de um snapshot específico, selecione-o na grade e escolha Actions (Ações), View details (Exibir detalhes).

AWS CLI

Para visualizar snapshots na lixeira usando a AWS CLI

Use o comando list-snapshots-in-recicle-bin da AWS CLI. Inclua a opção `--snapshot-id` para visualizar um snapshot específico. Ou omita a opção `--snapshot-id` para visualizar todos os snapshots na lixeira.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Por exemplo, o comando a seguir retorna informações sobre o snapshot `snap-01234567890abcdef` na lixeira.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Resultado do exemplo:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Restaurar os snapshots da lixeira

Você não pode usar um snapshot de nenhum modo enquanto ele está na lixeira. Para usar o snapshot, é necessário primeiro restaurá-lo. Quando você restaura um snapshot da lixeira, ele fica

imediatamente disponível para uso e é removido da lixeira. É possível usar um snapshot restaurado como usa qualquer outro snapshot em sua conta.

É possível restaurar um snapshot da lixeira usando um dos métodos a seguir.

Recycle Bin console

Para restaurar um snapshot da lixeira usando o console

1. Abra o console da Lixeira em https://console.aws.amazon.com/rbin/home/
2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade lista todos os snapshots que estão atualmente na lixeira. Selecione o snapshot a ser restaurado e escolha Recover (Recuperar).
4. Quando solicitado, escolha Recover (Recuperar).

AWS CLI

Para restaurar um snapshot excluído da lixeira usando o AWS CLI

Use o comando restore-snapshot-from-recycle-bin da AWS CLI. Em `--snapshot-id`, especifique o ID do snapshot a ser restaurado.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Por exemplo, o comando a seguir restaura o snapshot `snap-01234567890abcdef` da lixeira.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Resultado do exemplo:

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
```

```
    "VolumeSize": 30
}
```

Recuperar AMIs da Lixeira

A Recycle Bin (Lixeira) é um recurso de recuperação de dados que permite restaurar snapshots do Amazon EBS e AMIs apoiadas pelo EBS excluídos acidentalmente. Ao usar a Recycle Bin (Lixeira), se seus recursos forem excluídos, eles serão retidos na Recycle Bin (Lixeira) por um período de tempo que você especifica antes de serem excluídos permanentemente.

É possível restaurar um recurso da Recycle Bin (Lixeira) a qualquer momento antes que o período de retenção expire. Depois que um recurso é restaurado da Recycle Bin (Lixeira), ele é removido da Recycle Bin (Lixeira) e é possível usá-lo como usa qualquer outro recurso do mesmo tipo em sua conta. Se o período de retenção expirar e o recurso não for restaurado, ele será excluído permanentemente da Recycle Bin (Lixeira) e não estará mais disponível para recuperação.

As AMIs na Lixeira não têm nenhuma cobrança adicional.

Para ter mais informações, consulte Lixeira.

Tópicos

- Permissões para trabalhar com AMIs na Lixeira
- Visualizar AMIs na Lixeira
- Restaurar as AMIs da Lixeira

Permissões para trabalhar com AMIs na Lixeira

Por padrão, os usuário não têm permissão para trabalhar com as AMIs que estão na Lixeira. Para permitir que os usuários trabalhem com esses recursos, você deve criar políticas do IAM que concedam permissão para o uso de recursos e ações de API específicos. Depois que as políticas forem criadas, você deverá adicionar permissões para os usuários, grupos ou perfis.

Para visualizar e recuperar as AMIs que estão na Lixeira, os usuários precisam ter as seguintes permissões:

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Para gerenciar tags para AMIs que estão na Lixeira, os usuários precisam ter as permissões adicionais a seguir.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para usar o console da Lixeira, os usuários precisam ter a permissão `ec2:DescribeTags`.

A seguir está um exemplo de política do IAM. Ela inclui a permissão `ec2:DescribeTags` para usuários do console e inclui as permissões `ec2:CreateTags` e `ec2:DeleteTags` para gerenciar etiquetas. Se não forem necessárias permissões, será possível removê-las da política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para obter mais informações sobre permissões necessárias para usar a Lixeira, consulte Permissões para trabalhar com a Lixeira e com regras de retenção.

Visualizar AMIs na Lixeira

Enquanto uma AMI está na Lixeira, é possível visualizar informações limitadas sobre ela, incluindo:

- O nome, a descrição e o ID exclusivo da AMI.
- A data e a hora em que a AMI foi excluída e entrou na Lixeira.
- A data e a hora em que o período de retenção expira. A AMI será excluída permanentemente nesse momento.

É possível visualizar as AMIs na Lixeira usando um dos métodos a seguir.

Recycle Bin console

Para visualizar as AMIs excluídas na Lixeira usando o console

1. Abra o console da Lixeira em console.aws.amazon.com/rbin/home/.
2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade relaciona todos os recursos que estão atualmente na Lixeira. Para visualizar os detalhes de uma AMI específica, selecione-a na grade e escolha Actions (Ações), View details (Exibir detalhes).

AWS CLI

Para visualizar AMIs excluídas na Lixeira usando a AWS CLI

Use o comando list-snapshots-in-recicle-bin da AWS CLI. Para visualizar AMIs específicas, inclua a opção `--image-id` e especifique os IDs das AMIs a serem exibidas. É possível especificar até 20 IDs em uma única solicitação.

Para visualizar todas as AMIs na Lixeira, omita a opção `--image-id`. Se você não especificar um valor para `--max-items`, o comando retornará mil itens por página, por padrão. Para obter mais informações, consulte Pagination (Paginação) em Amazon EC2 API Reference (Referência de API do Amazon EC2).

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Por exemplo, o comando a seguir retorna informações sobre a AMI `ami-01234567890abcdef` na Lixeira.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Resultado do exemplo:

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

Important

Se receber o erro a seguir, talvez você precise atualizar sua versão do AWS CLI. Para obter mais informações, consulte Erros de comando não encontrados.

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Restaurar as AMIs da Lixeira

Você não pode usar uma AMI de nenhum modo enquanto ela está na Lixeira. Para usar a AMI, é necessário primeiro restaurá-la. Quando você restaura uma AMI da Lixeira, ela fica imediatamente disponível para uso e é removida da Lixeira. É possível usar uma AMI restaurada como usa qualquer outra AMI em sua conta.

É possível restaurar uma AMI da Lixeira usando um dos métodos a seguir.

Recycle Bin console

Para restaurar uma AMI da Lixeira usando o console

1. Abra o console da Lixeira em console.aws.amazon.com/rbin/home/.
2. No painel de navegação, selecione Recycle Bin (Lixeira).
3. A grade relaciona todos os recursos que estão atualmente na Lixeira. Selecione a AMI a ser restaurada e escolha Recover (Recuperar).
4. Quando solicitado, escolha Recover (Recuperar).

AWS CLI

Para restaurar uma AMI excluída da Lixeira usando o AWS CLI

Use o comando restore-snapshot-from-recycle-bin da AWS CLI. Em `--image-id`, especifique o ID da AMI a ser restaurada.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Por exemplo, o comando a seguir restaura a AMI `ami-01234567890abcdef` da Lixeira.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

Quando o comando tem êxito, não retorna nenhuma saída.

> **Important**
>
> Se receber o erro a seguir, talvez você precise atualizar sua versão do AWS CLI. Para obter mais informações, consulte Erros de comando não encontrados.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Monitorar a Lixeira

Você pode usar os seguintes recursos para monitorar a Lixeira.

Tópicos

- Monitorar a Lixeira usando o Amazon EventBridge
- Monitorar a Lixeira usando o AWS CloudTrail

Monitorar a Lixeira usando o Amazon EventBridge

A Lixeira envia eventos para o Amazon EventBridge para ações realizadas nas regras de retenção. Com o EventBridge, você pode estabelecer regras que iniciam ações programáticas em resposta a esses eventos. Por exemplo, você pode criar uma regra do EventBridge que envia uma notificação para seu e-mail quando uma regra de retenção é desbloqueada e entra no período de espera para o desbloqueio. Para obter mais informações, consulte Creating Amazon EventBridge rules that react to events (Criar regras do Amazon EventBridge que reagem a eventos).

Os eventos no EventBridge são representados como objetos JSON. Os campos que são exclusivos do evento estão contidos na seção `detail` do objeto JSON. O campo `event` contém o nome do evento. O campo `result` contém o status de concluído da ação que iniciou o evento. Para obter mais informações, consulte Padrões de eventos do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Para obter mais informações sobre o EventBridge, consulte What Is Amazon EventBridge? (O que é o Amazon EventBridge) no Amazon EventBridge User Guide (Guia do usuário do Amazon EventBridge).

Eventos

- RuleLocked

- RuleChangeAttempted
- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

Veja a seguir um exemplo de um evento que a Lixeira gera quando uma regra de retenção é bloqueada com êxito. Esse evento pode ser gerado pelas solicitações createRule e LockRule. A API que gerou o evento é anotada no campo `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
}
```

RuleChangeAttempted

Veja a seguir um exemplo de um evento que a Lixeira gera para tentativas de modificar ou excluir uma regra bloqueada sem êxito. Esse evento pode ser gerado pelas solicitações DeleteRule e UpdateRule. A API que gerou o evento é anotada no campo `api-name`.

```
{
  "version": "0",
```

```
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "DeleteRule"
  }
}
```

RuleUnlockScheduled

Veja a seguir um exemplo de um evento que a Lixeira gera quando uma regra de retenção é desbloqueada com êxito.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
```

```
}
```

RuleUnlockingNotice

Veja a seguir um exemplo de um evento que a Lixeira gera diariamente enquanto uma regra de retenção está em seu período de espera para o desbloqueio, até o dia anterior à expiração do período de espera para o desbloqueio.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

Veja a seguir um exemplo de um evento que a Lixeira gera quando o período de espera para o desbloqueio de uma regra de retenção expira e a regra de retenção pode ser modificada ou excluída.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
```

```
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

Monitorar a Lixeira usando o AWS CloudTrail

O serviço de lixeira é integrado ao AWS CloudTrail. O CloudTrail é um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS. O CloudTrail captura todas as chamadas de API realizadas na lixeira como eventos. Ao criar uma trilha, será possível habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3). Se você não configurar uma trilha, ainda poderá visualizar os eventos de gerenciamento mais recentes no console do CloudTrail em Event history (Histórico de eventos). É possível usar as informações coletadas pelo CloudTrail para determinar qual foi a solicitação feita à lixeira, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações da lixeira no CloudTrail

O CloudTrail é habilitado em sua AWS conta ao criá-la. Quando uma atividade de evento com suporte ocorre na lixeira, ela é registrada em um evento do CloudTrail juntamente com outros eventos de serviços da AWS no Histórico de eventos. É possível visualizar, pesquisar e baixar os eventos recentes em sua conta da AWS. Para obter mais informações, consulte Visualização de eventos com o histórico de eventos do CloudTrail.

Para ter um registro de eventos contínuo em sua conta da AWS, incluindo eventos da lixeira, crie uma trilha. Uma trilha permite que o CloudTrail forneça arquivos de log para um bucket do S3. Por padrão, ao criar uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log ao bucket do S3 que você especificar. Além disso, é possível configurar outros serviços da AWS para analisar mais

ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte Visão geral da criação de uma trilha no Guia do usuário do AWS CloudTrail.

Ações da API com suporte

Para a lixeira, é possível usar o CloudTrail para registrar em log as seguintes ações de API como eventos de gerenciamento.

- CreateRule
- UpdateRule
- GetRules
- ListRules
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Para obter mais informações sobre como registrar eventos de gerenciamento, consulte Registrar eventos de gerenciamento para trilhas no Manual do usuário do CloudTrail.

Informações de identidade

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte userIdentityElement do CloudTrail.

Compreender as entradas de arquivo de log da lixeira

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. Os arquivos de log CloudTrail não são um rastreamento de pilha ordenada de chamadas API públicas, portanto não são exibidos em qualquer ordem específica.

A seguir, estão exemplos de entradas de log do CloudTrail.

CreateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "CreateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
```

```
  "requestParameters": {
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": {
    "identifier": "jkrnexample"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


GetRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
```

```
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListRules

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
```

```
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "resourceTags": [
      {
        "resourceTagKey": "test",
        "resourceTagValue": "test"
      }
    ]
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UpdateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
```

```
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

DeleteRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:25Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "DeleteRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
```

```
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


TagResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
```

```
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


UntagResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tagKeys": [
      "purpose"
    ]
  },
  "responseElements": null,
  "requestID": "example7-6c1e-4f09-9e46-bb957example",
  "eventID": "example6-75ff-4c94-a1cd-4d5f5example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListTagsForResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
```

```
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

LockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:45:19Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "LockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
```

```
      }
    }
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EBS_SNAPSHOT",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "locked"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


UnlockRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
```

```
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UnlockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EC2_IMAGE",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "pending_unlock",
    "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
```

```
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

Localizações de recursos

Os recursos do Amazon EC2 são específicos para a região da AWS ou zona de disponibilidade de residência.

Recurso	Tipo	Descrição
Identificadores de recursos do Amazon EC2	Regional	Cada identificador de recursos, como um ID de AMI, ID de instância, ID de volume do EBS ou ID de snapshot do EBS, é vinculado à sua região e só pode ser usado na região em que você criou o recurso.
Nomes de recursos fornecidos pelo usuário	Regional	Cada nome de recurso, como um nome de grupo de segurança ou de par de chaves, é vinculado à sua região e só pode ser usado na região em que você criou o recurso. Embora você possa criar recursos com o mesmo nome em várias regiões, eles não são relacionados uns aos outros.
AMIs	Regional	A AMI é vinculada à região onde seus arquivos estão localizados no Amazon S3. É possível copiar

Recurso	Tipo	Descrição
		uma AMI de uma região para outra. Para ter mais informações, consulte Copiar um AMI.
Snapshots do EBS	Regional	Um snapshot EBS é vinculado à sua região e só pode ser usado para criar volumes na mesma região. É possível copiar um snapshot de uma região em outra.
Volumes do EBS	Zona de disponibilidade	Um volume do Amazon EBS é vinculado à sua zona de disponibilidade e só pode ser anexado a instâncias na mesma zona de disponibilidade.
Endereços IP elásticos	Regional	Um endereço IP elástico está vinculado a uma região e pode ser associado apenas a uma instância na mesma região.
Instâncias	Availability Zone	Uma instância é vinculada às zonas de disponibi lidade na qual você a executou. Contudo, observe que o ID da instância está vinculado à região.
Pares de chaves	Global ou regional	Os pares de chaves criados com o Amazon EC2 são vinculados à região onde você os criou. É possível criar seu próprio par de chaves de RSA e fazer upload dele na região em que deseja usá-lo; portanto, é possível tornar seu par de chaves globalmente disponível fazendo upload dele em cada região. Para ter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

Recurso	Tipo	Descrição
Grupos de segurança	Regional	Um grupo de segurança é vinculado a uma região e pode ser atribuído somente a instâncias na mesma região. Você não pode permitir que uma instância se comunique com uma instância fora de sua região usando regras de grupo de segurança. O tráfego de uma instância em outra região é considerado como a largura de banda de WAN.

IDs de recursos

Ao criarmos recursos, atribuímos a cada um deles um ID de recurso exclusivo. Um ID de recurso assume a forma de um identificador de recurso (como `snap` para um snapshot), seguido de um hífen e uma combinação única de oito letras e números.

Cada identificador de recursos, como um ID de AMI, ID de instância, ID de volume do EBS ou ID de snapshot do EBS, é vinculado à sua região e só pode ser usado na região em que você criou o recurso.

É possível usar IDs de recursos para localizar seus recursos no console do Amazon EC2. Se você estiver usando uma ferramenta da linha de comando ou a API do Amazon EC2 para trabalhar com o Amazon EC2, os IDs dos recursos serão necessários para determinados comandos. Por exemplo, se você estiver usando o comando stop-instances da AWS CLI para interromper uma instância, deverá especificar o ID da instância no comando.

Tamanho do ID do recurso

Antes de janeiro de 2016, os IDs atribuídos a recursos recém-criados de determinados tipos usavam 8 caracteres após o hífen (por exemplo, i-1a2b3c4d). De janeiro de 2016 a junho de 2018, alteramos os IDs desses tipos de recursos para 17 caracteres após o hífen (por exemplo, `i-1234567890abcdef0`). Dependendo de quando sua conta foi criada, é possível haver alguns recursos existentes com IDs curtos; no entanto, quaisquer novos recursos receberão os IDs mais longos.

Listar e filtrar seus recursos

É possível obter uma lista de alguns tipos de recursos usando o console do Amazon EC2. É possível obter uma lista de cada tipo de recurso usando seu comando ou ação de API correspondente. Se você tiver muitos recursos, é possível filtrar os resultados para incluir ou excluir somente aqueles que correspondem a determinados critérios.

Tópicos

- Listar e filtrar recursos usando o console
- Listar e filtrar usando a CLI e a API
- Visualizar recursos entre regiões usando a Visualização Global do Amazon EC2

Listar e filtrar recursos usando o console

Sumário

- Listar recursos usando o console
- Filtrar recursos usando o console
  - Filtros compatíveis

Listar recursos usando o console

É possível visualizar os tipos de recurso do Amazon EC2 mais comuns usando o console. Para ver os recursos adicionais, use a interface de linha de comando ou as ações de API.

Para listar os recursos do EC2 usando o console

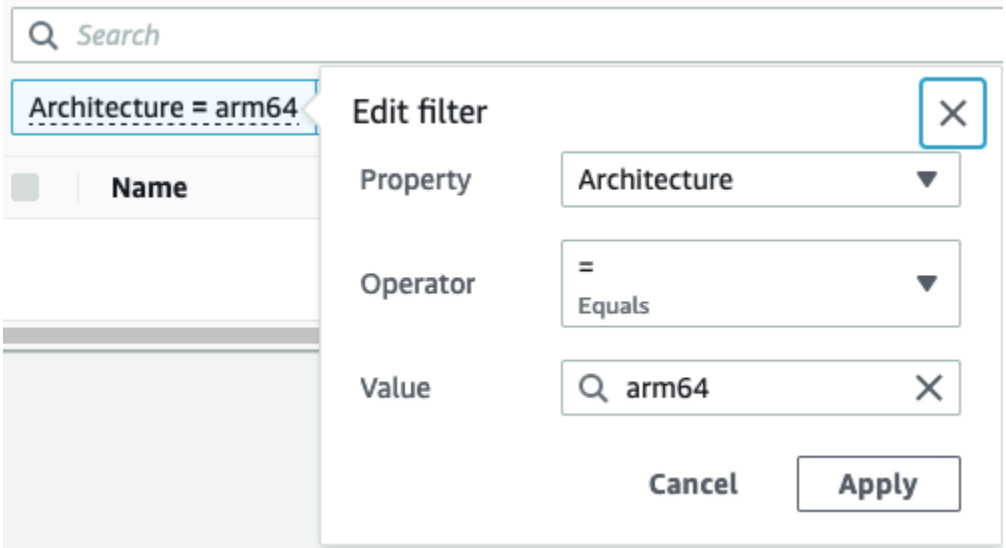
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha a opção que corresponde ao tipo de recurso. Por exemplo, para listar suas instâncias, escolha Instances (Instâncias).

   A página exibe todos os recursos do tipo de recurso selecionado.

Filtrar recursos usando o console

Para filtrar uma lista de recursos

1. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
2. Escolha o campo de pesquisa.
3. Escolha o filtro na lista.
4. Selecione um operador, por exemplo,= (Igual a). Alguns atributos têm mais operadores disponíveis para selecionar. Observe que nem todas as telas suportam a seleção de um operador.
5. Selecione um valor de filtro.
6. Para editar um filtro selecionado, escolha o token de filtro (caixa azul), faça as edições necessárias e escolha Apply (Aplicar). Observe que nem todas as telas suportam a edição do filtro selecionado.



7. Quando terminar, remova o filtro.

Filtros compatíveis

O console do Amazon EC2 é compatível com dois tipos de filtragem.

- A filtragem de API acontece no lado do servidor. A filtragem é aplicada na chamada de API, o que reduz o número de recursos retornados pelo servidor. Isso permite a filtragem rápida em grandes conjuntos de recursos e pode reduzir o tempo e o custo de transferência de dados entre o servidor

e o navegador. A filtragem de API oferece suporte a operadores = (igual a) e : (contém), e sempre diferencia maiúsculas de minúsculas.

- A filtragem do cliente acontece no lado do cliente. Isso permite filtrar dados que já estão disponíveis no navegador (em outras palavras, dados que já foram retornados pela API). A filtragem do cliente funciona bem em conjunto com um filtro de API para filtrar para conjuntos de dados menores no navegador. Além dos operadores = (igual a) e : (contém), a filtragem de clientes também pode oferecer suporte a operadores de intervalo, como >= (maior que ou igual a) e operadores de negação (inversa), como ! = (não igual a).

O console do Amazon EC2 é compatível com os seguintes tipos de pesquisa:

Pesquisa por palavra-chave

A pesquisa por palavra-chave é uma pesquisa de texto livre que permite pesquisar um valor em todos os atributos ou tags de seus recursos, sem especificar um atributo a ser pesquisado.

> **Note**
>
> Todas as pesquisas por palavras-chave usam filtragem do cliente.

Para pesquisar por palavra-chave, insira ou cole o que você procura na caixa de pesquisa e selecione Enter. Por exemplo, procurar por 123 corresponde a todas as instâncias que tenham 123 em qualquer um de seus atributos, como um endereço IP, ID de instância, ID de VPC ou ID de AMI, ou em qualquer uma de suas tags, como em Name (Nome). Se sua pesquisa de texto livre retornar correspondências inesperadas, aplique filtros adicionais.

Pesquisar por atributo

A pesquisa por um atributo permite que você pesquise um atributo específico em todos os recursos.

> **Note**
>
> As pesquisas de atributos usam filtragem de API ou filtragem de cliente, dependendo do atributo selecionado. Ao realizar uma pesquisa de atributo, os atributos são agrupados conforme necessário.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias para retornar apenas instâncias que estão no estado `stopped`. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Para pesquisar no lado do servidor, escolha Instance state (Estado da instância) em API filters (Filtros de API). Para pesquisar no lado do cliente, escolha Instance state (client) (Estado da instância (cliente)) em Client filters (Filtros de cliente).

   Uma lista de operadores possíveis para o atributo selecionado é exibida.
3. Selecione o operador = (igual a).

   Uma lista de valores possíveis para o atributo e operador selecionado é exibida.
4. Selecione stopped (interrompido) na lista.

Pesquisar por etiqueta

A pesquisa por uma tag permite filtrar os recursos na tabela exibida atualmente por uma chave de tag ou um valor de tag.

Pesquisas de tags usam filtragem de APIs ou filtragem de clientes, dependendo das configurações na janela Preferences (Preferências).

Para garantir a filtragem de APIs para tags

1. Abra a janela Preferences (Preferências).
2. Limpe a caixa de seleção Use regular expression matching (Usar correspondência de expressões regulares). Se essa caixa de seleção estiver marcada, a filtragem do cliente será executada.
3. Marque a caixa de seleção Use case sensitive matching (Usar correspondência com distinção de maiúsculas e minúsculas). Se essa caixa de seleção estiver desmarcada, a filtragem do cliente será executada.
4. Selecione a opção Confirmar.

Ao pesquisar por tag, é possível usar os seguintes valores:

- (empty) (vazio): encontra todos os recursos com a chave de tag especificada, mas não deve haver valor de tag.

- All values (Todos os valores): encontra todos os recursos com a chave de tag especificada e qualquer valor de tag.
- Not tagged (Sem tag aplicada): pesquisa por todos os recursos que não tenham uma determinada chave de tag.
- O valor exibido: encontra todos os recursos com a chave de tag especificada e o valor da tag especificado.

É possível usar as seguintes técnicas para aprimorar ou refinar suas pesquisas:

Pesquisa inversa

Pesquisas inversas permitem pesquisar recursos que não correspondem a um valor especificado. Nas telas Instances (Instâncias) e AMIs, as pesquisas inversas são realizadas selecionando o operador != (Não igual a) ou !: (Não contém) e, em seguida, selecionando um valor. Nas outras telas, as pesquisas inversas são realizadas colocando o caractere de ponto de exclamação (!) como prefixo da palavra-chave de pesquisa.

> **Note**
>
> A pesquisa inversa é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias a fim de excluir todas as instâncias que estão no estado `terminated`. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Em Client filters (Filtros de cliente), escolha Instance state (client) (Estado da instância, cliente). A pesquisa inversa é aceita somente em filtros de cliente.

   Uma lista de operadores possíveis para o atributo selecionado é exibida.
3. Selecione != (Não igual a) e, em seguida, escolha terminated (terminado).

Para filtrar instâncias com base em um atributo de estado de instância, também é possível usar os ícones de pesquisa

( )

na coluna Instance state (Estado da instância). O ícone de pesquisa com um sinal de mais (+) exibe todas as instâncias que correspondem a esse atributo. O ícone de pesquisa com um sinal de menos (-) exclui todas as instâncias que correspondem a esse atributo.

Aqui está outro exemplo de uso da pesquisa inversa: listar todas as instâncias que não são atribuídas ao grupo de segurança chamado `launch-wizard-1`. Em Client filters (Filtros do cliente), pesquise pelo atributo Security group name (Nome do grupo de segurança), escolha != e, na barra de pesquisa, insira `launch-wizard-1`.

Pesquisa parcial

Com pesquisas parciais, é possível procurar valores de string parciais. Para realizar uma pesquisa parcial, insira apenas uma parte da palavra-chave que você deseja pesquisar. Nas telas Instances (Instâncias) e AMIs, as pesquisas parciais só podem ser realizadas com o operador : (Contém). Em outras telas, é possível selecionar o atributo de filtro do cliente e inserir imediatamente apenas uma parte da palavra-chave que deseja pesquisar. Por exemplo, na tela Instance type (Tipo de instância), para pesquisar todas as instâncias `t2.micro`, `t2.small` e `t2.medium`, pesquise pelo atributo Instance Type (Tipo de instância) e, para a palavra-chave, insira `t2`.

Pesquisa de expressão regular

Para usar pesquisas de expressão regular, é necessário marcar a caixa de seleção Use regular expression matching (Usar correspondência de expressão regular) na janela Preferences (Preferências).

As expressões regulares são úteis quando você precisa corresponder os valores de um campo com um padrão específico. Por exemplo, para procurar um valor que comece com `s`, procure `^s`. Para procurar um valor que termine com `xyz`, procure `xyz$`. Ou para procurar um valor que começa com um número seguido por um ou mais caracteres, procure `[0-9]+.*`.

> **Note**
>
> A pesquisa de expressão regular é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Pesquisa com diferenciação de maiúsculas e minúsculas

Para fazer pesquisas que diferenciem maiúsculas de minúsculas, é necessário marcar a caixa de seleção Use case sensitive matching (Usar correspondência com distinção de maiúsculas e minúsculas) na janela Preferences (Preferências). A preferência com diferenciação de maiúsculas e minúsculas se aplica somente aos filtros de cliente e tag.

> **Note**
>
> Os filtros de API sempre diferenciam maiúsculas de minúsculas.

Pesquisa por curinga

Use o curinga `*` para corresponder a zero ou mais caracteres. Use o curinga `?` para corresponder a zero ou um caractere. Por exemplo, se você tiver um conjunto de dados com os valores `prod`, `prods`, e `production`, uma pesquisa por `prod*` corresponde a todos os valores, enquanto `prod?` corresponde somente a `prod` e `prods`. Para usar os valores literais, coloque uma barra invertida (\) antes. Por exemplo, "`prod\*`" corresponderia a `prod*`.

> **Note**
>
> A pesquisa por curingas é compatível apenas com pesquisas de atributos e tags em filtros de API. Não é compatível com pesquisas de palavras-chave e pesquisas de atributos e tags em filtros de cliente.

Combinar pesquisas

Em geral, vários filtros com o mesmo atributo são unidos automaticamente com `OR`. Por exemplo, pesquisar `Instance State : Running` e `Instance State : Stopped` retorna todas as instâncias que estão em execução OU interrompidas. Para unir a pesquisa com `AND`, pesquise em diferentes atributos. Por exemplo, pesquisar `Instance State : Running` e `Instance Type : c4.large` retorna apenas instâncias que são do tipo `c4.large` E que estão no estado de execução.

Listar e filtrar usando a CLI e a API

Cada tipo de recurso tem um comando da CLI correspondente e ação de API que você usa para listar os recursos desse tipo. As listas de recursos resultantes podem ser longas, portanto, pode ser mais rápido e mais útil filtrar os resultados para incluir apenas os recursos que correspondem a critérios específicos.

Considerações sobre filtragem

- É possível especificar até 50 filtros e até 200 valores por filtro em uma única solicitação.
- As strings do filtro podem ter até 255 caracteres.
- Também é possível usar caracteres curinga com os valores de filtro. Um asterisco (*) corresponde a zero ou mais caracteres, e um ponto de interrogação (?) corresponde a zero ou um caractere.
- Os valores do filtro diferenciam maiúsculas de minúsculas.
- Sua pesquisa pode incluir os valores literais dos caracteres curinga; apenas só precisa recuá-los uma barra invertida antes do caractere. Por exemplo, um valor `\*amazon\?\\` pesquisa pela string literal, `*amazon?\`.

Filtros compatíveis

Para ver os filtros compatíveis com cada recurso do Amazon EC2, consulte a documentação a seguir:

- AWS CLI: os comandos `describe` na Referência de comandos da AWS CLI - Amazon EC2.
- Tools for Windows PowerShell: os comandos `Get` na Referência de Cmdlet do AWS Tools for PowerShell - Amazon EC2.
- API de consulta: as ações `Describe` da API na Amazon EC2 API Reference (Referência da API do Amazon EC2).

Example Exemplo: Especificar um único filtro

Você pode listar suas instâncias do Amazon EC2 usando describe-instances. Sem filtros, a resposta contém informações de todos os recursos. É possível usar o seguinte comando para incluir apenas as instâncias em execução em sua saída.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Para listar apenas os IDs de suas instâncias em execução, adicione o parâmetro `--query` da seguinte maneira.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

A seguir está um exemplo de saída.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Exemplo: Especificar vários filtros ou valores de filtro

Se você especificar vários filtros ou vários valores de filtro, o recurso deverá corresponder a todos os filtros a serem incluídos nos resultados.

É possível usar o seguinte comando para listar todas as instâncias cujo tipo é `m5.large` ou `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

É possível usar o seguinte comando para listar todas as instâncias paradas cujo tipo é `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
 Name=instance-type,Values=t2.micro
```

Example Exemplo: Usar curingas em um valor de filtro

Se você especificar `database` como o valor do filtro `description` ao descrever snapshots do EBS usando describe-snapshots, o comando retornará somente os snapshots cuja descrição é “banco de dados”.

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

O curinga * corresponde a zero ou mais caracteres. Se você especificar `*database*` como o valor do filtro, o comando retornará apenas snapshots cuja descrição inclui a palavra banco de dados.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

O curinga ? corresponde exatamente a 1 caractere. Se você especificar `database?` como o valor do filtro, o comando retornará apenas snapshots cuja descrição é “banco de dados” ou “banco de dados” seguido por um caractere.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Se você especificar `database????`, o comando retornará apenas snapshots cuja descrição é “banco de dados” seguida de até quatro caracteres. Ele exclui descrições com “banco de dados” seguido por cinco ou mais caracteres.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Exemplo: filtro baseado em data

Com a AWS CLI, é possível usar JMESPath para filtrar resultados usando expressões. Por exemplo, o comando describe-snapshots a seguir exibe os IDs de todos os snapshots criados pela sua Conta da AWS (representada por *123456789012*) antes da data especificada (representada por *2020-03-31*). Se você não especificar o proprietário, os resultados incluirão todos os snapshots públicos.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

O comando a seguir exibe os IDs de todos os snapshots criados no intervalo de datas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --
output text
```

Filtrar com base em tags

Para obter exemplos de como filtrar uma lista de recursos de acordo com suas tags, consulte Trabalhar com tags usando a linha de comando.

Visualizar recursos entre regiões usando a Visualização Global do Amazon EC2

A Visualização Global do Amazon EC2 permite que você veja e pesquise recursos do Amazon EC2 e da Amazon VPC em uma única região da AWS ou em várias regiões simultaneamente em um único console. Para ter mais informações, consulte Amazon EC2 Global View.

Amazon EC2 Global View

O Amazon EC2 Global View permite que você visualize alguns de seus recursos do Amazon EC2 e do Amazon VPC em uma única região da AWS ou em várias regiões em um único console. O Amazon EC2 Global View também fornece a funcionalidade pesquisa global, que permite pesquisar recursos específicos ou tipos de recursos específicos em várias regiões simultaneamente.

O Amazon EC2 Global View não permite que você modifique recursos de forma alguma.

Atributos suportados

Usando o Amazon EC2 Global View, é possível visualizar um resumo global dos recursos a seguir em todas as regiões nas quais a sua Conta da AWS está habilitada.

- Grupos do Auto Scaling
- Conjunto de opção de DHCP
- Gateways da Internet apenas de saída
- IPs elásticos
- Serviços de endpoint
- Instâncias
- Gateways da Internet
- Listas de prefixos gerenciados
- Gateways NAT
- Network ACLs
- Interfaces de rede
- Tabelas de rotas
- Grupos de segurança
- Subredes

- Volumes
- VPCs
- Endpoints da VPC
- Conexões de emparelhamento da VPC

Permissões obrigatórias

Um usuário deve ter as seguintes permissões para usar a Visualização Global do Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Para usar o Amazon EC2 Global View

Abra o console do Amazon EC2 Global View em https://console.aws.amazon.com/ec2globalview/home.

> **Important**
>
> Não é possível usar uma janela privada no Firefox para acessar o Amazon EC2 Global View.

O console consiste no seguinte:

- Explorador de região: essa aba inclui as seções a seguir:
  - Resumo: fornece uma visão geral de alto nível dos recursos em todas as regiões.

    Regiões habilitadas indica o número de regiões para as quais a Conta da AWS está habilitada. Os campos restantes indicam o número de recursos que você tem atualmente nessas regiões. Escolha qualquer um dos links para visualizar os recursos desse tipo em todas as regiões. Por exemplo, se o link abaixo do rótulo Instâncias for 29 em 10 regiões, ele indica que você tem 29 instâncias em 10 regiões. Escolha o link para visualizar uma lista de todas as 29 instâncias.
  - Contagens de recursos por região: lista todas as Regiões da AWS (incluindo aquelas em que a conta não está habilitada) e fornece o número total de cada tipo de recurso em cada região.

    Escolha um nome de região para visualizar todos os recursos de todos os tipos para essa região específica. Por exemplo, escolha Africa (Cape Town) af-south-1 (África [Cidade do Cabo] af-south-1) para visualizar todas as VPCs, sub-redes, instâncias, grupos de segurança, volumes e grupos do Auto Scaling nessa região. Como alternativa, selecione uma região e escolha Exibir recursos para a região selecionada.

    Escolha o valor para um tipo de recurso específico em uma região específica para visualizar somente os recursos desse tipo nessa região. Por exemplo, escolha o valor para Instâncias para África (Cidade do Cabo) af-south-1 para visualizar somente as instâncias nessa região.
- Pesquisa global: essa guia permite que você pesquise recursos específicos ou tipos de recursos específicos em uma única região ou em várias regiões. Ela também permite que você veja detalhes de um recurso específico.

  Para pesquisar recursos, insira os critérios de pesquisa no campo anterior à grade. É possível pesquisar por região, por tipo de recurso e pelas etiquetas atribuídas aos recursos.

Para visualizar os detalhes de um recurso específico, selecione-o na grade. Também é possível escolher o ID de recurso para abrir o recurso no respectivo console. Por exemplo, escolha um ID de instância para abrir a instância no console do Amazon EC2 ou escolha um ID de sub-rede para abrir a sub-rede no console da Amazon VPC.

> **Tip**
>
> Se você usa apenas regiões ou tipos de recursos específicos, é possível personalizar a Visualização Global do Amazon EC2 para exibir somente essas regiões e tipos de recursos. Para personalizar as regiões e os tipos de recursos exibidos, no painel de navegação, escolha Configurações e, em seguida, nas guias Recursos e Regiões, selecione as regiões e os tipos de recursos que você não deseja que sejam exibidos na Visualização Global do Amazon EC2.

Marcar com tag os recursos do Amazon EC2

Para ajudá-lo a gerenciar instâncias, imagens e outros recursos do Amazon EC2, é possível atribuir seus próprios metadados a cada recurso na forma de tags. As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele. Este tópico descreve tags e mostra a você como criá-los.

> **Warning**
>
> As chaves de tag e seus valores são apresentados por várias chamadas de API diferentes. Negar acesso ao `DescribeTags` não nega automaticamente acesso às tags apresentadas por outras APIs. Como uma prática recomendada, sugerimos que você não inclua dados confidenciais nas suas tags.

Tópicos

- Conceitos Básicos de Tags
- Marcar com tag os recursos do
- Restrições de tags

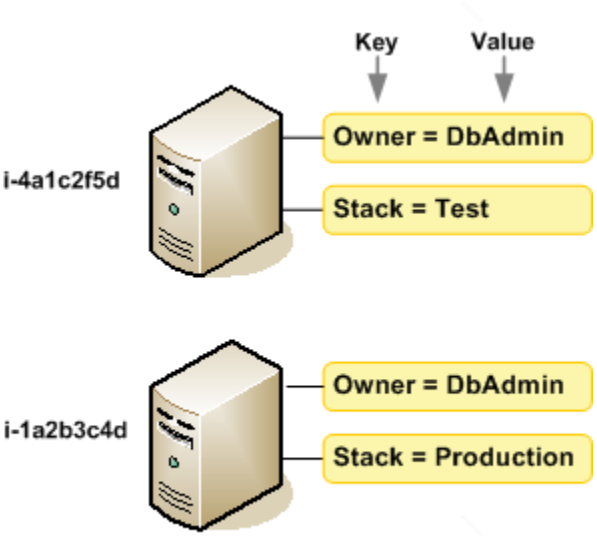
- Gerenciamento de tags e acesso
- Marcar com tag recursos para faturamento
- Trabalhar com tags usando o console
- Trabalhar com tags usando a linha de comando
- Trabalho com tags de instância em metadados de instância
- Adicionar tags a um recurso usando o CloudFormation

Conceitos Básicos de Tags

Uma tag um rótulo atribuído a um recurso AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Por exemplo, é possível definir um conjunto de tags para as instâncias do Amazon EC2 da sua conta que lhe ajudem a rastrear o proprietário e o nível do stack de cada instância.

O diagrama a seguir mostra como funciona o uso de tags. Neste exemplo, você atribuiu duas tags a cada uma de suas instâncias — uma tag com a chave `Owner` e outra com a chave `Stack`. Cada tag tem também um valor associado.



Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos da . É possível pesquisar e filtrar os recursos de acordo com as tags que

adicionar. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos, consulte o whitepaper da AWS Tagging Best Practices (Práticas recomendadas de marcação).

As tags não têm significado semântico no Amazon EC2 e são interpretadas estritamente como uma sequência dos caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

> **Note**
>
> Depois de excluir um recurso, suas etiquetas podem permanecer visíveis nas saídas do console, API e CLI por um curto período. Essas etiquetas serão gradualmente desassociadas do recurso e serão excluídas permanentemente.

Marcar com tag os recursos do

É possível usar tags na maioria dos recursos do Amazon EC2 que já existem na sua conta. A tabela a seguir lista os recursos compatíveis com o uso de tags.

Caso esteja usando o console do Amazon EC2, você poderá aplicar tags aos recursos usando a guia Tags na tela de recursos relevante ou usar o Editor de tags no console do AWS Resource Groups. Algumas telas de recursos permitem que você especifique tags para um recurso ao criá-lo; por exemplo, uma tag com uma chave de `Name` e um valor que você especificar. Na maioria dos casos, o console aplicará as tags imediatamente depois de o recurso ser criado (em vez de durante a criação de recursos). O console pode organizar os recursos de acordo com a tag `Name`, mas ela não tem nenhum significado semântico para serviço do Amazon EC2.

Se você estiver usando a API do Amazon EC2, a AWS CLI ou o AWS SDK, poderá usar a ação `CreateTags` da API do EC2 para aplicar tags aos recursos existentes. Além disso, algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, nós reverteremos o processo de criação de recursos. Isso garante que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso seja deixado sem tags. Ao marcar com tags os recursos no momento da

criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso. Para obter mais informações sobre como permitir que os usuários marquem os recursos durante a criação, consulte Conceder permissão para marcar recursos durante a criação.

A tabela a seguir descreve os recursos do Amazon EC2 que podem ser marcados e os recursos que podem ser marcados na criação usando a API do Amazon EC2, a AWS CLI ou um AWS SDK.

Suporte à marcação para recursos do Amazon EC2

Recurso	Compatível com tags	Oferece suporte à marcação na criação
AFI	Sim	Sim
AMI	Sim	Sim
Tarefa de pacote	Não	Não
Capacity Reservation	Sim	Sim
Gateway da operadora	Sim	Sim
Endpoint do Client VPN	Sim	Sim
Rota do Client VPN	Não	Não
Gateway do cliente	Sim	Sim
Dedicated Host	Sim	Sim
Reserva de Host dedicado	Sim	Sim
Opções do DHCP	Sim	Sim
Snapshot do EBS	Sim	Sim
Volume do EBS	Sim	Sim
EC2 Fleet	Sim	Sim
Gateway da Internet somente de saída	Sim	Sim

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Endereços elastic IP (EIPs)	Sim	Sim
Aceleradora do Elastic Graphics	Sim	Não
Instância	Sim	Sim
Janela de eventos de instância	Sim	Sim
Volumes de armazenamento de instâncias	N/D	N/D
Gateway da Internet	Sim	Sim
Grupo de endereços IP (BYOIP)	Sim	Sim
Par de chaves	Sim	Sim
Modelo de execução	Sim	Sim
Versão do modelo de execução	Não	Não
Gateway local	Sim	Não
Tabela de rotas do gateway local	Sim	Não
Interface virtual do gateway local	Sim	Não
Grupo de interface virtual do gateway local	Sim	Não

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Associação de VPC da tabela de rotas do gateway local	Sim	Sim
Associação de grupos de interface virtual da tabela de rotas do gateway local	Sim	Não
gateway NAT	Sim	Sim
Conexão ACL	Sim	Sim
Interface de rede	Sim	Sim
Placement group	Sim	Sim
Lista de prefixos	Sim	Sim
Reserved Instance	Sim	Não
Listagem do Instância reservada	Não	Não
Tabela de rotas	Sim	Sim
Solicitação de frota spot	Sim	Sim
Solicitação de instância Spot	Sim	Sim
Grupo de segurança	Sim	Sim
Regra do grupo de segurança	Sim	Não
Sub-rede	Sim	Sim
Filtro de espelho de tráfego	Sim	Sim
Sessão de espelho de tráfego	Sim	Sim

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Destino de espelho de tráfego	Sim	Sim
Transit gateway	Sim	Sim
Domínio multicast do gateway de trânsito	Sim	Sim
Tabela de rotas do Transit Gateway	Sim	Sim
Anexo da VPC do Transit Gateway	Sim	Sim
Gateway privado virtual	Sim	Sim
VPC	Sim	Sim
VPC endpoint	Sim	Sim
Serviço de VPC endpoint	Sim	Sim
Configuração do serviço do VPC endpoint	Sim	Sim
Log do fluxo da VPC	Sim	Sim
Conexão de emparelhamento de VPC	Sim	Sim
Conexão VPN	Sim	Sim

É possível aplicar tags em instâncias, volumes, gráficos elásticos, interfaces rede e solicitações de instâncias spot na criação usando o assistente de lançamento de instâncias do Amazon EC2 no console do Amazon EC2. Você pode marcar seus volumes do EBS ao criá-los usando a tela Volumes, ou snapshots do EBS usando a tela Snapshots. Se preferir, use as APIs do Amazon EC2 para criação de recursos (por exemplo, RunInstances) para aplicar tags ao criar seu recurso.

É possível aplicar permissões no nível do recurso com base em tags nas suas políticas do IAM para ações de API do Amazon EC2 que oferecem suporte à marcação durante a criação para implementar controle granular sobre os usuários e grupos que podem marcar recursos na criação. Seus recursos estão devidamente protegidos contra criação — as tags aplicadas imediatamente aos recursos; portanto, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor. Seus recursos podem ser rastreados e relatados com mais precisão. É possível obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Também é possível aplicar permissões em nível de recurso às ações `CreateTags` e `DeleteTags` da API do Amazon EC2 nas suas políticas do IAM, de forma a controlar quais chaves e valores de tags são definidos nos recursos existentes. Para obter mais informações, consulte Exemplo: marcar recursos.

Para obter mais informações sobre a aplicação de tags nos seus recursos para faturamento, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

Restrições de tags

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso –- 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e possuir apenas um valor.
- Comprimento máximo da chave –- 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Caracteres permitidos
  - Embora o EC2 permita qualquer caractere em suas tags, outros AWS serviços podem ser mais restritivos. Os caracteres permitidos em todos os serviços AWS são: letras (`a-z`, `A-Z`), números (`0-9`) e espaços representáveis em UTF-8, e os seguintes caracteres: `+ - = . _ : / @`.
  - Se você habilitar etiquetas de instância em metadados de instância, as chaves de etiquetas de instância só poderão usar letras (`a-z`, `A-Z`), números (`0-9`) e os seguintes caracteres:`+ - = . , _ : @`. As chaves de etiqueta de instância não podem conter espaços ou `/`, e não podem formar apenas `.` (um ponto), `..` (dois pontos) ou `_index`. Para ter mais informações, consulte Trabalho com tags de instância em metadados de instância.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.

- O prefixo `aws:` é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com esse prefixo. As tags com o prefixo `aws:` não contam para as tags por limite de recurso.

Você não pode encerrar, parar ou excluir um recurso baseado unicamente em suas tags; será preciso especificar o identificador de recursos. Por exemplo, para excluir snapshots marcados com uma chave de tag chamada `DeleteMe`, use a ação `DeleteSnapshots` com os identificadores de recursos dos snapshots, como `snap-1234567890abcdef0`.

Quando você marca recursos públicos ou compartilhados, as tags atribuídas ficam disponíveis somente para sua conta da AWS. Nenhuma outra conta da AWS terá acesso a essas tags. Para controle de acesso baseado em tags a recursos compartilhados, cada conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Você não pode marcar com tag todos os recursos. Para obter mais informações, consulte Suporte à marcação para recursos do Amazon EC2.

Gerenciamento de tags e acesso

Se você estiver usando o AWS Identity and Access Management (IAM), pode controlar quais usuários na sua conta da AWS têm permissão para criar, editar ou excluir tags. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

Também é possível usar tags de recurso para implementar o controle baseado em atributo (ABAC). É possível criar políticas do IAM que permitem operações com base nas tags do recurso. Para obter mais informações, consulte Controlar o acesso aos recursos do EC2 usando tags de recursos.

Marcar com tag recursos para faturamento

Também é possível usar tags para organizar sua conta da AWS para refletir sua própria estrutura de custo. Para isso, inscreva-se para obter sua conta da AWS com os valores de chave de tag incluídos. Para obter mais informações sobre como configurar um relatório de alocação de custos com tags, consulte Relatório mensal de alocação de custos no Manual do usuário do AWS Billing. Para ver o custo dos recursos combinados, é possível organizar as informações de faturamento com base nos recursos com os mesmos valores da chave da tag. Por exemplo, é possível etiquetar vários recursos com um nome de aplicação específico, e depois organizar suas informações de faturamento para ver o custo total daquela aplicação em vários serviços. Para obter mais informações, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

> **Note**
>
> Se você tiver acabado de habilitar a criação de relatórios, os dados do mês atual estarão disponíveis para visualização após 24 horas.

Tags de alocação de custos podem indicar quais recursos estão contribuindo para os custos, mas excluí-los ou desativá-los nem sempre reduz custos. Por exemplo, os dados de snapshots consultados por outro snapshot são preservados, mesmo se o snapshot que contém os dados originais for excluído. Para obter mais informações, consulte Volumes e snapshots do Amazon Elastic Block Store no Manual do usuário do AWS Billing.

> **Note**
>
> Os endereços IP elásticos marcados não são exibidos no seu relatório de alocação de custos.

Trabalhar com tags usando o console

Você pode usar o console do Amazon EC2 para exibir tags de um recurso individual e para aplicar ou remover tags de um recurso por vez.

Você pode usar o Editor de tags no console do AWS Resource Groups para exibir as tags de todos os seus recursos do Amazon EC2 em todas as regiões. É possível visualizar tags por recurso e por tipo de recurso, e você ver que tipos de recurso estão associados a uma tag especificada. Você pode aplicar ou remover tags de vários recursos e vários tipos de recursos por vez. O Editor de tags fornece uma forma central e unificada para criar e gerenciar suas tags. Para obter mais informações, consulte o Guia do usuário de recursos da AWS para marcação.

Tarefas

- Exibir tags
- Adicionar e excluir tags em um recurso individual
- Adicionar e excluir tags para vários recursos
- Adicionar uma tag ao executar uma instância
- Filtrar uma lista de recursos por tag

Exibir tags

Você pode exibir tags de um recurso individual no console do Amazon EC2. Para exibir as tags de todos os seus recursos, use o Editor de tags no console do AWS Resource Groups.

Exibir tags de um recurso individual

Quando você selecionar uma página específica do recurso no console do Amazon EC2, ela exibirá uma lista desses recursos. Por exemplo, se você selecionar Instances (Instâncias) no painel de navegação, o console exibirá uma lista das instâncias do Amazon EC2. Ao selecionar um recurso de uma dessas listas (por exemplo, uma instância), se o recurso é compatível com tags, é possível ver e gerenciá-las. Na maioria das páginas de recursos, é possível visualizar as tags ao escolher a guia Tags.

Você pode adicionar uma coluna à lista de recursos para exibir todos os valores das tags com a mesma chave. Você pode usar essa coluna para classificar e filtrar a lista de recursos pela tag.

New console

Para adicionar uma coluna à lista de recursos para exibir suas tags

1. No console do EC2, escolha o ícone Preferências com a engrenagem no canto superior direito da tela.
2. Na caixa de diálogo Preferências, em Marcar colunas (na parte inferior esquerda), selecione uma de mais chaves de tag e escolha Confirmar.

Old console

Há duas maneiras de adicionar uma coluna nova à lista de recursos para exibir suas tags:

- Na guia Tags, selecione Mostrar coluna. Uma nova coluna será adicionada ao console.
- Escolha o ícone de engrenagem Mostrar/ocultar colunas e a caixa de diálogo Mostrar/ocultar colunas, selecione a chave de tags em Suas chaves de tag.

Exibir tags para vários recursos

Você pode exibir tags em vários recursos usando o Editor de tags no console do AWS Resource Groups. Para obter mais informações, consulte o Guia do usuário de recursos da AWS para marcação.

Adicionar e excluir tags em um recurso individual

É possível gerenciar as tags para um recurso individual diretamente pela página de recursos.

Para adicionar uma tag a um recurso individual

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual o recurso a ser marcado estão localizados. Para ter mais informações, consulte Localizações de recursos.
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e escolha a guia Tags.
5. Escolha a guia Gerenciar tags e depois Adicionar nova tag. Insira a chave e o valor da tag. Escolha Adicionar nova tag novamente para cada tag adicional a acrescentar. Quando terminar de adicionar tags, selecione Save (Salvar).

Para excluir uma tag de um recurso individual

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual o recurso a ser desmarcado estão localizados. Para ter mais informações, consulte Localizações de recursos.
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e escolha a guia Tags.
5. Selecione Manage tags (Gerenciar tags). Para cada tag a ser removida, selecione Remover. Ao finalizar a remoção de tags, escolha Save (Salvar).

Adicionar e excluir tags para vários recursos

Para adicionar uma tag a vários recursos

1. Abra o Editor de tags no console do AWS Resource Groups em https://console.aws.amazon.com/resource-groups/tag-editor.
2. Para Regiões, selecione uma ou mais regiões nas quais os recursos a serem marcados estão localizados.
3. Para Tipos de recursos, selecione o tipo de recursos a serem marcados (por exemplo, AWS::EC2::Instance).

4. Escolha Recursos de pesquisa.
5. Em Resultados da pesquisa de recursos, marque a caixa de seleção ao lado de cada recurso a ser marcado.
6. Escolha Gerenciar tags de recursos selecionados.
7. Em Editar tags de todos os recursos selecionados, escolha Adicionar tag e, em seguida, insira a nova chave e o novo valor da tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

   > **Note**
   >
   > Se você adicionar uma nova tag com a mesma chave de uma tag existente, a nova sobrescreverá a tag existente.

8. Escolha Revisar e aplicar alterações de tag.
9. Selecione Apply changes to all selected (Aplicar alterações a todos os itens selecionados).

Para remover uma tag de vários recursos

1. Abra o Editor de tags no console do AWS Resource Groups em https://console.aws.amazon.com/resource-groups/tag-editor.
2. Para Regiões, selecione as regiões nas quais os recursos a serem desmarcados estão localizados.
3. Para Tipos de recursos, selecione o tipo de recursos a serem desmarcados (por exemplo, AWS::EC2::Instance).
4. Escolha Recursos de pesquisa.
5. Em Resultados da pesquisa de recursos, marque a caixa de seleção ao lado de cada recurso a ser desmarcado.
6. Escolha Gerenciar tags de recursos selecionados.
7. Em Editar tags de todos os recursos selecionados, ao lado da tag a ser removida, escolha Remover tag.
8. Escolha Revisar e aplicar alterações de tag.
9. Selecione Apply changes to all selected (Aplicar alterações a todos os itens selecionados).

Adicionar uma tag ao executar uma instância

New console

Para adicionar uma tag usando o assistente de inicialização de instância

1. Na barra de navegação, selecione a região da instância. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Selecione a região que satisfaz suas necessidades. Para obter mais informações, consulte Localizações de recursos.
2. Escolha Iniciar instância.
3. Em Name and tags (Nome e tags), você pode inserir um nome descritivo para a instância e especificar as tags.

   O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar. É possível marcar a instância, os volumes, os gráficos elásticos e as interfaces de rede. Para instâncias spot, é possível marcar apenas a solicitação de instância spot.

   A especificação de um nome de instância e de tags adicionais é opcional.

   - Em Name (Nome), insira um nome descritivo para a instância. Se você não especificar um nome, a instância poderá ser identificada por seu ID, que é gerado automaticamente quando você inicia a instância.
   - Para adicionar mais tags, selecione Add additional tag (Adicionar outra tag). Escolha Add tag (Adicionar tag), insira uma chave e um valor, e selecione o tipo de recurso a aplicar a tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha o sistema operacional da instância e selecione uma AMI. Para ter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).
5. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
6. Mantenha todos os outros campos com os valores padrão ou escolha valores específicos para a configuração de instância desejada. Para obter informações sobre os campos, consulte Iniciar uma instância usando parâmetros definidos.

7. No painel Summary (Resumo), revise a configuração da instância e selecione Launch instance (Iniciar instância).

Old console

Para adicionar uma tag usando o assistente de inicialização de instância

1. Na barra de navegação, selecione a região da instância. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Selecione a região que satisfaz suas necessidades. Para obter mais informações, consulte Localizações de recursos.
2. Escolha Launch Instance (Executar instância).
3. A página Choose an Amazon Machine Image (AMI) (Escolher uma Imagem de máquina da Amazon (AMI)) exibe uma lista de configurações básicas denominadas Imagens de máquina da Amazon (AMI). Selecione as AMIs a serem usadas e escolha Selecionar. Para obter mais informações, consulte Encontrar uma AMI.
4. Na página Configurar detalhes da instância, configure as configurações da instância conforme necessário e selecione Próximo: Adicionar armazenamento.
5. Na página Adicionar armazenamento, especifique os volumes de armazenamento adicionais para sua instância. Selecione Próximo: Adicionar tags ao concluir.
6. Na página Adicionar tags, especifique tags da instância, os volumes ou ambos. Escolha Adicionar outra tag para adicionar mais de uma tag à sua instância. Escolha Next: Configure Security Group (Próximo: Configurar grupo de segurança) ao concluir.
7. Na página Configurar security group (Configurar grupo de segurança), escolha qualquer grupo de segurança existente que você possui ou deixe o assistente criar um novo grupo de segurança para você. Selecione Revisar e executar ao concluir.
8. Examine suas configurações. Quando você estiver satisfeito com suas seleções, escolha Executar. Selecione um par de chaves existente ou crie um novo, selecionando a caixa de confirmação e escolhendo Executar instâncias.

Filtrar uma lista de recursos por tag

É possível filtrar sua lista de recursos baseados em uma ou mais chaves e valores de tags.

Para filtrar uma lista de recursos por tag no console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
3. Escolha o campo de pesquisa.
4. Na lista, em Tags, escolha a chave da tag.
5. Escolha o valor de tag correspondente na lista.
6. Quando terminar, remova o filtro.

Para obter mais informações sobre o uso de filtros no console do Amazon EC2, consulte Listar e filtrar seus recursos.

Para filtrar vários recursos entre regiões por tag usando o Editor de tags

Você pode usar o Editor de tags no console do AWS Resource Groups para filtrar vários recursos entre várias regiões por tag. Para obter mais informações, consulte Descobrir recursos para marcar no Guia do usuário de recursos da AWS.

Trabalhar com tags usando a linha de comando

Você pode adicionar tags a muitos recursos do EC2 ao criá-las usando o parâmetro de especificações de tag para o comando de criação. É possível visualizar as tags de um recurso usando o comando de descrição para o recurso. Também é possível adicionar, atualizar ou excluir tags para seus recursos existentes usando os seguintes comandos.

Tarefa	AWS CLI	AWS Tools for Windows PowerShell
Adicione ou substitua uma ou mais tags	create-tags	New-EC2Tag
Exclua uma ou mais tags	delete-tags	Remove-EC2Tag
Descreva uma ou mais tags	describe-tags	Get-EC2Tag

Tarefas

- Adicionar tags na criação de recursos

- Adicionar tags a um recurso existente
- Descrever recursos marcados com tags

Adicionar tags na criação de recursos

Os exemplos a seguir demonstram como aplicar tags ao criar recursos.

> **Note**
>
> A maneira como insere os parâmetros formatados pelo JSON na linha de comando difere dependendo de seu sistema operacional.
>
> - Linux, macOS ou Unix e Windows PowerShell: use aspas simples (') para delimitar a estrutura de dados JSON.
> - Windows: omita as aspas simples ao usar os comandos com a linha de comando do Windows.
>
> Para obter mais informações, consulte Specifying parameter values for the AWS CLI (Especificar valores de parâmetro para a CLI).

Example Exemplo: execute uma instância e aplique tags à instância e ao volume

O seguinte comando run-instances inicia uma instância e aplica uma tag com a chave **webserver** e o valor **production** à instância. O comando também aplica uma tag com uma chave de **cost-center** e um valor de **cc123** a qualquer volume do EBS criado (neste caso, o volume do dispositivo raiz).

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications
 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

É possível aplicar as mesmas chaves da tag e os mesmos valores aos dois volumes e instâncias durante a execução. O comando a seguir executa uma instância e aplica uma tag com uma chave de **`cost-center`** e um valor de **`cc123`** à instância e a qualquer volume do EBS criado.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example Exemplo: crie um o volume e aplique uma tag

O comando create-volume cria um volume e aplica duas tags: **`purpose=production`** e **`cost-center=cc123`**.

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

Adicionar tags a um recurso existente

Os exemplos a seguir demonstram como adicionar tags a um recurso existente usando o comando create-tags.

Example Exemplo: adicionar uma tag a um recurso

O seguinte comando adiciona a tag **`Stack=production`** à imagem especificada ou substitui uma tag existente para a AMI na qual a chave de tag é **`Stack`**. Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example Exemplo: adicionar tags a vários recursos

Este exemplo adiciona (ou substitui) duas tags para uma AMI e uma instância. Uma das tags contém apenas uma chave (**webserver**), sem valor (definimos o valor como uma string vazia). A outra tag consiste em uma chave (**stack**) e um valor (**Production**). Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Exemplo: adicionar tags com caracteres especiais

Este exemplo adiciona a tag **[Group]=test** a uma instância. Os colchetes (**[** e **]**) são caracteres especiais, que devem ser recuados.

Se você estiver usando o Linux ou o OS X, para recuar os caracteres especiais, coloque o elemento com o caractere especial entre aspas duplas (**"**) e coloque toda a estrutura de chave e valor entre aspas simples (**'**).

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Se você estiver usando o Windows, para recuar os caracteres especiais, coloque o elemento que tem caracteres especiais entre aspas duplas (") e preceda cada caractere de aspas duplas com uma barra invertida (****) da seguinte maneira:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Se você estiver usando o Windows PowerShell, para recuar os caracteres especiais, coloque o valor que tem caracteres especiais entre aspas duplas (**"**), preceda cada caractere de aspas duplas com uma barra invertida (****) e coloque toda a estrutura de chave e valor entre aspas simples (**'**) da seguinte maneira:

```
aws ec2 create-tags `
```

```
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Descrever recursos marcados com tags

Os exemplos a seguir mostram como usar filtros com describe-instances para visualizar instâncias com tags específicas. Todos os comandos “describe” do EC2 usam essa sintaxe para filtrar por tag em um único tipo de recurso. Como alternativa, é possível usar o comando describe-tags para filtrar por tag entre os tipos de recursos do EC2.

Example Exemplo: descreva as instâncias com a chave de tags especificada

O comando a seguir descreve as instâncias com a tag **`Stack`**, independentemente do valor da tag.

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example Exemplo: descreva as instâncias com a tag especificada

O comando a seguir descreve as instâncias com a tag **`Stack=production`**.

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example Exemplo: descreva as instâncias com o valor de tag especificado

O comando a seguir descreve as instâncias com uma tag com o valor **`production`**, independentemente da chave da tag.

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example Exemplo: descrever todos os recursos do EC2 com a tag especificada

O comando a seguir descreve todos os recursos do EC2 com a tag **`Stack=Test`**.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Trabalho com tags de instância em metadados de instância

É possível acessar as tags de uma instância a partir dos metadados da instância. Ao acessar tags dos metadados da instância, não é mais necessário usar chamadas de API `DescribeInstances` ou `DescribeTags` para recuperar informações de tags, o que reduz suas transações de API por segundo e permite que as recuperações de tags sejam escaladas com o número de instâncias que você controla. Além disso, os processos locais que estão sendo executados em uma instância podem visualizar as informações de tag da instância diretamente dos metadados da instância.

Por padrão, as tags não estão disponíveis a partir dos metadados da instância; permita explicitamente o acesso. É possível permitir o acesso no início da instância ou após o início em uma instância em execução ou parada. Também é possível permitir o acesso a tags especificando isso em um modelo de execução. As instâncias iniciadas usando o modelo permitem acesso a tags nos metadados da instância.

Se você adicionar ou remover uma tag de instância, os metadados da instância serão atualizados enquanto a instância estiver em execução, sem precisar interromper e iniciar a instância.

Tópicos

- Permitir acesso a tags em metadados de instância
- Desativar o acesso a tags em metadados de instância
- Visualize se é permitido o acesso a tags em metadados da instância
- Recuperar tags dos metadados da instância

Permitir acesso a tags em metadados de instância

Por padrão, não há acesso a tags de instância nos metadados da instância. Para cada instância, permita explicitamente o acesso usando um dos métodos a seguir.

Para permitir acesso a tags em metadados de instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Instance settings (Configurações da instância), Allow tags in instance metadata (Permitir tags em metadados de instância).
4. Para permitir o acesso a tags nos metadados da instância, marque a caixa de seleção Allow (Permitir).

5. Escolha Salvar.

Para permitir acesso a tags em metadados de instância no início usando a AWS CLI

Use o comando run-instances e defina `InstanceMetadataTags` como `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

Para permitir o acesso a tags em metadados de instância em uma instância em execução ou parada usando a AWS CLI

Use o comando modify-instance-metadata-options e defina `--instance-metadata-tags` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

Desativar o acesso a tags em metadados de instância

Para desativar o acesso a tags de instância nos metadados da instância, use um dos métodos a seguir. Você não precisa desativar o acesso a tags de instância nos metadados da instância no início, pois ele está desativado por padrão.

Para desativas o acesso a tags em metadados de instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Instance settings (Configurações da instância), Allow tags in instance metadata (Permitir tags em metadados de instância).
4. Para desativar o acesso a tags nos metadados da instância, limpe a caixa de seleção Allow (Permitir).
5. Escolha Salvar.

Para desativar o acesso a tags em metadados de instância usando a AWS CLI

Use o comando modify-instance-metadata-options e defina `--instance-metadata-tags` como `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags disabled
```

Visualize se é permitido o acesso a tags em metadados da instância

Para cada instância, você pode usar o console ou a AWS CLI do Amazon EC2 para visualizar se é permitido o acesso a tags da instância nos metadados da instância.

Para visualizar se é permitido o acesso a tags nos metadados da instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione uma instância.
3. Na guia Details (Detalhes), marque o campo Allow tags in instance metadata (Permitir tags nos metadados da instância). Se o valor for Enabled (Habilitado), serão permitidas tags nos metadados da instância. Se o valor for Disabled (Desabilitado), serão permitidas tags nos metadados da instância não.

Para visualizar se é permitido o acesso a tags nos metadados da instância usando a AWS CLI

Use o comando describe-instances e especifique o ID da instância.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

Este exemplo de saída foi truncado por questão de espaço. O parâmetro `"InstanceMetadataTags"` indica se são permitidas tags nos metadados da instância. Se o valor for `enabled`, serão permitidas tags nos metadados da instância. Se o valor for `disabled`, não serão permitidas tags nos metadados da instância.

```
{
    "Reservations": [
        {
```

```
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
    ...

    "MetadataOptions": {
    "State": "applied",
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "disabled",
    "InstanceMetadataTags": "enabled"
    },
    ...
```

Recuperar tags dos metadados da instância

Se as tags de instância forem permitidas nos metadados da instância, a categoria `tags/instance` será acessível a partir dos metadados da instância. Para obter exemplos sobre como recuperar tags dos metadados da instância, consulte Obter as tags de instância de uma instância de uma instância.

Adicionar tags a um recurso usando o CloudFormation

Com tipos de recursos do Amazon EC2, você especifica tags usando uma propriedade `Tags` ou `TagSpecifications`.

Os exemplos a seguir adicionam a tag **`Stack=Production`** ao AWS::EC2::Instance usando a propriedade `Tags`.

Example Exemplo: tags em YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Exemplo: tags em JSON

```
"Tags": [
```

```
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

Os exemplos a seguir adicionam a tag **`Stack=Production`** ao AWS::EC2::LaunchTemplate LaunchTemplateData usando a propriedade `TagSpecifications`.

Example Exemplo: TagSpecifications em YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Exemplo: TagSpecifications em JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Service Quotas do Amazon EC2

O Amazon EC2 fornece recursos diferentes que é possível usar. Esses recursos incluem imagens, instâncias, volumes e snapshots. Ao criar sua Conta da AWS, definimos cotas padrão (também chamadas de limites) nesses recursos de acordo com a região. Por exemplo, há um limite no número máximo de instâncias que podem ser iniciadas em uma região. Assim, se for necessário executar uma instância na região Oeste dos EUA (Oregon), por exemplo, a solicitação não deverá fazer com que o uso exceda o número máximo de instâncias nessa região.

O console de Service Quotas é um local central onde é possível visualizar e gerenciar suas cotas de serviços da AWS e solicitar um aumento de cota para muitos dos recursos que você usa. Use as informações de cota que fornecemos para gerenciar sua infraestrutura da AWS. Planeje a solicitação de aumentos das cotas com antecedência antes que sejam necessários.

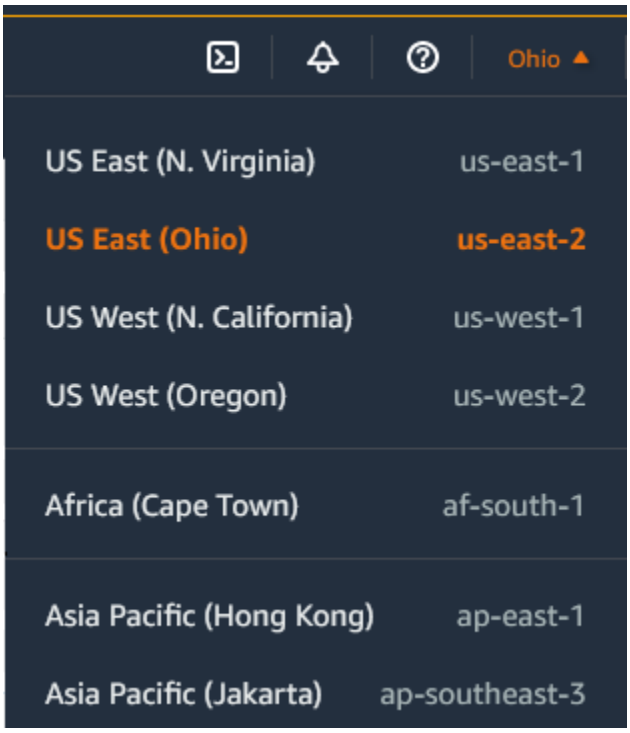
Para obter mais informações, consulte Endpoints e cotas do Amazon EC2 e Endpoints e cotas do Amazon EBS na Referência geral da Amazon Web Services.

Visualizar as cotas atuais

É possível visualizar suas cotas de cada região usando o console do Service Quotas do .

Para visualizar as cotas atuais usando o console do Service Quotas

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação (na parte superior da tela), selecione uma região.



3. Use o campo de filtro para filtrar a lista por nome de recurso. Por exemplo, insira **`On-Demand`** para localizar as cotas para instâncias sob demanda.
4. Para ver mais informações, escolha o nome da cota para abrir a página de detalhes sobre a cota.

Solicitar um aumento

É possível solicitar um aumento de cota para cada região.

Para solicitar um aumento, visite o Console do Service Quotas

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação (na parte superior da tela), selecione uma região.
3. Use o campo de filtro para filtrar a lista por nome de recurso. Por exemplo, insira **`On-Demand`** para localizar as cotas para instâncias sob demanda.
4. Se a cota for ajustável, escolha a cota e, em seguida, escolha Solicitar aumento de cota.
5. Em Alterar valor da cota, insira o novo valor da cota.
6. Escolha Solicitar.
7. Para visualizar quaisquer solicitações pendentes ou resolvidas recentemente no console, escolha Painel no painel de navegação. Para solicitações pendentes, escolha o status da solicitação para abrir o recibo da solicitação. O status inicial de uma solicitação é Pending (Pendente). Depois que o status for alterado para Cota solicitada, você verá o número do caso com o AWS Support. Escolha o número do caso para abrir o tíquete de sua solicitação.

Para obter mais informações, incluindo como usar a AWS CLI ou os SDKs para solicitar um aumento de cota, consulte Solicitação de aumento de cota no Guia do usuário do Service Quotas.

Restrição para e-mails enviados usando a porta 25

Em todas as instâncias, o Amazon EC2 restringe o tráfego de saída para endereços IP públicos na porta 25 por padrão. É possível solicitar que essa restrição seja removida. Para obter mais informações, consulte Como removo a restrição à porta 25 de uma instância do Amazon EC2 ou de uma função do Lambda?

> **Note**
>
> Essa restrição não se aplica ao tráfego de saída enviado pela porta 25 para:
>
> - Endereços IP no bloco CIDR primário da VPC na qual a interface de rede de origem exista.
> - Endereços IP nos CIDRs definidos em RFC 1918, RFC 6598, e RFC 4193.

Solução de problemas de instâncias do EC2

Os procedimentos e dicas apresentados a seguir podem ajudar você a solucionar problemas relacionados às instâncias do Amazon EC2.

Conteúdo

- Problemas comuns com instâncias do Windows
- Mensagens comuns com instâncias do Windows
- Solucionar problemas de execução de instâncias
- Solução de problemas de conexão com a instância do Linux
- Solução de problemas para conexão à instância do Windows
- Redefinir uma senha de administrador do Windows perdida ou expirada
- Solucionar problemas de uma instância não acessível
- Solução de problemas na interrupção da instância
- Solucionar problemas de encerramento (desativação) da instância
- Solução de problemas de instâncias do Linux com falhas nas verificações de status
- Solução de problemas de inicialização da instância do Linux usando o volume errado
- Solução de problemas de Sysprep com instâncias do Windows
- Usar o EC2Rescue para Linux
- Usar o EC2Rescue for Windows Server
- Console de Série do EC2 para as instâncias do Amazon EC2
- Enviar uma interrupção para diagnóstico (para usuários avançados)

Problemas comuns com instâncias do Windows

Veja a seguir dicas de solução de problemas para ajudar a resolver problemas comuns com instâncias do EC2 Windows Server.

Problemas

- Os volumes do EBS não são inicializados no Windows Server 2016 e 2019
- Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)

- A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado
- Não foi possível obter o resultado do console
- Windows Server 2012 R2 não disponível na rede
- Colisão de assinatura em disco

Os volumes do EBS não são inicializados no Windows Server 2016 e 2019

Instâncias criadas nas Imagens de máquina da Amazon (AMIs) para Windows Server 2016 e 2019 usam o agente EC2Launch v1 para uma variedade de tarefas de inicialização, incluindo a inicialização de volumes do EBS. Por padrão, o EC2Launch v1 não inicializa volumes secundários. No entanto, é possível configurar o EC2Launch v1 para inicializar esses discos automaticamente, como mostrado a seguir.

Mapear letras de unidade a volumes

1. Conecte-se à instância para configurar e abrir o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` em um editor de texto.
2. Especifique as configurações do volume da seguinte maneira:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
   "driveLetter": "H"
 }]
}
```

3. Salve as alterações e feche o arquivo.
4. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch v1 que inicializa os discos:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

   Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador `-Schedule` da seguinte forma:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

O agente EC2Launch v1 pode executar scripts de inicialização de instâncias, como `initializeDisks.ps1` em paralelo com o script `InitializeInstance.ps1`. Se o script `InitializeInstance.ps1` reinicializar a instância, ele poderá interromper outras tarefas agendadas que são executadas na inicialização da instância. Para evitar possíveis conflitos, recomendamos que você adicione lógica ao seu script `initializeDisks.ps1` para garantir que a inicialização da instância tenha sido concluída primeiro.

> **Note**
>
> Se o script EC2Launch não inicializar os volumes, verifique se os volumes estão online. Se os volumes estiverem offline, execute o comando a seguir para colocar todos os discos online.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)

Se uma instância que estiver executando o Microsoft Active Directory tiver uma falha do sistema ou outros problemas críticos, você poderá solucionar problemas na instância inicializando em uma versão especial do modo seguro denominado Directory Services Restore Mode (DSRM). No DSRM, você pode reparar ou recuperar o Ative Directory.

Suporte a drivers para DSRM

A forma como você habilita o DSRM e faz a inicialização na instância depende dos drivers que a instância estiver executando. No console do EC2, você pode visualizar os detalhes de versão do driver para uma instância no log do sistema. As tabelas a seguir mostram quais drivers são compatíveis com o DSRM.

Versões do driver	DSRM com suporte?	Próximas etapas
Citrix PV 5.9	Não	Restaure a instância de um backup. Você não pode habilitar o DSRM.
AWS PV 7.2.0	Não	Embora o DSRM não tenha suporte para esse driver, você ainda pode desanexar o volume raiz da instância , criar um snapshot do volume ou criar uma AMI dele e anexá-la a outra instância na mesma zona de disponibi lidade que um volume secundário. Em seguida, você pode habilitar o DSRM (como descrito nesta seção).
AWS PV 7.2.2 e posteriores	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).
Redes avançadas	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).

Para obter informações sobre como habilitar as redes aperfeiçoadas, consulte the section called “Elastic Network Adapter (ENA)”. Para obter informações sobre como atualizar drivers PV da AWS, consulte Upgrade PV drivers on Windows instances.

Configurar uma instância para ser inicializada no DSRM

As instâncias do EC2 Windows não têm conectividade de rede antes que o sistema operacional seja executado. Por esse motivo, você não pode pressionar o botão F8 no teclado para selecionar uma opção de inicialização. Você deve usar um dos seguintes procedimentos para inicializar uma instância do EC2 Windows Server no DSRM.

Se você suspeitar que o Active Directory foi danificado e a instância ainda estiver em execução, você poderá configurar a instância para fazer a inicialização no DSRM usando a caixa de diálogo Configurações do sistema ou o prompt de comando.

Para inicializar uma instância online no DSRM usando a caixa de diálogo Configurações do sistema

1. Na caixa de diálogo Executar, digite `msconfig` e pressione Enter.
2. Escolha a guia Inicializar.

3. Em Opções de inicialização, escolha Inicialização segura.
4. Escolha Reparo do Active Directory e escolha OK. O sistema solicita que você reinicialize o servidor.

Para inicializar uma instância online no DSRM usando a linha de comando

Em uma janela do prompt de comando, execute o comando a seguir:

```
bcdedit /set safeboot dsrepair
```

Se uma instância estiver offline e inacessível, você deverá desanexar o volume raiz e anexá-lo a outra instância para habilitar o modo DSRM.

Para inicializar uma instância offline no DSRM

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize e selecione a instância afetada. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância).
4. Escolha Launch instances (Executar instância) e crie uma instância temporária na mesma zona de disponibilidade que a instância afetada. Escolha um tipo de instância que use uma versão diferente do Windows. Por exemplo, se sua instância for o Windows Server 2016, escolha uma instância do Windows Server 2019.

   > **Important**
   >
   > Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No painel de navegação, escolha Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Separe o volume e associe-o à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use a Área de Trabalho Remota para conectar-se à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.

8. Abra um prompt de comando e execute o seguinte comando. Substitua D pela letra real de unidade do volume secundário que você acabou de anexar:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
10. No console do EC2, separe o volume afetado de instância temporária e reanexe-o à sua instância original com o nome de dispositivo `/dev/sda1`. Você deve especificar o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
11. Inicie a instância.
12. Depois que a instância passar nas verificações de integridade no console do EC2, conecte-se à instância usando o Remote Desktop e verifique se ela é inicializada no modo DSRM.
13. (Opcional) Exclua ou interrompa a instância temporária que você criou nesse procedimento.

A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado

Se você reiniciar sua instância e perder a conectividade de rede, é possível que a instância tenha o horário errado.

Por padrão, as instâncias do Windows usam o tempo universal coordenado (UTC). Se você definir o horário de sua instância como outro fuso horário e, em seguida, reiniciá-la, ocorrerá um desvio no horário, e a instância perderá temporariamente seu endereço IP. A instância recuperará a conectividade de rede, mas isso pode levar várias horas. A quantidade de tempo que leva para a instância recuperar a rede de conectividade depende da diferença entre o UTC e o outro fuso horário.

Esse mesmo problema no horário também pode fazer com que as tarefas agendadas não sejam executadas no horário esperado. Nesse caso, as tarefas agendadas não são executadas quando esperado porque a instância tem o horário incorreto.

Para usar um fuso horário diferente do UTC de forma persistente, você deve definir a chave de Registro RealTimeIsUniversal. Sem essa chave, a instância usará o UTC depois de reiniciá-la.

Para resolver problemas no horário que causam a perda da conectividade de rede

1. Certifique-se de que você esteja executando os drivers PV recomendados. Para ter mais informações, consulte the section called “Atualizar drivers de PV”.
2. Verifique se a chave de Registro a seguir existe e está definida como 1: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation \RealTimeIsUniversal

Não foi possível obter o resultado do console

Para instâncias do Windows, o console da instância exibe o resultado das tarefas realizadas durante o processo de inicialização do Windows. Se o Windows for inicializado com êxito, a última mensagem registrada será `Windows is Ready to use`. Você também pode exibir mensagens de log de eventos no console, mas esse recurso pode não estar habilitado por padrão, dependendo da sua versão do Windows. Para ter mais informações, consulte the section called “Definição de agentes de inicialização do Windows”.

Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema). Para obter a saída do console usando a linha de comando, use um dos seguintes comandos: get-console-output (AWS CLI) ou Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell).

Para instâncias executadas no Windows Server 2012 R2 e anteriores, se a saída do console estiver vazia, poderá indicar um problema com o serviço EC2Config, como um arquivo de configuração desconfigurado ou que o Windows não foi inicializado corretamente. Para corrigir o problema, faça download e instale a versão mais recente do EC2Config. Para ter mais informações, consulte the section called “Instalar o EC2Config”.

Windows Server 2012 R2 não disponível na rede

Para obter informações sobre como solucionar problemas de uma instância do Windows Server 2012 R2 que não está disponível na rede, consulte Windows Server 2012 R2 loses network and storage connectivity after an instance reboot.

Colisão de assinatura em disco

Você pode conferir e resolver colisões de assinatura em disco usando o EC2Rescue para Windows Server. Como alternativa, você pode resolver problemas de assinatura em disco manualmente realizando as etapas a seguir.

> **Warning**
>
> O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulteConfigure the Registry (Configurar o Registro).

1. Abra um prompt de comando, digite regedit.exe e pressione Enter.
2. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.
3. Digite Windows Boot Manager e escolha Localizar Próxima.
4. Escolha a chave chamada `11000001`. Essa chave é irmã da chave que você localizou na etapa anterior.
5. No painel direito, selecione `Element` e escolha Modificar no menu de contexto (clique com o botão direito do mouse).
6. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Esta é a assinatura do Boot Configuration Database (BCD). Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é `E9EB3AA5`:

   ```
   ...
   0030  00 00 00 00 01 00 00 00
   0038  A5 3A EB E9 00 00 00 00
   0040  00 00 00 00 00 00 00 00
   ...
   ```

7. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

   ```
   diskpart
   ```

8. Execute o comando `select disk` DiskPart e especifique o número do disco para o volume com a colisão da assinatura do disco.

> **Tip**
>
> Para verificar o número do disco do volume com a colisão da assinatura do disco, use o utilitário de Gerenciamento de disco. Abra um prompt de comando, digite `compmgmt.msc` e pressione Enter. No painel de navegação à esquerda, clique duas vezes em Gerenciamento de disco. No utilitário de Gerenciamento de disco, verifique o número do disco do volume off-line com a colisão de assinatura do disco.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Mensagens comuns com instâncias do Windows

Esta seção inclui dicas para ajudar a solucionar problemas com base em mensagens comuns.

Mensagens

- "A senha não está disponível"
- "A senha ainda não está disponível"
- "Não é possível recuperar a senha do Windows"
- "Esperando o serviço de metadados"
- "Não é possível ativar o Windows"

- "O Windows não é genuíno (0x80070005)"
- "Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"
- “Algumas configurações são gerenciadas pela sua organização”

"A senha não está disponível"

Para se conectar a uma instância do Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. Você pode recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

É possível gerar uma senha para a conta do administrador para instâncias iniciadas usando uma AMI personalizada do Windows. Para gerar a senha, você precisará definir algumas configurações no sistema operacional antes da criação da AMI. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Se sua instância do Windows não estiver configurada para gerar uma senha aleatória, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Verifique a saída do console relativa à instância para ver se a AMI usada para executá-la foi criada com a geração de senha desabilitada. Se a geração de senha estiver desabilitada, a saída do console conterá o seguinte:

```
Ec2SetPassword: Disabled
```

Se a geração de senha estiver desabilitada e não se lembrar da senha da instância original, você poderá redefinir a senha para essa instância. Para ter mais informações, consulte Redefinir uma senha de administrador do Windows perdida ou expirada.

"A senha ainda não está disponível"

Para se conectar a uma instância do Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. Você pode recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

A senha deve estar disponível em instantes. Se a senha não estiver disponível, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Se estiver demorando mais do que quatro minutos e você ainda não conseguiu obter a senha, é possível que o agente de execução da sua instância não esteja configurado para gerar uma senha. Verifique se a saída do console está vazia. Para ter mais informações, consulte Não foi possível obter o resultado do console.

Verifique também se a conta do AWS Identity and Access Management (IAM) que está sendo usada para acessar o Portal de Gerenciamento tem a ação `ec2:GetPasswordData` permitida. Para obter mais informações sobre as permissões do IAM, consulte O que é IAM?.

"Não é possível recuperar a senha do Windows"

Para recuperar a senha gerada automaticamente para a conta de administrador, você deve usar a chave privada para o par de chaves que você especificou ao executar a instância. Se você não tiver especificado um par de chaves quando executou a instância, você receberá a seguinte mensagem.

```
Cannot retrieve Windows password
```

Você pode encerrar essa instância e executar uma nova instância usando a mesma AMI, certificando-se de especificar um par de chaves.

"Esperando o serviço de metadados"

Uma instância do Windows deve obter informações dos metadados de sua instância para poder se ativar. Por padrão, a configuração `WaitForMetaDataAvailable` assegura que o serviço EC2Config aguardará que os metadados da instância fiquem acessíveis antes de continuar com

o processo de inicialização. Para ter mais informações, consulte Trabalhar com metadados de instância.

Se a instância falhar no teste de acessibilidade, experimente o seguinte para resolver o problema.

- Verifique o bloco CIDR de sua VPC. Uma instância do Windows não pode ser inicializada corretamente se for executada em uma VPC com um intervalo de endereços IP de `224.0.0.0` a `255.255.255.255` (intervalos de endereços IP de classe D e classe E). Esses intervalos de endereços IP são reservados e não devem ser atribuídos a dispositivos de host. Recomendamos criar uma VPC com um bloco CIDR dos intervalos de endereços IP (não roteáveis publicamente) privados especificados na RFC 1918.
- É possível que o sistema foi configurado com um endereço IP estático. Tente criar uma interface de rede e anexá-la à instância.
- Para habilitar o DHCP em uma instância do Windows à qual você não pode se conectar

  1. Interrompa a instância afeta e desanexe seu volume raiz.
  2. Execute uma instância temporária na mesma zona de disponibilidade que a instância afetada.

     > **Warning**
     >
     > Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usa a AMI AWS do Windows para Windows Server 2016, inicie a instância temporária usando a AMI AWS do Windows para Windows Server 2019.

  3. Anexe o volume raiz da instância afetada a essa instância temporária. Conecte-se à instância temporária, abra o utilitário Disk Management e ative a unidade.
  4. Na instância temporária, abra o Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SYSTEM` e especifique um nome de chave quando solicitado (você pode usar qualquer nome).
  5. Selecione a chave que você acabou de carregar e vá até `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Cada interface de rede é listada por um GUID. Selecione a interface de rede correta. Se o DHCP estiver desabilitado e um endereço IP

estático for atribuído, `EnableDHCP` será definido como 0. Para habilitar o DHCP, defina `EnableDHCP` como 1 e exclua as seguintes chaves se existirem: `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.

> **Note**
>
> Se você possuir várias interfaces de rede, precisará identificar a interface correta para habilitar o DHCP. Para identificar a interface de rede correta, reveja os seguintes valores de chave `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Esses valores exibem a configuração estática da instância anterior.

6. (Opcional) Se o DHCP já estiver ativado, é possível que você não tenha uma rota para o serviço de metadados. Atualizar o EC2Config pode resolver esse problema.

   a. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.

   b. Extraia arquivos do arquivo `.zip` para o diretório `Temp` na unidade que você associou.

   c. Abra Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SOFTWARE` e especifique um nome de chave quando solicitado (você pode usar qualquer nome).

   d. Selecione a chave que você acabou de carregar e vá até `Microsoft\Windows\CurrentVersion`. Selecione a chave `RunOnce`. (Se essa chave não existir, clique com o botão direito do mouse em `CurrentVersion`, aponte para Novo, selecione Chave e nomeie a chave `RunOnce`.) Clique com o botão direito do mouse, aponte para Novo e selecione Valor de string. Insira `Ec2Install` como o nome e `C:\Temp\Ec2Install.exe -q` como dados.

   e. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.

7. (Opcional) Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas a seguir ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco.

> **Warning**
>
> O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou

como fazer alterações com segurança usando o Editor do Registro, consulteConfigure the Registry (Configurar o Registro).

a. Abra um prompt de comando, digite regedit.exe e pressione Enter.

b. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.

c. Digite Windows Boot Manager e escolha Localizar Próxima.

d. Escolha a chave chamada `11000001`. Essa chave é irmã da chave que você localizou na etapa anterior.

e. No painel direito, selecione `Element` e escolha Modificar no menu de contexto (clique com o botão direito do mouse).

f. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

```
diskpart
```

h. Execute o comando DiskPart a seguir para selecionar o volume. (É possível verificar se o número do disco é 1 usando o utilitário Gerenciamento de disco.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART>  uniqueid disk
```

```
Disk ID: 0C764FA8
```

j. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco do BCD que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Usando o utilitário Disk Management, desative o volume da unidade.

> **Note**
>
> A unidade ficará offline automaticamente se a instância temporária estiver executando o mesmo sistema operacional que a instância afetada, portanto, você não precisará deixá-la offline manualmente.

9. Desanexe o volume da instância temporária. Você pode encerrar a instância temporária se você não tiver utilização adicional para ela.
10. Restaure o volume raiz da instância afetada anexando o volume como `/dev/sda1`.
11. Inicie a instância afetada.

Se você estiver conectado à instância, abra um navegador de Internet na instância e insira a seguinte URL do servidor de metadados:

```
http://169.254.169.254/latest/meta-data/
```

Se você não conseguir entrar em contato com o servidor de metadados, tente o seguinte para resolver o problema:

- Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.
- Verifique se a instância do Windows está executando drivers PV de RedHat. Em caso afirmativo, atualize os drivers PV. Para ter mais informações, consulte the section called “Atualizar drivers de PV”.
- Verifique se o firewall, o IPSec e as configurações de servidor não bloquearem o tráfego de saída para o serviço de metadados (`169.254.169.254`) ou os servidores de AWS KMS (os endereços

são especificados nos elementos do `TargetKMSServer` em `C:\Program Files\Amazon \Ec2ConfigService\Settings\ActivationSettings.xml`).

- Verifique se você tem uma rota para o serviço de metadados (`169.254.169.254`) usando o seguinte comando.

```
route print
```

- Verifique se há problemas de rede que podem afetar a zona de disponibilidade para sua instância. Acesse http://status.aws.amazon.com/.

"Não é possível ativar o Windows"

As instâncias do Windows usam a ativação do AWS KMS no Windows. Você pode receber esta mensagem: `A problem occurred when Windows tried to activate. Error Code 0xC004F074`, se sua instância não conseguir acessar o servidor de AWS KMS. O Windows deve ser ativado a cada 180 dias. O EC2Config tenta entrar em contato com o servidor de AWS KMS antes que o período de ativação expire para garantir que o Windows permaneça ativado.

Se você detectar um problema de ativação do Windows, execute o procedimento a seguir para resolver o problema.

Para EC2Config (AMIs do Windows Server 2012 R2 e anteriores)

1. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.
2. Faça login na instância e abra o seguinte arquivo: `C:\Program Files\Amazon \Ec2ConfigService\Settings\config.xml`.
3. Localize o plugin Ec2WindowsActivate no arquivo `config.xml`. Altere o estado para Habilitado e salve suas alterações.
4. No snap-in Windows Services, reinicie o serviço EC2Config ou reinicialize a instância.

Se isso não resolver o problema de ativação, siga estas etapas adicionais.

1. Defina o AWS KMS de destino: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Ative o Windows: C:\> slmgr.vbs /ato

Para EC2Launch (AMIs do Windows Server 2016 e posteriores)

1. De um prompt do PowerShell com direitos administrativos, importe o módulo do EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Chame a função Add-Routes para ver a lista de novas rotas:

```
PS C:\> Add-Routes
```

3. Chamar a função Set-ActivationSettings:

```
PS C:\> Set-Activationsettings
```

4. Em seguida, execute o seguinte script para ativar o Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Tanto para EC2Config como para EC2Launch, se você ainda estiver recebendo um erro de ativação, verifique as informações a seguir.

- Verifique se você tem rotas para os servidores de AWS KMS. Abra `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` e localize os elementos `TargetKMSServer`. Execute o comando a seguir e verifique se os endereços para esses servidores de AWS KMS estão listados.

```
route print
```

- Verifique se a chave do cliente de AWS KMS está definida. Execute o seguinte comando e verifique a saída.

```
C:\Windows\System32\slmgr.vbs /dlv
```

  Se o resultado contiver o erro Error: product key not found (Erro: chave de produto não encontrada), a chave de cliente do AWS KMS não estará definida. Se a chave de cliente do AWS KMS não estiver definida, procure pela chave de cliente conforme descrito neste artigo da Microsoft: AWS KMSClient Setup Keys (Chaves de configuração de cliente) e execute o comando a seguir para definir a chave de cliente do AWS KMS.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Verifique se o sistema tem a hora e o fuso horário corretos. Se você estiver usando um fuso horário diferente do UTC, adicione a seguinte chave de registro e configure-a 1 para garantir que a hora esteja correta: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Se o Firewall do Windows estiver habilitado, desabilite-o temporariamente usando o seguinte comando.

```
netsh advfirewall set allprofiles state off
```

"O Windows não é genuíno (0x80070005)"

As instâncias do Windows usam a ativação do AWS KMS no Windows. Se uma instância não conseguir concluir o processo de ativação, ela relatará que a cópia do Windows não é genuína.

Tente as sugestões para "Não é possível ativar o Windows".

"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"

Por padrão, o Windows Server é licenciado para dois usuários simultâneos por meio do Remote Desktop. Se você precisar fornecer a mais de dois usuários acesso simultâneo à sua instância do Windows por meio do Remote Desktop, compre uma licença de acesso de cliente (CAL) do Remote Desktop Services e instale as funções Remote Desktop Session Host e Remote Desktop Licensing Server.

Verifique se há os seguintes problemas:

- Você excedeu o número máximo de sessões simultâneos de RDP.
- Você instalou a função Windows Remote Desktop Services.
- O licenciamento expirou. Se o licenciamento expirou, você não poderá se conectar à sua instância do Windows como um usuário. Você pode tentar o seguinte:
  - Conecte-se à instância da linha de comando usando um parâmetro `/admin`, por exemplo:

```
mstsc /v:instance /admin
```

Para obter mais informações, consulte o seguinte artigo da Microsoft: Acessar a área de trabalho remota por meio da linha de comando.

- Interrompa a instância, desanexe seus volumes do Amazon EBS e anexe-os a outra instância na mesma zona de disponibilidade para recuperar os dados.

“Algumas configurações são gerenciadas pela sua organização”

As instâncias executadas a partir das AMIs mais recentes do Windows Server podem exibir uma mensagem do Windows Update informando “Algumas configurações são gerenciadas por sua organização”. Essa mensagem aparece como resultado de alterações no Windows Server e não afeta o comportamento do Windows Update nem sua capacidade de gerenciar as configurações de atualização.

Como remover o aviso

1. Abra `gpedit.msc` e navegue até Configuração do Computador, Modelos Administrativos, Componentes do Windows, Atualizações do Windows. Edite Configurar a atualização automática e defina-a como habilitada.
2. Em um prompt de comando, atualize a política de grupo usando gpupdate /force.
3. Feche e reabra as configurações do Windows Update. Você verá a mensagem acima sobre as configurações serem gerenciadas por sua organização, seguida por "Baixaremos automaticamente as atualizações, exceto em conexões limitadas (em que taxas podem ser cobradas). Nesse caso, faremos automaticamente download dessas atualizações necessárias para manter o Windows funcionando sem problemas.
4. Retorne para `gpedit.msc` e defina a política de grupo como não configurada. Execute gpupdate /force novamente.
5. Feche o prompt de comando e aguarde alguns minutos.
6. Reabra as configurações do Windows Update. Você não deve ver a mensagem “Algumas configurações são gerenciadas pela sua organização”

Solucionar problemas de execução de instâncias

Os problemas a seguir impedem que você execute uma instância.

Problemas de execução

- Nome de dispositivo inválido
- Limite de instâncias excedido
- Capacidade insuficiente da instância
- A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis.
- A instância é encerrada imediatamente
- Permissões insuficientes
- Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows)

Nome de dispositivo inválido

Descrição

Você obtém o erro `Invalid device name` *`device_name`* ao tentar iniciar uma nova instância.

Causa

Se você receber esse erro ao tentar executar uma instância, o nome do dispositivo especificado para um ou mais volumes da solicitação terá um nome de dispositivo inválido. As possíveis causas incluem:

- O nome do dispositivo pode estar em uso pela AMI selecionada.
- O nome do dispositivo pode estar reservado para volumes raiz.
- O nome do dispositivo pode estar sendo usado para outro volume da solicitação.
- O nome do dispositivo pode não ser válido para o sistema operacional.

Solução

Como resolver o problema:

- Verifique se o nome do dispositivo não está sendo usado na AMI que você selecionou. Execute o comando a seguir para visualizar os nomes de dispositivo usados pela AMI.

```
aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Verifique se não está usando um nome de dispositivo reservado para volumes raiz. Para ter mais informações, consulte Nomes de dispositivos disponíveis.
- Verifique se cada volume especificado em sua solicitação tem um nome de dispositivo exclusivo.
- Verifique se os nomes de dispositivo especificados estão no formato correto. Para ter mais informações, consulte Nomes de dispositivos disponíveis.

Limite de instâncias excedido

Descrição

Você obtém o erro `InstanceLimitExceeded` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Causa

Se obtiver um erro `InstanceLimitExceeded` ao tentar executar uma nova instância ou reiniciar uma instância interrompida, isso significa que atingiu o limite do número de instâncias que você pode executar em uma região. Ao criar uma conta da AWS, definimos limites padrão para o número de instâncias que você pode executar por região.

Solução

Você pode solicitar um aumento de limite de instâncias por região. Para obter mais informações, consulte Service Quotas do Amazon EC2.

Capacidade insuficiente da instância

Descrição

Você obtém o erro `InsufficientInstanceCapacity` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Causa

Se você receber esse erro ao tentar executar uma instância ou reiniciar uma instância interrompida, isso significa que, no momento, a AWS não tem capacidade sob demanda suficiente para atender à sua solicitação.

Solução

Para resolver esse problema, experimente o seguinte:

- Espere alguns minutos e envie uma solicitação novamente; a capacidade pode mudar com frequência.
- Envie uma solicitação nova com um número de instâncias reduzido. Por exemplo, se você estiver fazendo uma única solicitação para executar 15 instâncias, tente fazer 3 solicitações para 5 instâncias, ou 15 solicitações de 1 instância.
- Se você estiver executando uma instância, envie uma nova solicitação sem especificar uma zona de disponibilidade.
- Se você estiver executando uma instância, envie uma solicitação nova usando um tipo de instância diferente (que você pode redimensionar posteriormente). Para obter mais informações, consulte Alterar o tipo de instância.
- Se você estiver executando instâncias em um placement group de cluster, é possível obter um erro de capacidade insuficiente. Para obter mais informações, consulte Trabalho com grupos de posicionamento.

A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis.

Descrição

Você obtém o erro `Unsupported` ao tentar executar uma nova instância porque a configuração da instância não é compatível.

Causa

A mensagem de erro fornece detalhes adicionais. Por exemplo, é possível que um tipo de instância ou opção de compra de instância não seja compatível com a região ou Zona de Disponibilidade especificada.

Solução

Tente uma configuração de instância diferente. Para pesquisar um tipo de instância que atenda aos seus requisitos, consulte Localizar um tipo de instância do Amazon EC2.

A instância é encerrada imediatamente

Descrição

Sua instância passa do estado `pending` para o estado `terminated`.

Causa

A seguir estão alguns motivos pelos quais a instância pode ser imediatamente encerrada:

- Você excedeu os limites de volume do EBS. Para obter mais informações, consulte Limites de volumes de instância.
- Um snapshot do EBS está corrompido.
- O volume raiz do EBS está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia.
- Um snapshot especificado no mapeamento de dispositivo de blocos para a AMI está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia ou não tem acesso à Chave do KMS para criptografar os volumes restaurados.
- A AMI com armazenamento de instâncias que você usou para executar a instância não tem um item necessário (um arquivo image.part.xx).

Para obter mais informações, saiba o motivo do encerramento usando um dos métodos a seguir.

Para obter o motivo do encerramento usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Na primeira guia, encontre o motivo ao lado de State transition reason (Motivo de transição de estado).

Para obter o motivo do encerramento usando a AWS Command Line Interface

1. Use o comando describe-instances e especifique o ID da instância.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Revise a resposta JSON retornada pelo comando e observe os valores no elemento de resposta `StateReason`.

O bloco de código a seguir mostra um exemplo de elemento de resposta `StateReason`:

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Como saber o motivo do encerramento usando a AWS CloudTrail

Para obter mais informações, consulte o tópico sobre como Visualizar eventos com o histórico de eventos do CloudTrail, no Guia do usuário do AWS CloudTrail.

Solução

Dependendo do motivo do encerramento, execute uma das seguintes ações:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — exclua volumes não utilizados. É possível enviar uma solicitação para aumentar seu limite de volume.
- **`Client.InternalError: Client error on launch`**: verifique se você tem as permissões necessárias para acessar as AWS KMS keys usadas para descriptografar e criptografar volumes. Para obter mais informações, consulte Uso de políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Permissões insuficientes

Descrição

Você recebe o erro `"errorMessage": "You are not authorized to perform this operation."` ao tentar iniciar uma nova instância e não é possível iniciá-la.

Causa

Se você receber esse erro ao tentar iniciar uma instância, você não tem as permissões do IAM necessárias para iniciá-la.

As possíveis permissões ausentes incluem:

- `ec2:RunInstances`

- `iam:PassRole`

Outras permissões também podem estar faltando. Para ver a lista de permissões necessárias para iniciar uma instância, consulte o exemplo de políticas do IAM em Exemplo: uso do assistente de início de instância do EC2 e Executar instâncias (RunInstances).

Solução

Como resolver o problema:

- Se você estiver fazendo solicitações como um usuário IAM, verifique se tem as seguintes permissões:
  - `ec2:RunInstances` com um caractere curinga ("*")
  - `iam:PassRole` com o recurso correspondente ao nome de região da Amazon (ARN) da função (por exemplo, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Se você não tiver as permissões anteriores, edite a política do IAM associada ao perfil ou usuário do IAM para adicionar as permissões necessárias que estão faltando.

Se o problema não for resolvido e um erro de falha na inicialização continuar sendo recebido, você poderá decodificar a mensagem de falha de autorização incluída no erro. A mensagem decodificada inclui as permissões que estão faltando na política do IAM. Para obter mais informações, consulte Como posso decodificar uma mensagem de falha de autorização depois de receber um erro de "UnauthorizedOperation" durante a execução de uma instância do EC2?

Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows)

> **Note**
>
> Esta dica de solução de problemas é dedicada somente para instâncias do Windows.

Se o Windows Update for definido como Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las (a configuração de instância padrão), essa verificação poderá consumir entre 50 e 99% da CPU na instância. Se esse consumo de CPU causar problemas para seus aplicativos, você poderá alterar manualmente as configurações do Windows Update no Painel de controle ou usar o seguinte script no campo de dados de usuário do Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Quando você executar esse script, especifique um valor para /d. O valor padrão é 3. Os valores possíveis incluem o seguinte:

1. Nunca verificar se há atualizações
2. Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las
3. Fazer download de atualizações, mas permitir que eu escolha fazer download e instalá-las
4. Instalar atualizações automaticamente

Depois de modificar os dados do usuário para sua instância, você poderá executá-la. Para obter mais informações, consulte Run commands on your Windows instance at launch.

Solução de problemas de conexão com a instância do Linux

As informações e os erros comuns a seguir podem ajudar você a solucionar problemas de conexão com a instância Linux.

Problemas de conectividade

- Causas comuns de problemas de conexão
- Erro ao se conectar à sua instância: limite de tempo da conexão atingido
- Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA
- Erro: Chave do usuário não reconhecida pelo servidor
- Erro: permissão negada ou conexão fechada pela porta 22 de [instância]
- Erro: arquivo de chave privada desprotegido
- Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----"
- Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis
- Não é possível fazer o ping da instância
- Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor)
- Erro: falha na validação da chave do host para EC2 Instance Connect

- Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect
- Perdi minha chave privada. Como posso me conectar à minha instância do Linux?

Causas comuns de problemas de conexão

Recomendamos que você comece a solucionar problemas de conexão de instâncias verificando se realizou com precisão as tarefas a seguir.

Verificar o nome de usuário da instância

É possível se conectar à instância usando o nome de usuário da conta de usuário ou o nome de usuário padrão da AMI que você usou para iniciar a instância.

- Obtenha o nome de usuário da sua conta de usuário.

  Para obter mais informações sobre como criar uma conta de usuário, consulte Gerenciamento de usuários do sistema na instância do Linux.
- Obtenha o nome de usuário padrão da AMI usada para iniciar a instância:

A AMI usada para iniciar a instância	Nome de usuário padrão
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`

A AMI usada para iniciar a instância	Nome de usuário padrão
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

Verificar se as regras do grupo de segurança permitem tráfego

Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de execução de instância permite o tráfego SSH de entrada por padrão. Para ver as etapas para adicionar uma regra para o tráfego SSH de entrada à sua instância do Linux, consulte Regras para se conectar a instâncias pelo computador. Para obter as etapas de verificação, consulte Erro ao se conectar à sua instância: limite de tempo da conexão atingido.

Verificar se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique a instância para se certificar de que ela está sendo executada e passou em suas verificações de status.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Verifique o seguinte:

    a. Na coluna Instance state (Estado da instância), verifique se sua instância está no estado `running`.
    b. Na coluna Status check (Verificação de status), verifique se sua instância passou nas duas verificações de status.

Verifique se você atendeu a todos os pré-requisitos para se conectar

Certifique-se de ter todas as informações necessárias para se conectar. Para ter mais informações, consulte Conecte-se à sua instância do Linux.

Para obter os pré-requisitos específicos para os tipos de conexão, como SSH, EC2 Instance Connect, OpenSSH, PuTTY e muito mais, consulte as opções a seguir.

Linux ou macOS X

Se o sistema operacional do computador local for Linux ou macOS X, verifique os pré-requisitos específicos das seguintes opções de conexão:

- Cliente SSH
- EC2 Instance Connect
- Gerenciador de sessões do AWS Systems Manager

Windows

Se o sistema operacional do computador local for Windows, verifique os pré-requisitos específicos das seguintes opções de conexão:

- OpenSSH
- PuTTY
- Gerenciador de sessões do AWS Systems Manager
- Subsistema Windows para Linux

Erro ao se conectar à sua instância: limite de tempo da conexão atingido

Se você tentar se conectar à sua instância e receber uma mensagem de erro `Network error: Connection timed out` ou `Error connecting to [instance], reason: -> Connection timed out: connect`, experimente o seguinte:

Verifique as regras do seu security group.

Você precisa de uma regra de grupo de segurança que permita tráfego de entrada proveniente do endereço IPv4 público do seu computador local na porta adequada.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Security (Segurança) na parte inferior da página do console, em Inbound rules (Regras de entrada), verifique a lista de regras que estão em vigor para a instância selecionada.

   - Para instâncias do Linux: verifique se há uma regra para permitir tráfego do seu computador local para a porta 22 (SSH).
   - Para instâncias do Windows: verifique se há uma regra para permitir tráfego do seu computador local para a porta 3389 (RDP).

Se seu grupo de segurança não tiver uma regra que permita tráfego de entrada proveniente do seu computador local, adicione uma regra para seu grupo de segurança. Para ter mais informações, consulte Regras para se conectar a instâncias pelo computador.

4. Para a regra que permite tráfego de entrada, verifique o campo Source (Origem). Se o valor for um só endereço IP e se o endereço IP não for estático, um novo endereço IP será atribuído sempre que você reiniciar o computador. Isso fará com que a regra não inclua o tráfego de endereço IP do seu computador. Talvez o endereço IP não seja estático se seu computador estiver em uma rede corporativa, se você estiver se conectando por um provedor de serviços de Internet (ISP), ou se seu endereço IP do computador for dinâmico e mudar sempre que você reiniciar o computador. Para garantir que a regra do grupo de segurança permita o tráfego de entrada do computador local, em vez de especificar um único endereço IP para Source (Origem), em vez disso, especifique o intervalo de endereços IP usado por seus computadores cliente.

   Para obter mais informações sobre regras de grupos de segurança, consulte Regras de grupos de segurança no Guia do usuário da Amazon VPC.

Verifique a tabela de rotas para a sub-rede.

Você precisa de uma rota que envie todo o tráfego que sai da VPC para o gateway da Internet da VPC.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Networking (Redes), anote os valores para VPC ID (ID da VPC) e Subnet ID (ID de sub-rede).
4. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
5. No painel de navegação, escolha Gateways da Internet. Verifique se há um gateway de internet associado à sua VPC. Caso contrário, escolha Create internet gateway (Criar gateway da Internet), insira um nome para o gateway da Internet e escolha Create internet gateway (Criar gateway da Internet). Em seguida, para o gateway da internet criado, escolha Actions (Ações), Attach to VPC (Anexar à VPC), selecione sua VPC e, em seguida, escolha Attach internet gateway (Anexar gateway da internet)para anexá-lo à sua VPC.
6. No painel de navegação, selecione Sub-redes e selecione sua sub-rede.

7. Na guia Route tabl (Tabela de rotas), verifique se há uma rota com `0.0.0.0/0` como destino e o gateway da Internet para sua VPC como alvo. Se você estiver se conectando à sua instância usando o endereço IPv6, verifique se há uma rota para todo o tráfego IPv6 (`::/0`) que aponta para o gateway de Internet. Caso contrário, faça o seguinte:

   a. Escolha o ID da tabela de rotas (rtb-xxxxxxxx) para navegar para a tabela de rotas.

   b. Na guia Routes (Rotas), escolha Edit routes (Editar rotas). Escolha Add route (Adicionar rota), use `0.0.0.0/0` como o destino, e o gateway da Internet como o destino. Para IPv6, escolha Add route (Adicionar rota), use `::/0` como o destino, e o gateway da Internet como o destino.

   c. Escolha Save routes (Salvar rotas).

Verifique a lista de controle de acesso (ACL) da rede para a sub-rede.

As ACLs da rede devem permitir tráfego de entrada do seu endereço IP local na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows). Também deve permitir tráfego de saída para as portas efêmeras (1024-65535).

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Na guia Network ACL (ACL da rede), em Inbound rules,(Regras de entrada), verifique se as regras permitem tráfego de entrada na porta obrigatória de seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.
5. Em Outbound rules (Regras de saída), verifique se as regras permitem tráfego nas portas efêmeras para seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.

Caso seu computador esteja em uma rede corporativa

Pergunte ao administrador da rede se o firewall interno permite tráfego de entrada e saída do seu computador na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows).

Se você tiver um firewall no seu computador, verifique se ele permite tráfego de entrada e de saída do seu computador na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows).

Verifique se sua instância tem um endereço IPv4 público.

Se não tiver, associe um endereço IP elástico à sua instância. Para ter mais informações, consulte Endereços IP elásticos.

Verifique a carga de CPU na sua instância; o servidor pode estar sobrecarregado.

A AWS fornece automaticamente dados, como status de métricas e instâncias de Amazon CloudWatch, que é possível usar para ver quanta carga de CPU está na sua instância e, caso necessário, ajusta como suas cargas são manuseadas. Para ter mais informações, consulte Monitorar instâncias usando o CloudWatch.

- Se sua carga for variável, será possível expandir ou reduzir automaticamente suas instâncias usando o Auto Scaling e o Elastic Load Balancing.
- Se sua carga estiver crescendo constantemente, é possível mudá-la para um tipo de instância maior. Para ter mais informações, consulte Alterar o tipo de instância.

Para conectar-se à sua instância usando um endereço IPv6, verifique o seguinte:

- Sua sub-rede deve estar associada a uma tabela de rotas que tenha uma rota para tráfego IPv6 (`::/0`) para um gateway de Internet.
- As regras do security group devem permitir tráfego de entrada do seu endereço IPv6 local na porta apropriada (22 para Linux e 3389 para Windows).
- As regras de Network ACL devem permitir tráfego de IPv6 de entrada e saída.
- Se você executou a instância de uma AMI mais antiga, ela pode não estar configurada para DHCPv6 (endereços IPv6 não são automaticamente reconhecidos na interface de rede). Para obter mais informações, consulte Configurar o IPv6 em suas instâncias no Guia do usuário da Amazon VPC.
- Seu computador local deve ter um endereço IPv6 e ser configurado para usar IPv6.

Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA

Se você tentar se conectar à sua instância e obter a mensagem de erro `unable to load key ... Expecting: ANY PRIVATE KEY`, o arquivo no qual a chave privada está armazenada foi configurado incorretamente. Se o arquivo da chave privada terminar em `.pem`, ele ainda

poderá estar configurado incorretamente. Uma possível causa para um arquivo da chave privada configurado incorretamente é a ausência de um certificado.

Se o arquivo da chave privada estiver configurado incorretamente, siga estas etapas para solucionar o erro:

1. Crie um novo par de chaves. Para ter mais informações, consulte Criar um par de chaves usando o Amazon EC2.

   > **Note**
   >
   > Como alternativa, é possível criar um novo par de chaves usando uma ferramenta de terceiros. Para ter mais informações, consulte Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.

2. Adicione o novo par de chaves à sua instância. Para ter mais informações, consulte Perdi minha chave privada. Como posso me conectar à minha instância do Linux?.
3. Conecte-se à instância usando o novo par de chaves.

Erro: Chave do usuário não reconhecida pelo servidor

Se você usar o SSH para conectar à sua instância

- Use `ssh -vvv` para obter o triplo de informações de depuração detalhadas (verbose) ao se conectar:

  ```
  ssh -vvv -i path/key-pair-name.pem instance-user-
  name@ec2-203-0-113-25.compute-1.amazonaws.com
  ```

  O exemplo de saída a seguir demonstra o que é possível ver se estivesse tentando se conectar à sua instância com uma chave não reconhecida pelo servidor:

  ```
  open/ANT/myusername/.ssh/known_hosts).
  debug2: bits set: 504/1024
  debug1: ssh_rsa_verify: signature correct
  debug2: kex_derive_keys
  debug2: set_newkeys: mode 1
  debug1: SSH2_MSG_NEWKEYS sent
  debug1: expecting SSH2_MSG_NEWKEYS
  ```

```
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Se você usar o PuTTY para se conectar à instância

- Verifique se o arquivo de chave privada (.pem) foi convertido para o formato reconhecido pelo PuTTY (.ppk). Para obter mais informações sobre a conversão da sua chave privada, consulte Conectar à instância do Linux a partir do Windows usando PuTTY.

  > **Note**
  >
  > No PuTTYgen, carregue o arquivo de chave privada e selecione Salvar chave privada em vez de Gerar.

- Verifique se você está se conectando com o nome de usuário adequado para sua AMI. Insira o nome de usuário na caixa Nome do host na janela Configuração do PuTTY.

A AMI usada para iniciar a instância	Nome de usuário padrão
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

- Verifique se você tem uma regra do security group de entrada para permitir tráfego de entrada para a porta apropriada. Para ter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Erro: permissão negada ou conexão fechada pela porta 22 de [instância]

Se você se conectar à instância usando SSH e obtiver algum dos erros a seguir, `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied`, ou `Connection closed by [instance] port 22`, verifique se está se conectando com o nome de usuário apropriado para a AMI e se especificou o arquivo de chave privada (arquivo `.pem`) apropriado para a instância).

Os nomes de usuários apropriados são os seguintes:

A AMI usada para iniciar a instância	Nome de usuário padrão
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

Por exemplo, para usar um cliente SSH para se conectar a uma instância do Amazon Linux, use o seguinte comando:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirme se você está usando um arquivo de chave privada que corresponde ao par de chaves que selecionou ao executar a instância.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Instances (Instâncias) e, em seguida, selecione sua instância.
3. Na guia Details (Detalhes), em Instance details (Detalhes da instância), verifique o valor do Nome do par de chaves.
4. Se você não tiver especificado um par de chaves ao executar a instância, pode encerrar a instância e executar uma nova, especificando um par de chaves. Se essa for uma instância que você está usando mas não tiver mais o arquivo `.pem` para seu par de chaves, pode substituir o par de chaves por um novo. Para ter mais informações, consulte Perdi minha chave privada. Como posso me conectar à minha instância do Linux?.

Se você tiver gerado seu próprio par de chaves, garanta que o gerador de chaves está configurado para criar chaves RSA. Chaves DSA não são aceitas.

Se você obtiver um erro `Permission denied (publickey)` e nenhum dos casos acima se aplicar (por exemplo, você conseguiu se conectar previamente), as permissões no diretório inicial da sua instância podem ter sido alteradas. As permissões para /home/*instance-user-name*/.ssh/authorized_keys devem ser limitadas somente ao proprietário.

Para verificar as permissões na sua instância

1. Pare sua instância e separe o volume do dispositivo raiz. Para ter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
2. Execute uma instância temporária na mesma zona de disponibilidade que sua instância atual (use uma AMI semelhante ou a mesma AMI usada para sua instância atual) e associe o volume do dispositivo raiz à instância temporária.
3. Conecte-se à instância temporária, crie um ponto de montagem e monte o volume associado.
4. Na instância temporária, verifique as permissões do diretório /home/*instance-user-name*/ do volume associado. Se necessário, ajuste as permissões da seguinte forma:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Desmonte o volume, separe-o da instância temporária e reassocie-o à instância original. Especifique o nome correto do dispositivo para o volume do dispositivo raiz; por exemplo, `/dev/xvda`.
6. Execute sua instância. Se você não precisar mais da instância temporária, pode encerrá-la.

Erro: arquivo de chave privada desprotegido

Seu arquivo de chave privada deve estar protegido contra operações de leitura e gravação por parte de qualquer outro usuário. Se sua chave privada puder ser lida ou gravada por qualquer pessoa menos você, o SSH ignorará sua chave e você verá a mensagem de advertência abaixo.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Se você vir uma mensagem semelhante ao tentar fazer login na sua instância, examine a primeira linha da mensagem de erro para verificar se está usando a chave pública correta para sua instância. O exemplo acima usa a chave privada `.ssh/my_private_key.pem` com permissões de arquivo `0777`, que permitem que qualquer pessoa leia ou grave nesse arquivo. O nível de permissão é muito inseguro, por isso o SSH ignora essa chave.

Se você está se conectando do macOS ou Linux, execute o comando a seguir para corrigir esse erro, substituindo o caminho para o arquivo de chave privada.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Se você estiver se conectando do Windows, execute as etapas a seguir no computador local.

1. Navegue até o arquivo .pem.
2. Clique com o botão direito do mouse no arquivo .pem e selecione Properties (Propriedades).
3. Escolha a guia Segurança.
4. Selecione Advanced (Avançado).

5. Verifique se você é o proprietário do arquivo. Caso contrário, altere o proprietário para seu nome de usuário.
6. Selecione Disable inheritance (Desabilitar herança) e Remove all inherited permissions from this object (Remover todas as permissões herdadas deste objeto).
7. Selecione Add (Adicionar), Select a principal (Selecionar um principal), insira seu nome de usuário e selecione OK.
8. Na janela Permission Entry (Entrada de permissão), conceda as permissões Read (Leitura) e selecione OK.
9. Clique em Apply (Aplicar) para garantir que todas as configurações sejam salvas.
10. Selecione OK para fechar a janela Advanced Security Settings (Configurações avançadas de segurança).
11. Selecione OK para fechar a janela Properties (Propriedades).
12. É necessário ser capaz de se conectar à instância Linux no Windows por meio de SSH.

No prompt de comando do Windows, execute os comandos a seguir.

1. No prompt de comando, navegue até o local do caminho do arquivo .pem.
2. Execute o seguinte comando para redefinir e remover permissões explícitas:

```
icacls.exe $path /reset
```

3. Execute o seguinte comando para conceder permissões de leitura ao usuário atual:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Execute o seguinte comando para desabilitar a herança e remover permissões herdadas.

```
icacls.exe $path /inheritance:r
```

5. É necessário ser capaz de se conectar à instância Linux no Windows por meio de SSH.

Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----"

Se usar uma ferramenta de terceiros, como ssh-keygen, para criar um par de chaves RSA, ela gerará a chave privada no formato de chave OpenSSH. Quando você se conecta à sua instância, se

você usar a chave privada no formato OpenSSH para descriptografar a senha, você receberá o erro `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Para resolver o erro, a chave privada deve estar no formato PEM. Use o comando a seguir para criar a chave privada no formato PEM:

```
ssh-keygen -m PEM
```

Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis

Se você usar o PuTTY para se conectar à instância e obtiver algum dos erros a seguir, Erro: o servidor recusou nossa chave ou Erro: não há métodos de autenticação compatíveis, verifique se está se conectando com o nome de usuário apropriado para a AMI. Digite o nome de usuário em Nome do usuário na janela Configuração do PuTTY.

Os nomes de usuários apropriados são os seguintes:

A AMI usada para iniciar a instância	Nome de usuário padrão
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`

A AMI usada para iniciar a instância	Nome de usuário padrão
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

Você também deve verificar:

- Se está usando a versão mais recente do PuTTY. Para obter mais informações, consulte a página do PuTTY.
- Se o arquivo de chave privada (.pem) foi convertido corretamente para o formato reconhecido pelo PuTTY (.ppk). Para obter mais informações sobre a conversão da sua chave privada, consulte Conectar à instância do Linux a partir do Windows usando PuTTY.

Não é possível fazer o ping da instância

O comando `ping` é um tipo de tráfego de ICMP — se você não conseguir fazer o ping da sua instância, verifique se as regras do grupo de segurança de entrada permitem tráfego de ICMP para a mensagem `Echo Request` de todas as origens, ou do computador ou da instância em que você está emitindo o comando.

Caso você não consiga emitir um comando `ping` por sua instância, assegure-se de que suas regras do security group de saída permitam tráfego de ICMP para a mensagem `Echo Request` a todos os destinos ou para o host no qual você está tentando fazer o ping.

Os comandos `Ping` também podem ser bloqueados por um firewall ou tempo de espera devido a problemas de latência de rede ou hardware. É necessário consultar o administrador de sistema ou de rede local para obter ajuda com mais solução de problemas.

Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor)

Se você estiver se conectando à instância com o PuTTY e receber o erro "A conexão de rede foi fechada inesperadamente pelo servidor", verifique se os keepalives estão habilitados na página Conexão da Configuração do PuTTY para evitar ser desconectado. Alguns servidores desconectam

clientes quando eles não recebem nenhum dado em determinado período. Defina os segundos entre os keepalives para 59 segundos.

Se você ainda tiver problemas após habilitar os keepalives, tente desabilitar o algoritmo de Nagle na página Conexão da Configuração do PuTTY.

Erro: falha na validação da chave do host para EC2 Instance Connect

Se você alternar as chaves do host da instância, as novas chaves do host não serão automaticamente carregadas para o banco de dados de chaves de host confiáveis da AWS. Isso faz com que a validação da chave do host apresente falha quando você tenta se conectar à instância usando o cliente EC2 Instance Connect baseado em navegador e você não consegue se conectar à instância.

Para resolver o erro, é necessário executar o script `eic_harvest_hostkeys` na instância, o que carregará sua nova chave de host para EC2 Instance Connect. O script está localizado em `/opt/aws/bin/` nas instâncias do Amazon Linux 2 e em `/usr/share/ec2-instance-connect/` nas instâncias do Ubuntu.

Amazon Linux 2

Para resolver o erro de falha de validação da chave de host em uma instância do Amazon Linux 2.

1. Conecte-se à sua instância usando SSH.

   Faça a conexão usando a CLI EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

   Por exemplo, se a instância tiver sido executada usando o Amazon Linux 2, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..
2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora é possível usar o cliente EC2 Instance Connect baseado em navegador para se conectar à instância.

Ubuntu

Para resolver o erro de falha de validação da chave de host em uma instância do Ubuntu

1. Conecte-se à sua instância usando SSH.

Faça a conexão usando a CLI EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para Ubuntu, o nome de usuário padrão é `ubuntu`.

Por exemplo, se a instância tiver sido executada usando o Ubuntu, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o nome do par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte Conectar à sua instância do Linux a partir do Linux ou MacOS usando SSH..

2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora é possível usar o cliente EC2 Instance Connect baseado em navegador para se conectar à instância.

Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect

Se você usar o EC2 Instance Connect para se conectar à sua instância do Ubuntu e receber um erro ao tentar se conectar, poderá usar as informações a seguir para tentar corrigir o problema.

Possível causa

O pacote `ec2-instance-connect` na instância não é a versão mais recente.

Solução

Atualize o pacote `ec2-instance-connect` na instância para a versão mais recente, desta forma:

1. Conecte-se à sua instância usando um método diferente do EC2 Instance Connect.
2. Execute o comando a seguir em sua instância para atualizar o pacote `ec2-instance-connect` para a versão mais recente.

```
apt update && apt upgrade
```

Perdi minha chave privada. Como posso me conectar à minha instância do Linux?

Se você perder a chave privada de uma instância com EBS, poderá recobrar o acesso à sua instância. É necessário parar a instância, separar seu volume raiz e associá-lo a outra instância como um volume de dados, modificar o arquivo `authorized_keys` com uma nova chave pública, mover o volume de volta para a instância original e reiniciar a instância. Para obter mais informações sobre executar, conectar e parar instâncias, consulte Ciclo de vida da instância.

Este procedimento é compatível apenas com instâncias com volumes raiz do EBS. Se o dispositivo raiz for um volume de armazenamento de instâncias, você não poderá usar esse procedimento

para recuperar o acesso à instância. É necessário ter a chave privada para se conectar à instância. Para determinar o tipo de dispositivo raiz da instância, abra o console do Amazon EC2, escolha Instâncias, selecione a instância, escolha a guia Armazenamento e, na seção Detalhes do dispositivo raiz, verifique o valor de Tipo de dispositivo raiz.

O valor é `EBS` ou `INSTANCE-STORE`.

Além das etapas a seguir, há outras formas de se conectar à instância do Linux em caso de perda da chave privada. Para obter mais informações, consulte Como posso me conectar à instância do Amazon EC2 se tiver perdido meu par de chaves SSH após o lançamento inicial?

Etapas para se conectar a uma instância com EBS com um par de chaves diferente

- Etapa 1: Criar um novo par de chaves
- Etapa 2: Obter informações sobre a instância original e seu volume raiz
- Etapa 3: Interromper a instância original
- Etapa 4: Executar uma instância temporária
- Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária
- Etapa 6: Adicionar a nova chave pública authorized_keys no volume original montado à instância temporária
- Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original
- Etapa 8: Conectar-se à instância original usando o novo par de chaves
- Etapa 9: Limpeza

Etapa 1: Criar um novo par de chaves

Crie um novo par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros. Se você quiser nomear seu novo par de chaves exatamente igual ao par de chaves privadas perdido, primeiro exclua o par de chaves existente. Para obter mais informações sobre como criar um par de chaves, consulte Criar um par de chaves usando o Amazon EC2 ou Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.

Etapa 2: Obter informações sobre a instância original e seu volume raiz

Anote as seguintes informações, porque elas serão necessárias para a conclusão deste procedimento.

Como obter informações sobre a instância original

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias no painel de navegação e selecione a instância à qual você deseja se conectar. (Nós a chamamos de instância original.)
3. Na guia Details (Detalhes) , anote o ID da instância e a ID da AMI.
4. Na guia Networking (Redes), anote a zona de disponibilidade.
5. Na guia Storage (Armazenamento), em Root device name (Nome do dispositivo raiz), anote o nome do dispositivo para o volume raiz (por exemplo, `/dev/xvda`). Em seguida, em Block devices (Dispositivos de bloco), encontre este nome do dispositivo e anote o ID do volume (por exemplo, vol-0a1234b5678c910de).

Etapa 3: Interromper a instância original

Escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Etapa 4: Executar uma instância temporária

New console

Para executar uma instância temporária

1. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
2. Na seção Name and tags (Nome e etiquetas), em Name (Nome), insira Temporary (Temporário).
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a mesma AMI usada para iniciar a instância original. Se essa AMI estiver indisponível, será possível

criar uma AMI que pode usar a partir da instância interrompida. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

4. Na seção Instance type (Tipo de instância), mantenha o tipo de instância padrão.
5. Na seção Key pair (Par de chaves), em Key pair name (Nome do par de chaves), selecione o par de chaves existente para usar ou crie um novo.
6. Na seção Network settings (Configurações de rede), selecione Edit (Editar), e, em seguida, em Subnet (Sub-rede), selecione uma sub-rede na mesma zona de disponibilidade que a instância original.
7. No painel Summary (Resumo) painel, escolha Launch (Iniciar).

Old console

Escolha Launch Instance (Executar instância) e use o assistente de execução para executar uma instância temporária com as seguintes opções:

- Na página Escolha uma AMI, selecione a mesma AMI usada para executar a instância original. Se essa AMI estiver indisponível, será possível criar uma AMI que pode usar a partir da instância interrompida. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
- Na página Escolher um tipo de instância, deixe o tipo de instância padrão que o assistente seleciona para você.
- Na página Configure Instance Details (Configurar detalhes da instância) especifique a mesma zona de disponibilidade que a instância original. Se você estiver executando uma instância em uma VPC, selecione uma sub-rede nesta zona de disponibilidade.
- Na página Adicionar tags, adicione a tag `Name=Temporary` à instância para indicar que isso é uma instância temporária.
- Na página Revisar, escolha Iniciar. Escolha o par de chaves criado na Etapa 1 e selecione Iniciar instâncias.

Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária

1. No painel de navegação, selecione Volumes e selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior). Escolha Actions (Ações),

Detach Volume (Desanexar volume) e Yes, Detach (Sim, desanexar). Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)

2. Com o volume ainda selecionado, escolha Actions (Ações) e, em seguida, Attach volume (Anexar volume). Selecione o ID de instância da instância temporária, anote o nome do dispositivo especificado em Device (Dispositivo) (por exemplo, `/dev/sdf`) e selecione Attach (Anexar).

> **Note**
>
> Se você tiver executado a instância original a partir de uma AMI de AWS Marketplace e seu volume contiver códigos de AWS Marketplace, você deverá primeiro parar a instância temporária antes de associar o volume.

Etapa 6: Adicionar a nova chave pública **`authorized_keys`** no volume original montado à instância temporária

1. Conecte-se à instância temporária.
2. Na instância temporária, monte o volume que você associou à instância de forma que possa acessar seu sistema de arquivos. Por exemplo, se o nome do dispositivo for `/dev/sdf`, use os comandos a seguir para montar o volume como `/mnt/tempvol`.

> **Note**
>
> O nome de dispositivo pode aparecer de forma diferente em sua instância. Por exemplo, dispositivos montados como `/dev/sdf` podem ser exibidos como `/dev/xvdf` na instância. Algumas versões do Red Hat (ou suas variantes, como o CentOS) podem até mesmo incrementar a letra final com 4 caracteres, em que `/dev/sd`*`f`* torna-se `/dev/xvd`*`k`*.

   a. Use o comando lsblk determinar se o volume é particionado.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
```

```
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

No exemplo acima, `/dev/xvda` e `/dev/xvdf` são volumes particionados, e `/dev/xvdg` não é. Se seu volume estiver particionado, você montará a partição (`/dev/xvdf1`) em vez do dispositivo raw (`/dev/xvdf`) nas próximas etapas.

b. Crie um diretório temporário para montar o volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Monte o volume (ou a partição) no ponto de montagem temporário usando o nome do volume ou do dispositivo identificado anteriormente. O comando necessário depende do sistema de arquivos do sistema operacional. Observe que o nome de dispositivo pode aparecer de forma diferente em sua instância. Consulte note na etapa 6 para obter mais informações.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se você receber um erro informando que o sistema de arquivos está corrompido, execute o seguinte comando para usar o utilitário fsck para verificar o sistema de arquivos e reparar quaisquer problemas:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Pela instância temporária, use o comando a seguir para atualizar `authorized_keys` no volume montado com a nova chave pública nova de `authorized_keys` para a instância temporária.

> **Important**
>
> Os exemplos a seguir usam o nome de usuário do Amazon Linux `ec2-user`. É possível precisar substituir um nome de usuário diferente, como `ubuntu` para instâncias Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se essa cópia tiver sido bem-sucedida, será possível passar para a próxima etapa.

(Opcional) Caso contrário, se você não tiver permissão para editar arquivos em `/mnt/tempvol`, será necessário atualizar o arquivo usando sudo e conferir as permissões no arquivo para verificar se é possível fazer login na instância original. Use o comando a seguir para verificar as permissões no arquivo:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Nesta saída de exemplo, *222* é o ID do usuário e *500* é o ID do grupo. Em seguida, use sudo para executar novamente o comando de cópia que falhou.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Execute o comando a seguir novamente para determinar se as permissões foram alteradas.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se o ID do usuário e do grupo tiverem sido alterados, use o comando a seguir para restaurá-los.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original

1. Na instância temporária, desmonte o volume que você associou para que possa reassociá-lo à instância original. Por exemplo, use o comando a seguir para desmontar o volume em `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Desanexe o volume da instância temporária (você o desmontou na etapa anterior): no console do Amazon EC2, selecione Volumes (Volumes) no painel de navegação, selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior), escolha Actions (Ações), Detach Volume (Desanexar volume) e, depois, Detach (Desanexar). Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)
3. Associe o volume novamente à instância original: com o volume ainda selecionado, escolha Actions (Ações), Attach Volume (Anexar volume). Selecione o ID de instância da instância original, especifique o nome do dispositivo anotado anteriormente na etapa 2 para o anexo do dispositivo raiz original (`/dev/sda1` ou `/dev/xvda`) e selecione Attach volume (Anexar volume).

   > **Important**
   >
   > Se você não especificar o mesmo nome do dispositivo do anexo original, não poderá iniciar a instância original. O Amazon EC2 espera que o volume raiz seja `sda1` ou `/dev/xvda`.

Etapa 8: Conectar-se à instância original usando o novo par de chaves

Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após a instância entrar no estado `running`, é possível se conectar a ela usando o arquivo de chave privada do seu novo par de chaves.

> **Note**
>
> Se o nome do novo par de chaves e do arquivo de chaves privadas correspondente for diferente do nome do par de chaves original, especifique o nome do novo arquivo de chave privada conectado à sua instância.

Etapa 9: Limpeza

(Opcional) É possível encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Solução de problemas para conexão à instância do Windows

As informações e os erros comuns apresentados a seguir podem ajudar você a solucionar problemas de conexão com a instância do Windows.

Problemas de conectividade

- O Remote Desktop não pode se conectar ao computador remoto
- Erro ao usar o cliente RDP do macOS
- O RDP exibe uma tela preta em vez da área de trabalho
- Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador
- Resolução de problemas do desktop remoto usando o AWS Systems Manager
- Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto
- Perdi minha chave privada. Como posso me conectar à minha instância do Windows?

O Remote Desktop não pode se conectar ao computador remoto

Tente o seguinte para resolver problemas relacionados à conexão com sua instância:

- Verifique se você está usando o nome de host DNS público correto. No console do Amazon EC2, selecione a instância e verifique o DNS público (IPv4) no painel de detalhes. Se sua instância estiver em uma VPC e você não vir um nome DNS público, deverá habilitar nomes de host DNS.

Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC.

- Verifique se sua instância tem um endereço IPv4 público. Se não tiver, associe um endereço IP elástico à sua instância. Para obter mais informações, consulte Endereços IP elásticos.
- Para conectar-se à sua instância usando um endereço IPv6, verifique se seu computador local tem um endereço IPv6 e está configurado para usar IPv6. Para obter mais informações, consulte Configurar o IPv6 em suas instâncias no Guia do usuário da Amazon VPC.
- Verifique se o grupo de segurança tem uma regra que permita o acesso RDP.
- Se você copiou a senha, mas obtiver o erro `Your credentials did not work`, tente digitá-la manualmente quando solicitado. É possível que você tenha omitido um caractere ou inserido um espaço em branco extra ao copiar a senha.
- Verifique se a instância passou nas verificações de status. Para obter mais informações, consulte Verificações de status para as instâncias e the section called “Falha nas verificações de status no Linux”.
- Verifique se a tabela de rotas da sub-rede tem uma rota que envie todo o tráfego destinado para fora da VPC para o gateway da Internet da VPC. Para obter mais informações, consulte Criação de uma tabela de rotas personalizada (gateways da Internet) no Guia do usuário da Amazon VPC.
- Verifique se o Firewall do Windows ou outros softwares de firewall não estão bloqueando o tráfego de RDP para a instância. Recomendamos que você desabilite o Firewall do Windows e controle o acesso à sua instância usando regras de grupo de segurança. Você pode usar o AWSSupport-TroubleshootRDP para disable the Windows Firewall profiles using SSM Agent. Para desabilitar o Firewall do Windows em uma instância do Windows que não esteja configurada para o AWS Systems Manager, use AWSSupport-ExecuteEC2Rescue ou use as seguintes etapas manuais:

Etapas manuais

1. Interrompa a instância afeta e desanexe seu volume raiz.
2. Execute uma instância temporária na mesma zona de disponibilidade que a instância afetada.

> **Warning**
>
> Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por

exemplo, se a instância original usa a AMI AWS do Windows para Windows Server 2016, inicie a instância temporária usando a AMI AWS do Windows para Windows Server 2019.

3. Anexe o volume raiz da instância afetada a essa instância temporária. Conecte-se à instância temporária, abra o utilitário Disk Management e ative a unidade.
4. Abra Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SYSTEM` e especifique um nome de chave quando solicitado (é possível usar qualquer nome).
5. Selecione a chave que você acabou de carregar e vá até `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Para cada chave com um nome da forma xxxxProfile, selecione a chave e altere `EnableFirewall` de 1 a 0. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.
6. (Opcional) Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas a seguir ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco.

   > **Warning**
   >
   > O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulteConfigure the Registry (Configurar o Registro).

   a. Abra um prompt de comando, digite regedit.exe e pressione Enter.
   b. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.
   c. Digite Windows Boot Manager e escolha Localizar Próxima.
   d. Escolha a chave chamada `11000001`. Essa chave é irmã da chave que você localizou na etapa anterior.
   e. No painel direito, selecione `Element` e escolha Modificar no menu de contexto (clique com o botão direito do mouse).

f. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é E9EB3AA5:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

```
diskpart
```

h. Execute o comando DiskPart a seguir para selecionar o volume. (É possível verificar se o número do disco é 1 usando o utilitário Gerenciamento de disco.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco do BCD que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. Usando o utilitário Disk Management, desative o volume da unidade.

> **Note**
>
> A unidade ficará offline automaticamente se a instância temporária estiver executando o mesmo sistema operacional que a instância afetada, portanto, você não precisará deixá-la offline manualmente.

8. Desanexe o volume da instância temporária. É possível encerrar a instância temporária se você não tiver utilização adicional para ela.
9. Restaure o volume raiz da instância afetada anexando-a como `/dev/sda1`.
10. Inicie a instância.

- Verifique se a autenticação no nível de rede está desabilitada nas instâncias que não fazem parte de um domínio do Active Directory (use AWSSupport-TroubleshootRDP para disable NLA).
- Verifique se o tipo de startup do serviço da área de trabalho remota (TermService) é automático e se o serviço foi iniciado (use AWSSupport-TroubleshootRDP para enable and start the RDP service).
- Verifique se você está se conectando à porta correta do protocolo RDP, que por padrão é 3389 (use AWSSupport-TroubleshootRDP para read the current RDP port e change it back to 3389).
- Verifique se as conexões da área de trabalho remota são permitidas na sua instância (use AWSSupport-TroubleshootRDP para enable Remote Desktop connections).
- Verifique se a senha não expirou. Se a senha expirou, será possível redefini-la. Para ter mais informações, consulte Redefinir uma senha de administrador do Windows perdida ou expirada.
- Se você tentar conectar-se usando um usuário que você criou na instância e receber o erro `The user cannot connect to the server due to insufficient access privileges`, verifique se você concedeu ao usuário o direito de fazer login localmente. Para obter mais informações, consulte Conceder o direito de fazer login localmente a um membro.
- Se você tentar mais sessões simultâneas do RDP do que o máximo permitido, sua sessão será encerrada com a mensagem `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Por padrão, são permitidas duas sessões simultâneas do RDP para sua instância.

Erro ao usar o cliente RDP do macOS

Se estiver se conectando a uma instância do Windows Server usando o cliente de Conexão de Área de Trabalho Remota do site da Microsoft, poderá receber o seguinte erro:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Faça download do aplicativo Área de Trabalho Remota da App Store do Mac e use o aplicativo para conectar-se à instância.

O RDP exibe uma tela preta em vez da área de trabalho

Tente o seguinte para resolver esse problema:

- Verifique a saída do console para ver se há informações adicionais. Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
- Verifique se você está executando a versão mais recente do cliente do RDP.
- Tente as configurações padrão para o cliente do RDP. Para obter mais informações, consulte Ambiente de sessão remota.
- Se você estiver usando o Remote Desktop Connection, tente iniciá-lo com a opção `/admin` da seguinte forma.

  ```
  mstsc /v:instance /admin
  ```

- Se o servidor estiver executando um aplicativo de tela total, talvez tenha parado de responder. Use Ctrl+Shift+Esc para iniciar o Windows Task Manager e feche o aplicativo.
- Se o servidor for utilizado em excesso, talvez tenha parado de responder. Para monitorar a instância usando o console do Amazon EC2, selecione a instância e escolha a guia Monitoramento. Se você precisar alterar o tipo de instância para um tamanho maior, consulte Alterar o tipo de instância.

Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador

Se você não puder fazer login remotamente em uma instância do Windows com um usuário que não seja uma conta de administrador, conceda ao usuário o direito de fazer login localmente. Veja Dar a um usuário ou grupo o direito de entrar localmente nos controladores de domínio no domínio.

Resolução de problemas do desktop remoto usando o AWS Systems Manager

É possível usar o AWS Systems Manager para resolver problemas conectando-se à sua instância do Windows usando RDP.

AWSSupport-TroubleshootRDP

O documento de automação AWSSupport-TroubleshootRDP permite ao usuário verificar ou modificar configurações comuns na instância de destino que possam afetar as conexões RDP (Remote Desktop Protocol), como os perfis RDP Port, Network Layer Authentication (NLA) e Windows Firewall. Por padrão, o documento lê e exibe os valores dessas configurações.

O documento de automação AWSSupport-TroubleshootRDP pode ser usado com instâncias do EC2, instâncias on-premises e máquinas virtuais (VMs) habilitadas para uso com o AWS Systems Manager (instâncias gerenciadas). Além disso, ele também pode ser usado com instâncias do EC2 para Windows Server não habilitadas para uso com o Systems Manager. Para obter informações sobre a habilitação de instâncias para uso com o AWS Systems Manager, consulte Nós gerenciado do no Guia do usuário do AWS Systems Manager.

Para resolver os problemas usando o documento AWSSupport-TroubleshootRDP

1. Faça login no console do Systems Manager.
2. Verifique se você está na mesma região que a instância prejudicada.
3. Escolha Documents (Documentos) no painel de navegação à esquerda.
4. Na guia Owned by Amazon (Pertencente à Amazon), insira `AWSSupport-TroubleshootRDP` no campo de pesquisa. Quando o documento `AWSSupport-TroubleshootRDP` aparecer, selecione-o.
5. Escolha Execute automation.
6. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).

7. Em Input parameters (Parâmetros de entrada), InstanceId, ative Show interactive instance picker (Mostrar seletor interativo de instâncias).
8. Escolha a instância do Amazon EC2.
9. Revise os exemplos e escolha Execute (Executar).
10. Para monitorar o progresso da execução, no Execution status (Status execução), aguarde o status mudar de Pending (Pendente) para Success (Êxito). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha um item da Step ID (ID da etapa).

Exemplos do AWSSupport-TroubleshootRDP

Os exemplos a seguir mostram como conquistar tarefas de resolução de problema comuns usando AWSSupport-TroubleshootRDP. É possível usar o comando de exemplo AWS CLI start-automation-execution ou o link fornecido para o AWS Management Console.

Example Exemplo: verifique o status atual de RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Exemplo: desativar o Firewall do Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Exemplo: desativar a autenticação no nível da rede

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Exemplo: definir o tipo de startup do serviço RDP como automático e iniciar o serviço RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Exemplo: restaurar a porta RDP padrão (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Example: permitir conexões remotas

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

O documento de automação AWSSupport-ExecuteEC2Rescue usa o EC2Rescue para Windows Server com a finalidade de solucionar e restaurar automaticamente a conectividade e os problemas relacionados ao protocolo RDP da instância do EC2. Para obter mais informações, consulte Executar a ferramenta EC2Rescue em instâncias inacessíveis.

O documento de automação AWSSupport-ExecuteEC2Rescue exige que a instância seja interrompida e reiniciada. O Systems Manager Automation interrompe a instância e cria uma Imagem de máquina da Amazon (AMI). Dados armazenados nos volumes de armazenamento da instância são perdidos. O endereço IP público será alterado se você não estiver usando um endereço IP elástico. Para obter mais informações, consulte Executar a ferramenta EC2Rescue em instâncias inacessíveis no Guia do usuário do AWS Systems Manager.

Para resolver o problema usando o documento AWSSupport-ExecuteEC2Rescue

1. Abra o console do Systems Manager.
2. Verifique se você está na mesma região que a instância Amazon EC2 prejudicada.
3. No painel de navegação, escolha Documentos.
4. Pesquise e selecione o documento `AWSSupport-ExecuteEC2Rescue` e depois escolha Executar automação.
5. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).
6. Na seção Input parameters (Parâmetros de entrada), em UnreachableInstanceId, insira o ID da instância do Amazon EC2 para a instância inacessível.

7. (Opcional) Para LogDestination, insira o nome do bucket do Amazon Simple Storage Service (Amazon S3) se quiser coletar logs do sistema operacional para solucionar problemas da sua instância do Amazon EC2. Os logs são enviados automaticamente para o bucket especificado.
8. Selecione Execute (Executar).
9. Para monitorar o progresso da execução, no status Execution (Execução), aguarde o status mudar de Pending (Pendente) para Success (Concluído com sucesso). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha Step ID (ID da etapa).

Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto

Se a instância inacessível não for gerenciada pelo Gerenciador de sessões do AWS Systems Manager, será possível usar o registro remoto para habilitar a área de trabalho remota.

1. No console do EC2, interrompa a instância inacessível.
2. Desvincule o volume raiz da instância inacessível e anexe-o a uma instância acessível na mesma zona de disponibilidade como um volume de armazenamento. Se você não tiver uma instância acessível na mesma zona de disponibilidade, inicie uma. Observe o nome do dispositivo do volume raiz na instância inacessível.
3. Na instância acessível, abra Gerenciamento de disco. Você pode fazer isso executando o comando a seguir em uma janela de prompt de comando.

   ```
   diskmgmt.msc
   ```
4. Clique com o botão direito do mouse no volume recém-conectado que veio da instância inacessível e escolha Online.
5. Abrir o Editor do Registro do Windows. Você pode fazer isso executando o comando a seguir em uma janela de prompt de comando.

   ```
   regedit
   ```
6. No Editor do registro, escolha HKEY_LOCAL_MACHINE e selecione Arquivo, Carregar hive.
7. Selecione a unidade do volume conectado, navegue até `\Windows\System32\config\`, `SYSTEM`, selecione e escolha Open (Abrir).
8. Em Key Name (Nome da chave), insira um nome exclusivo para o hive e escolha OK.

9. Faça uma cópia de backup do hive do registro antes de fazer qualquer alteração no registro.

   a. *Na árvore de console do Editor do Registro, selecione o hive que você carregou:* ***HKEY_LOCAL_MACHINE*** *your-key-name*.

   b. Escolha Arquivo, Exportar.

   c. Na caixa de diálogo Export Registry File (Exportar arquivo do registro), escolha o local no qual deseja salvar a cópia de backup e digite um nome para o arquivo de backup no campo File Name (Nome do arquivo).

   d. Escolha Salvar.

10. No Editor do Registro, navegue para `HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server` e depois no painel de detalhes, clique duas vezes em fDenyTSConnections.

11. Na caixa de valor Edit DWORD (Editar DWORD) insira `0` no campo Value Data (Dados do valor).

12. Escolha OK.

> **Note**
>
> Se o valor no campo Value data (Dados do valor) for `1`, a instância negará conexões de área de trabalho remota. Um valor de `0` permitirá conexões de área de trabalho remota.

13. No Editor do Registro, escolha HKEY_LOCAL_MACHINE*your-key-name* e selecione Arquivo, Descarregar hive.

14. Feche o Editor do registro e Gerenciamento de disco.

15. No console do EC2, desanexe o volume raiz da instância acessível à qual você o anexou e anexe-o novamente à instância inacessível. Ao anexar o volume à instância inacessível, insira o nome do dispositivo que você salvou anteriormente no campo dispositivo.

16. Reinicie a instância inacessível.

Perdi minha chave privada. Como posso me conectar à minha instância do Windows?

Quando você se conecta a uma instância do Windows recém-iniciada, você descriptografa a senha da conta do administrador usando a chave privada para o par de chaves que você especificou quando iniciou a instância.

Se você perder a senha do Administrador e não tiver mais a chave privada, é preciso redefinir a senha ou criar uma nova instância. Para ter mais informações, consulte Redefinir uma senha de administrador do Windows perdida ou expirada. Para conhecer as etapas e redefinir a senha usando um documento do Systems Manager, consulte Redefinir senhas e chaves SSH nas instâncias do EC2 no Manual do usuário do AWS Systems Manager.

Redefinir uma senha de administrador do Windows perdida ou expirada

> **Note**
>
> Esta seção se aplica somente a instâncias do Windows.

Se não conseguir mais acessar sua instância do Amazon EC2 no Windows porque a senha do administrador do Windows está incorreta ou expirou, você poderá redefinir a senha.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Os métodos manuais para redefinir a senha de administrador usam o EC2Launch v2, o EC2Config ou o EC2Launch.

- Para todas as AMIs do Windows compatíveis que incluem o agente EC2Launch v2, use o EC2Launch v2.
- Para AMIs do Windows anteriores ao Windows Server 2016, você pode usar o serviço EC2Config.
- Para AMIs do Windows Server 2016 e posterior, use o serviço EC2Launch.

Esses procedimentos também descrevem como se conectar a uma instância se você perder o par de chaves que foi usado para criar a instância. O Amazon EC2 usa uma chave pública para criptografar uma parte dos dados, como uma senha, e uma chave privada para descriptografar os dados. As

chaves pública e privada são conhecidas como par de chaves. Com instâncias do Windows, você usa um par de chaves para obter a senha do administrador e faz login usando o RDP.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

Conteúdo

- Redefinir a senha de administrador do Windows usando o EC2Launch v2
- Redefinir a senha de administrador do Windows usando o EC2Config
- Redefinir a senha de administrador do Windows usando o EC2Launch

Redefinir a senha de administrador do Windows usando o EC2Launch v2

Se você perdeu a senha de administrador do Windows e está usando uma AMI compatível do Windows que inclua o agente EC2Launch v2, poderá usar o EC2Launch v2 para gerar uma nova senha.

Se estiver usando uma AMI do Windows Server 2016 ou posterior que não inclua o agente EC2Launch v2, consulte Redefinir a senha de administrador do Windows usando o EC2Launch.

Se estiver usando uma AMI do Windows Server anterior a 2016 que não inclua o agente EC2Launch v2, consulte Redefinir a senha de administrador do Windows usando o EC2Config.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir a senha de administrador do Windows usando o EC2Launch v2, é necessário fazer o seguinte:

- Etapa 1: verificar se o agente EC2Launch v2 está em execução
- Etapa 2: Desanexar o volume raiz da instância
- Etapa 3: Anexar o volume a uma instância temporária
- Etapa 4: Excluir o arquivo .run-once
- Etapa 5: Reiniciar a instância original

Etapa 1: verificar se o agente EC2Launch v2 está em execução

Antes de tentar redefinir a senha de administrador, verifique se o agente EC2Launch v2 está instalado e em execução. O agente EC2Launch v2 será utilizado para redefinir a senha de administrador posteriormente nesta seção.

Verificar se o agente EC2Launch v2 está em execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.
4. Localize a entrada do EC2 Launch, por exemplo, Launch: EC2Launch v2 service v2.0.124 (Launch: serviço EC2Launch v2 v2.0.124). Se essa entrada for exibida, o serviço EC2Launch v2 estará em execução.

   Se a saída do log do sistema estiver vazia ou se o agente EC2Launch v2 não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para ter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.

Etapa 2: Desanexar o volume raiz da instância

Não será possível usar o EC2Launch v2 para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

    a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.
    b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.
    c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).
    d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.
    e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.
    f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.
    g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.
5. Desanexe o volume raiz da instância original da seguinte forma:

a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

b. No painel de navegação, escolha Volumes.

c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

> **Important**
>
> Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

> **Important**
>
> A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

d. Na página Review Instance Launch, escolha Launch.

e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

   a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

   b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

   c. Em Device (Dispositivo), digite **`xvdf`** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Excluir o arquivo .run-once

Agora, você deve excluir o arquivo `.run-once` do volume off-line anexado à instância. Isso instrui o EC2Launch v2 a executar todas as tarefas com uma frequência de `once`, o que inclui a definição da senha de administrador. O caminho do arquivo no volume secundário que você anexou será semelhante a `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Excluir o arquivo .run-once

1. Abra o utilitário Gerenciamento de Disco e coloque a unidade on-line usando estas instruções: Make an Amazon EBS volume available for use.
2. Localize o arquivo `.run-once` no disco que você colocou on-line.
3. Exclua o arquivo .run-once.

> **Important**
>
> Todos os scripts definidos para uma execução serão acionados por essa ação.

Etapa 5: Reiniciar a instância original

Depois de excluir o arquivo `.run-once`, anexe novamente o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:
   a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).
   b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.
   c. Em Device (Dispositivo), digite **`/dev/sda1`**.
   d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.
2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à sua instância do Windows do .

   > **Important**
   >
   > A instância recebe um novo endereço IP público depois de você a interrompe e a inicia. Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte Ciclo de vida da instância.

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows usando o EC2Config

Se você perdeu a senha de administrador do Windows e está usando uma AMI do Windows anterior ao Windows Server 2016, poderá usar o agente EC2Config para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server 2016 ou posterior, consulte Redefinir a senha de administrador do Windows usando o EC2Launch, ou poderá usar a ferramenta EC2Rescue, que utiliza o serviço EC2Launch para gerar uma nova senha.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Config, você precisa fazer o seguinte:

- Etapa 1: Verificar se o serviço do EC2Config está em execução
- Etapa 2: Desanexar o volume raiz da instância
- Etapa 3: Anexar o volume a uma instância temporária
- Etapa 4: Modificar o arquivo de configuração
- Etapa 5: Reiniciar a instância original

Etapa 1: Verificar se o serviço do EC2Config está em execução

Antes de tentar redefinir a senha de administrador, verifique se o serviço EC2Config está instalado e em execução. Você utilizará o serviço EC2Config para redefinir a senha de administrador posteriormente nesta seção.

Para verificar se o serviço do EC2Config está em execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. (Novo console) Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.

   (Console antigo) Escolha Actions (Ações), System Settings(Configurações do sistema), Get System Log (Obter log do sistema).
4. Encontre a entrada agente do EC2, por exemplo, EC2 Agent: Ec2Config service v3.18.1118 (Agente do EC2: serviço Ec2Config v3.18.1118). Se você vir essa entrada, o serviço EC2Config estará em execução.

   Se a saída do log do sistema estiver vazia, ou se o serviço EC2Config não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para ter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.

Etapa 2: Desanexar o volume raiz da instância

Você não poderá usar o EC2Config para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.

b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.

c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).

d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.

e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.

f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.

g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.

5. Desanexe o volume raiz da instância original da seguinte forma:

a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

b. No painel de navegação, escolha Volumes.

c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

   > **Important**
   >
   > Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

   b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

   c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

   > **Important**
   >
   > A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

   d. Na página Review Instance Launch, escolha Launch.

   e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

c. Em Device (Dispositivo), digite **xvdf** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Modificar o arquivo de configuração

Depois de anexar o volume à instância temporária como um volume secundário, modifique o plug-in `Ec2SetPassword` no arquivo de configuração.

Para modificar o arquivo de configuração

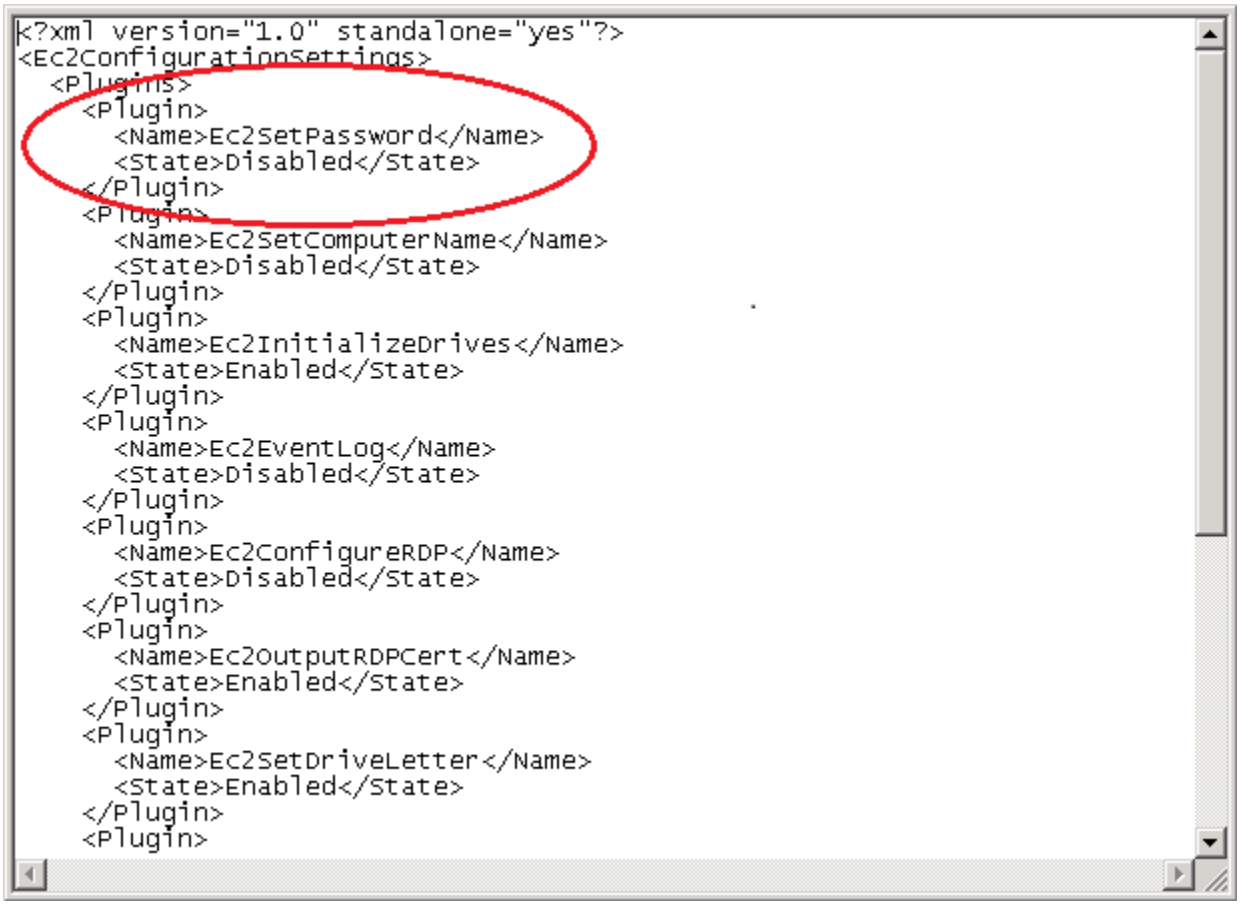
1. Na instância temporária, modifique o arquivo de configuração no volume secundário da seguinte maneira:

   a. Execute a instância temporária e conecte-se a ela.

   b. Use as instruções a seguir para ativar a unidade online: Disponibiliar o volume do Amazon EBS para uso.

   c. Navegue até o volume secundário e abra `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` usando um editor de texto, como o Bloco de notas.

   d. Na parte superior do arquivo, localize o plugin com o nome `Ec2SetPassword`, como mostrado no screenshot. Altere o estado de `Disabled` para `Enabled` e salve o arquivo.



2. Depois de modificar o arquivo de configuração, desconecte o volume secundário da instância temporária da seguinte maneira:

   a. Usando o utilitário Disk Management (Gerenciamento de disco), desative o volume.

   b. Desconecte-se da instância temporária e volte para o console Amazon EC2.

   c. No painel de navegação, selecione Volumes, selecione o volume e escolha Actions (Ações), Detach Volume (Desanexar volume). Quando o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 5: Reiniciar a instância original

Depois de modificar o arquivo de configuração, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.

c. Em Device (Dispositivo), digite **`/dev/sda1`**.

d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.

3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à sua instância do Windows do .

> **Important**
>
> A instância recebe um novo endereço IP público depois de você a interrompe e a inicia. Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte Ciclo de vida da instância.

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows usando o EC2Launch

Se você esqueceu a senha de administrador do Windows e está usando uma AMI do Windows Server 2016 ou posterior, poderá usar a ferramenta EC2Rescue, que utiliza o serviço EC2Launch para gerar uma nova senha.

Caso esteja usando uma AMI do Windows Server 2016 ou posterior que não inclua o agente EC2Launch v2, você pode usar o EC2Launch para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server anterior ao Windows Server 2016, consulte Redefinir a senha de administrador do Windows usando o EC2Config.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Launch, você precisa fazer o seguinte:

- Etapa 1: Desanexar o volume raiz da instância
- Etapa 2: Anexar o volume a uma instância temporária
- Etapa 3: Redefinir a senha de administrador
- Etapa 4: Reiniciar a instância original

Etapa 1: Desanexar o volume raiz da instância

Você não poderá usar o EC2Launch para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

   a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.

   b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.

   c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).

   d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.

   e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.

   f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.

   g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.

5. Desanexe o volume raiz da instância original da seguinte forma:

   a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

   b. No painel de navegação, escolha Volumes.

c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 2: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância que você usa para executar o EC2Launch.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

   > **Important**
   >
   > Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

   b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

   c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

   > **Important**
   >
   > A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de

disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

d. Na página Review Instance Launch, escolha Launch.

e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

c. Em Device (Dispositivo), digite **`xvdf`** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 3: Redefinir a senha de administrador

Em seguida, conecte-se à instância temporária e use o EC2Launch para redefinir a senha do administrador.

Para redefinir a senha de administrador

1. Conecte-se à instância temporária e use a ferramenta EC2Rescue for Windows Server na instância para redefinir a senha de administrador, da seguinte maneira:

a. Faça download do arquivo zip EC2Rescue for Windows Server, extraia o conteúdo e execute EC2Rescue.exe.

b. Na tela License Agreement (Contrato de licença), leia o contrato de licença e, se você aceitar os termos, escolha I Agree (Eu aceito).

c. Na tela Welcome to EC2Rescue for Windows Server (Bem-vindo ao EC2Rescue for Windows Server), escolha Next (Avançar).

d. Na tela Select mode (Selecionar modo), escolha Offline instance (Instância offline).

e. Na tela Select a disk (Selecionar um disco), selecione o dispositivo xvdf e, em seguida, Next (Avançar).

f. Confirme a seleção do disco e escolha Yes.

g. Depois que o volume for carregado, escolha OK.

h. Na tela Select Offline Instance Option (Selecionar opção de instância offline), escolha Diagnose and Rescue (Diagnosticar e recuperar).

i. Na tela Summary (Resumo), leia as informações e escolha Next (Avançar).

j. Na tela Detected possible issues (Problemas possíveis detectados), selecione Reset Administrator Password (Redefinir senha do administrador) e escolha Next (Avançar).

k. Na tela Confirm (Confirmar), escolha Rescue (Recuperar), OK.

l. Na tela Done (Concluído), escolha Finish (Concluir).

m. Feche a ferramenta EC2Rescue for Windows Server, desconecte-se da instância temporária e, em seguida, retorne para o console do Amazon EC2.

2. Desanexe o volume (`xvdf`) secundário da instância temporária da seguinte forma:

a. No painel de navegação, escolha Instances (Instâncias) e selecione a instância temporária.

b. Na guia Storage (Armazenamento) da instância temporária, observe o ID do volume do EBS listado como xvdf.

c. No painel de navegação, escolha Volumes.

d. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 4: Reiniciar a instância original

Depois de redefinir a senha do administrador usando o EC2Launch, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

Para reiniciar a instância original

1. Reanexe o volume à instância original da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.

c. Em Device (Dispositivo), digite **`/dev/sda1`**.

d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à sua instância do Windows do .
4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Solucionar problemas de uma instância não acessível

É possível usar os métodos apresentados a seguir para solucionar problemas de uma instância do Amazon EC2 inacessível.

Conteúdo

- Reinicialização da instância
- Saída do console da instância
- Fazer uma captura de tela de uma instância inacessível
- Capturas de tela comuns para instâncias do Windows
- Recuperação da instância quando um computador host falhar

Reinicialização da instância

A capacidade de reinicializar instâncias que de outra forma seriam inacessíveis é valiosa para a solução de problemas e o gerenciamento geral de instâncias.

Assim como poderá redefinir um computador pressionando o botão de restauração, você pode também redefinir instâncias do EC2 usando o console, a CLI ou a API do Amazon EC2. Para ter mais informações, consulte Reinicializar a instância.

Saída do console da instância

A saída do console é uma ferramenta valiosa para o diagnóstico de problemas. É especialmente útil para resolver problemas de kernel e problemas de configuração de serviço que possam fazer com que uma instância seja encerrada ou torne-se inalcançável antes de seu daemon SSH ser iniciado.

- Instâncias do Linux: a saída do console da instância exibe exatamente o que seria mostrado em um monitor físico conectado a um computador. A saída do console retorna as informações armazenadas em buffer que foram postadas logo após um estado de transição de instância (iniciar, parar, reinicializar e finalizar). A saída publicada não é atualizada continuamente; somente quando for provável que seja do valor principal.
- Instâncias do Windows: a saída do console da instância inclui os três últimos erros do log de eventos do sistema.

É possível recuperar a saída mais recente do console de série em qualquer momento durante o ciclo de vida da instância. Há suporte para essa opção somente em instâncias desenvolvidas no AWS Nitro System. Não é compatível por meio do console do Amazon EC2.

> **Note**
>
> Somente os 64 KB mais recentes da saída postada são armazenados, que estão disponíveis por no mínimo 1 hora após a última postagem.

Somente o proprietário da instância pode acessar a saída do console.

Use um dos métodos a seguir para obter o resultado do console.

Console

Para obter o resultado do console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância e escolha Ações, Monitorar e solucionar problemas e Obter log do sistema.

Command line

Para obter o resultado do console

É possível usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- get-console-output (AWS CLI)

- Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell)

Fazer uma captura de tela de uma instância inacessível

Caso não seja possível realizar a conexão com a instância, você pode capturar uma captura de tela da instância e visualizá-la como uma imagem. A imagem pode dar visibilidade quanto ao status da instância e permite uma solução de problemas mais rápida.

É possível gerar capturas de tela enquanto a instância estiver em execução ou após haver falha. A imagem é gerada em formato JPG e não é maior que 100 KB. Não há custo de transferência de dados para a captura de tela.

Limitações

Este recurso não é compatível com as seguintes instâncias:

- Instâncias bare metal (instâncias do tipo `*.metal`)
- A instância está usando um driver NVIDIA GRID
- Instâncias com processadores Graviton baseados em ARM
- Instâncias Windows em AWS Outposts

Supported Regions (Regiões compatíveis)

Este recurso está disponível nas seguintes Regiões da :

- US East (N. Virginia) Region
- Região Leste dos EUA (Ohio)
- Região Oeste dos EUA (Norte da Califórnia)
- Região Oeste dos EUA (Oregon)
- Região África (Cidade do Cabo)
- Região Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Haiderabade)
- Região Ásia-Pacífico (Jacarta)
- Região Ásia-Pacífico (Melbourne)
- Região Ásia-Pacífico (Mumbai)
- Região Ásia-Pacífico (Osaka)

- Região Ásia-Pacífico (Seul)
- Região Ásia-Pacífico (Singapura)
- Região Ásia-Pacífico (Sydney)
- Região Ásia-Pacífico (Tóquio)
- Região do Canadá (Central)
- Região Oeste do Canadá (Calgary)
- Região da China (Pequim)
- Região da China (Ningxia)
- Região Europa (Frankfurt)
- Região Europa (Irlanda)
- Região Europa (Londres)
- Região Europa (Milão)
- Região Europa (Paris)
- Região Europa (Espanha)
- Região Europa (Estocolmo)
- Região Europa (Zurique)
- Região de Israel (Tel Aviv)
- Região América do Sul (São Paulo)
- Região Oriente Médio (Bahrein)
- Região do Oriente Médio (Emirados Árabes Unidos)

Console

Para obter uma captura de tela de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância a ser capturada.
4. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get instance screenshot (Obter captura de tela da instância).
5. Escolha Download ou clique com o botão direito do mouse na imagem para fazer download e salvá-la.

Command line

Para obter uma captura de tela de uma instância

É possível usar um dos comandos a seguir. O conteúdo apresentado é codificado por base64. Para obter mais informações sobre essas interfaces de linha de comando, consulte Acessar o Amazon EC2.

- get-console-screenshot (AWS CLI)
- GetConsoleScreenshot (API de consulta do Amazon EC2)

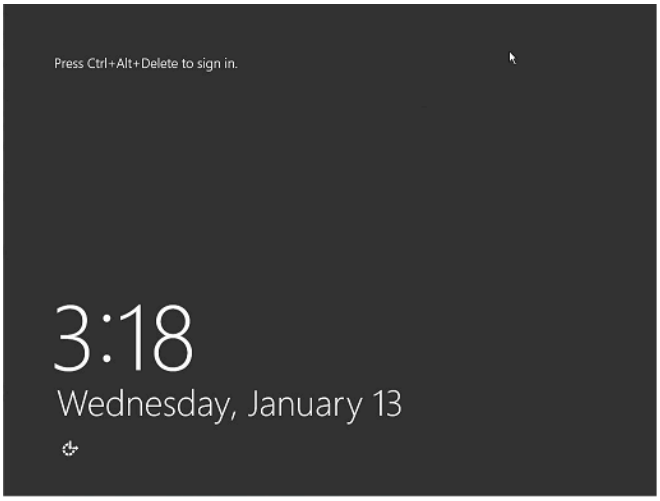
Capturas de tela comuns para instâncias do Windows

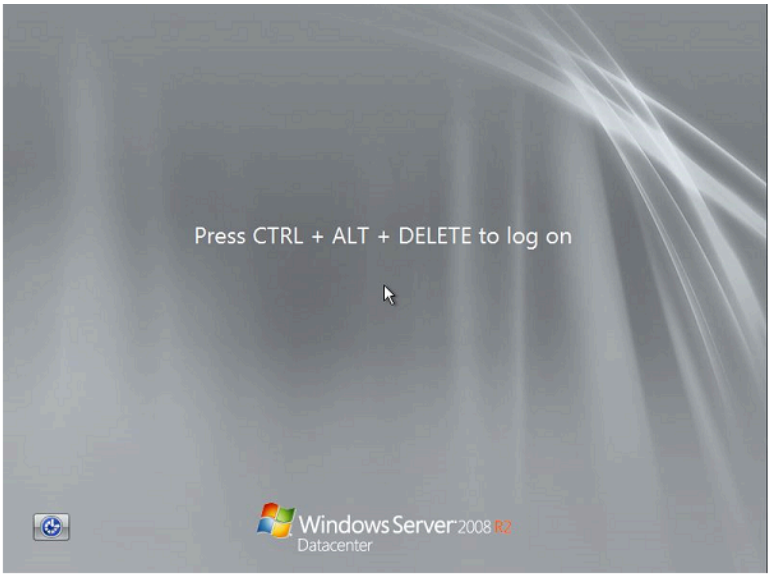
É possível usar as informações a seguir para ajudar a solucionar problemas de uma instância inacessível do Windows com base nas capturas de tela retornadas pelo serviço.

- Tela de login (Ctrl+Alt+Delete)
- Tela de console de recuperação
- Tela do gerenciador de inicialização do Windows
- Tela Sysprep
- Tela de preparação
- Tela do Windows Update
- Chkdsk

Tela de login (Ctrl+Alt+Delete)

O serviço de captura de tela de console retornou o seguinte.





Se uma instância se tornar inacessível durante o login, talvez haja um problema com a configuração de rede ou com os Serviços de Área de Trabalho Remota do Windows. Uma instância também poderá não responder se um processo estiver usando grandes quantidades de CPU.

Configuração de rede

Use as seguintes informações para verificar se as configurações da AWS, do Microsoft Windows e da rede local (ou on-premises) não estão bloqueando o acesso à instância.

Configuração de rede da AWS

Configuração	Verificar
Configuração do security group	Verifique se a porta 3389 está aberta para o security group. Verifique se você está se conectando ao endereço IP público certo. Se a instância não foi associada a um IP elástico, o IP público será alterado depois que a instância for interrompida/iniciada. Para ter mais informações, consulte O Remote Desktop não pode se conectar ao computador remoto.
Configuração da VPC (Network ACLs)	Verifique se a lista de controle de acesso (ACL) para sua Amazon VPC não está bloqueand o acesso. Para obter informações, consulte

Configuração	Verificar
	Network ACLs no Guia do usuário da Amazon VPC.
Configuração de VPN	Se você estiver se conectando à VPC usando uma rede virtual privada (VPN), verifique a conectividade do túnel VPN. Para obter mais informações, consulte Como solucionar problemas de conectividade do túnel VPN para uma Amazon VPC?

Configuração de rede do Windows

Configuração	Verificar
Firewall do Windows	Verifique se o firewall do Windows não está bloqueando as conexões com a sua instância . Desabilite o firewall do Windows como descrito no item 7 da seção sobre solução de problemas do Remote Desktop, O Remote Desktop não pode se conectar ao computador remoto.
Configuração avançada de TCP/IP (uso de IP estático)	A instância pode não responder porque você configurou um endereço IP estático. Para uma VPC, crie uma interface de rede e anexe-a à instância.

Configuração de rede local ou on-premises

Verifique se uma configuração de rede local não está bloqueando o acesso. Tente se conectar a uma outra instância na mesma VPC onde se encontra a instância inacessível. Se você não conseguir acessar outra instância, trabalhe com o administrador de rede local para determinar se uma política local está restringindo o acesso.

Problemas com o Remote Desktop Services

Se não for possível acessar a instância durante o login, talvez haja um problema com os Serviços de Área de Trabalho Remota (RDS - Remote Desktop Services) na instância.

> **Tip**
>
> Você pode usar o runbook `AWSSupport-TroubleshootRDP` para verificar e modificar várias configurações que podem afetar as conexões do Remote Desktop Protocol (RDP). Para obter mais informações, consulte `AWSSupport-TroubleshootRDP` na Referência do runbook do AWS Systems Manager Automation.

Configuração do Remote Desktop Services

Configuração	Verificar
O RDS está em execução	Verifique se o RDS está em execução na instância. Conecte-se à instância usando o snap-in de serviços do Microsoft Management Console (MMC) (`services.msc`). Na lista de serviços, verifique se o Remote Desktop Services está Running (Em execução). Se não estiver, inicie-o e defina o tipo de inicialização como Automático. Se você não puder se conectar à instância usando o snap-in Services, desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e modifique a chave de Registro Start. Ao terminar, anexe novamente o volume raiz à instância original.
O RDS está habilitado	Mesmo se o serviço tiver sido iniciado, ele pode estar desabilitado. Desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e habilite o serviço modificando a chave do registro Terminal Server (Servidor de terminal) conforme descrito em Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto.

Configuração	Verificar
	Ao terminar, anexe novamente o volume raiz à instância original.

Alto uso da CPU

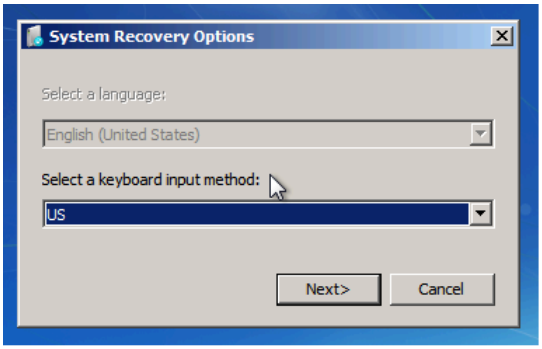
Verifique a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch. Se CPUUtilization (máximo) for um número alto, aguarde a desativação da CPU e tente se conectar novamente. A utilização elevada da CPU pode ser causada por:

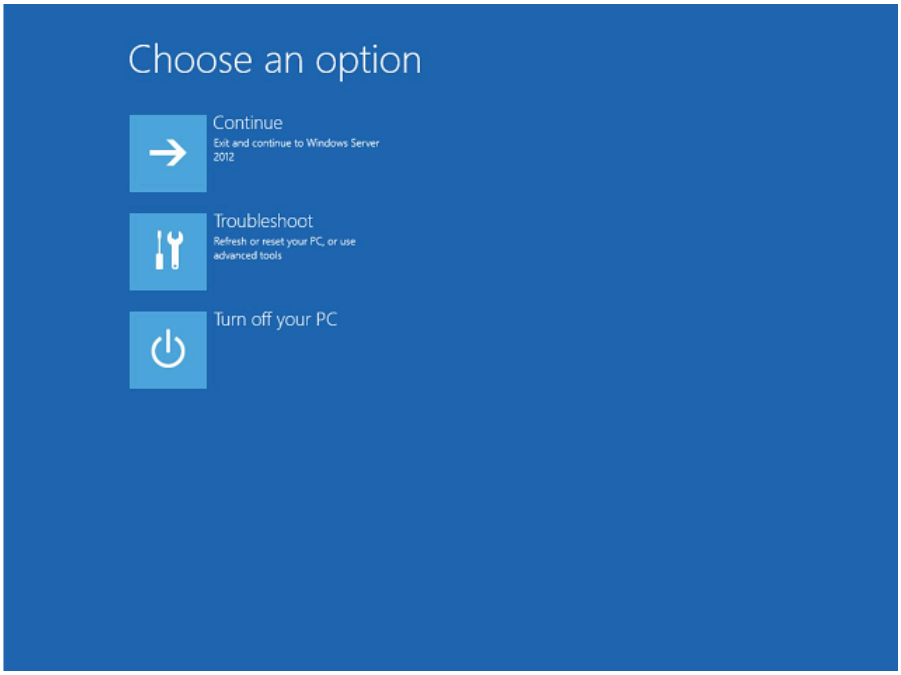
- Atualizações do Windows
- Verificação de software de segurança
- Script de inicialização personalizado
- Programador de tarefas

Para obter mais informações, consulte Obter as estatísticas de um recurso específico no Guia do usuário do Amazon CloudWatch. Para obter mais dicas sobre solução de problemas, consulte Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows).

Tela de console de recuperação

O serviço de captura de tela de console retornou o seguinte.





O sistema operacional pode ser inicializado no console de recuperação e travar nesse estado se `bootstatuspolicy` não estiver definido como `ignoreallfailures`. Use o procedimento a seguir para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`.

Por padrão, a configuração de políticas para AMIs públicas do Windows fornecidas pela AWS é definida como `ignoreallfailures`.

1. Interrompa a instância inacessível.
2. Crie um snapshot de novo volume raiz. O volume raiz é anexado à instância como `/dev/sda1`.

   Desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele e anexe-a a outra instância na mesma zona de disponibilidade que um volume secundário.

   > **Warning**
   >
   > Se sua instância temporária e instância original tiverem sido iniciadas usando a mesma AMI, será necessário executar etapas adicionais ou você não poderá iniciar a instância original após restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Se você precisar criar uma instância temporária com base na mesma AMI, siga as etapas em Colisão de assinatura em disco para evitar uma colisão de assinatura de disco.

Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usa uma AMI para Windows Server 2016, inicie a instância temporária usando uma AMI para Windows Server 2019.

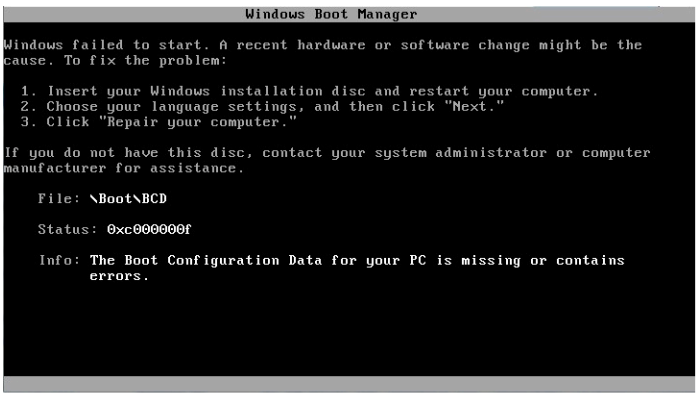
3. Faça login na instância e execute o seguinte comando em um prompt de comando para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`.

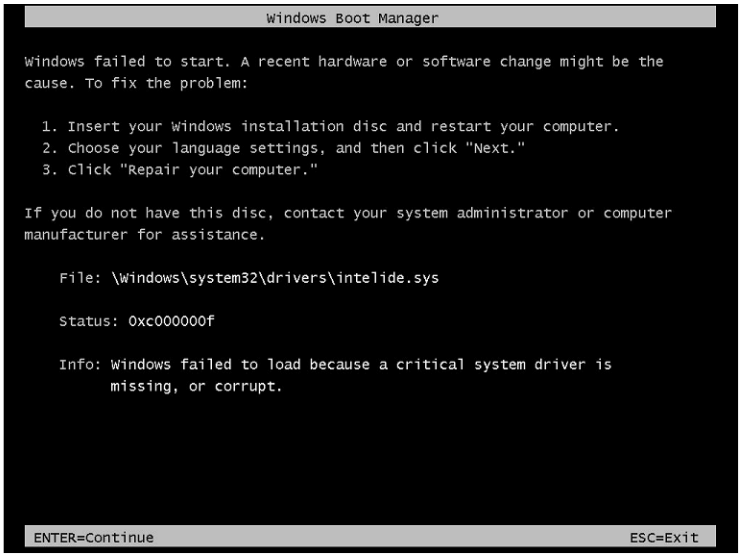
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Reanexe o volume à instância inacessível e inicie a instância novamente.

Tela do gerenciador de inicialização do Windows

O serviço de captura de tela de console retornou o seguinte.

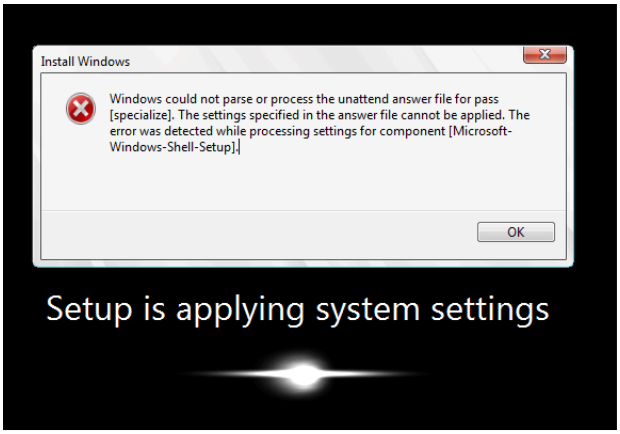


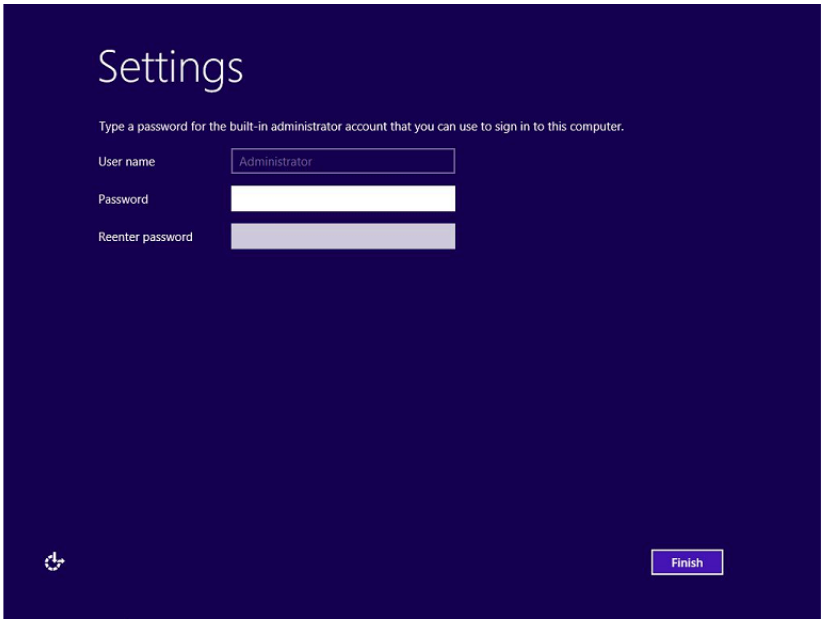


O sistema operacional experimentou um dano fatal no arquivo de sistema e/ou no Registro. Quando a instância trava nesse estado, é necessário recuperá-la de uma AMI de backup recente ou executar uma instância de substituição. Se você precisar acessar dados na instância, desanexe todos os volumes raiz da instância inacessível, crie um snapshot desses volumes ou crie uma AMI deles e anexe-os a outra instância na mesma zona de disponibilidade como um volume secundário.

Tela Sysprep

O serviço de captura de tela de console retornou o seguinte.

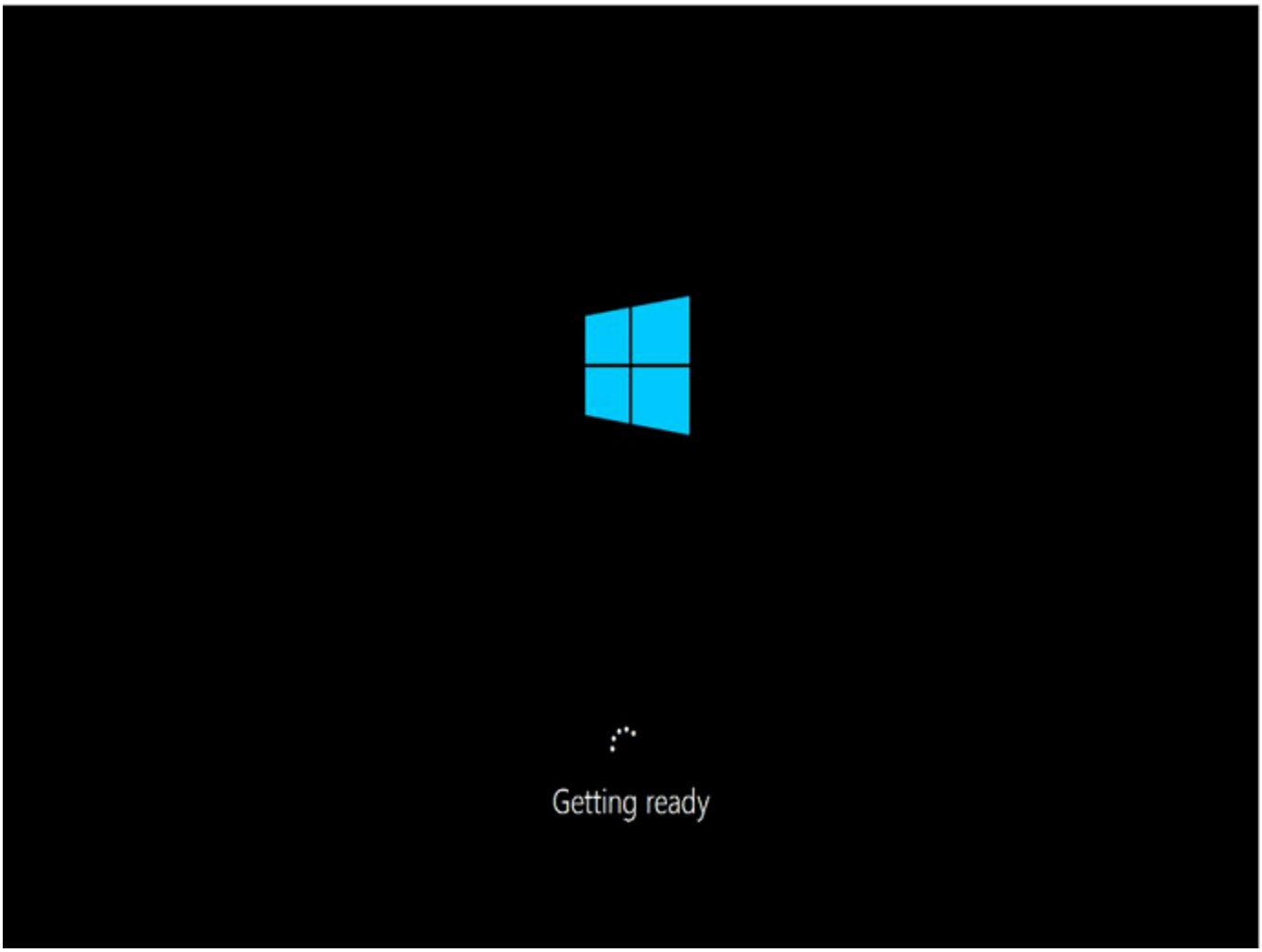




Será possível ver essa tela se não tiver usado o EC2Config Service para chamar Sysprep ou se o sistema operacional falhar ao executar o Sysprep. É possível redefinir a senha usando o EC2Rescue. Caso contrário, consulte Criação de uma AMI com a ferramenta Sysprep do Windows.

Tela de preparação

O serviço de captura de tela de console retornou o seguinte.



Atualize o Instance Console Screenshot Service repetidamente para verificar se o anel de andamento está girando. Se o anel estiver girando, aguarde a inicialização do sistema operacional. Também é possível verificar a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch para ver se o sistema operacional está ativo. Se o anel de andamento não estiver girando, a instância poderá travar no processo de inicialização. Reinicialize a instância. Se a reinicialização não resolver o problema, recupere a instância de uma AMI de backup recente ou execute uma instância de substituição. Se você precisar acessar os dados na instância, desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele. Em seguida, anexe-o a outra instância na mesma zona de disponibilidade que o volume secundário.

Tela do Windows Update

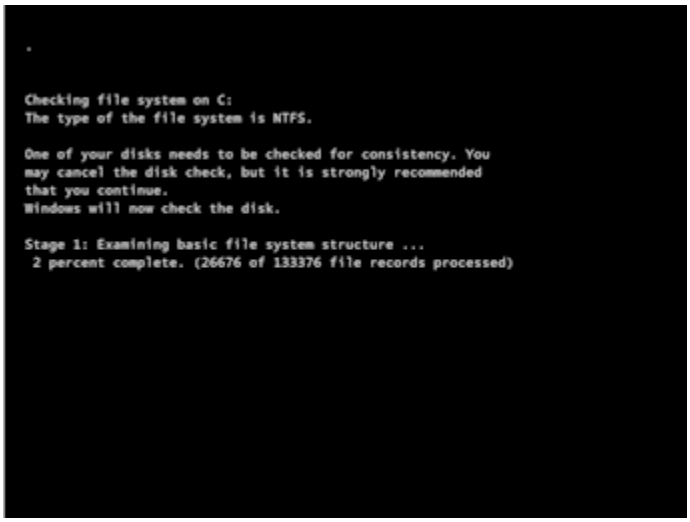
O serviço de captura de tela de console retornou o seguinte.

O processo do Windows Update está atualizando o Registro. Aguarde o término da atualização. Não reinicialize nem interrompa a instância, pois isso pode causar danos aos dados durante a atualização.

> **Note**
>
> O processo do Windows Update pode consumir recursos no servidor durante a atualização. Se você tiver esse problema com frequência, considere usar um tipo de instância e volumes do EBS mais rápidos.

Chkdsk

O serviço de captura de tela de console retornou o seguinte.



O Windows está executando a ferramenta de sistema chkdsk na unidade para verificar a integridade do sistema de arquivos e corrigir os erros lógicos do sistema de arquivos. Aguarde a conclusão do processo.

Recuperação da instância quando um computador host falhar

Se houver um problema irrecuperável com o hardware de um computador host subjacente, a AWS poderá programar um evento de interrupção da instância. Você será notificado desse evento com antecedência, por e-mail.

Para recuperar uma instância baseada no Amazon EBS sendo executada em um computador host que falhou

1. Faça backup de todos os dados importantes nos volumes do seu armazenamento de instâncias para Amazon EBS ou Amazon S3.
2. Pare a instância.
3. Inicie a instância.
4. Restaure todos os dados importantes.

Para ter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

Para recuperar uma instância com armazenamento de instâncias executada em um computador host que falhou

1. Crie um AMI a partir da instância.
2. Faça upload da imagem para Amazon S3.
3. Faça backup dos dados importantes para Amazon EBS ou Amazon S3.
4. Encerre a instância.
5. Execute uma nova instância a partir da AMI.
6. Restaure todos os dados importantes para a nova instância.

Solução de problemas na interrupção da instância

Se você tiver parado sua instância baseada no Amazon EBS e parecer que ela travou no estado `stopping`, pode haver um problema com o computador host subjacente.

Não existe qualquer custo para uso da instância enquanto ela está no estado `stopping` ou em qualquer outro estado, exceto `running`. Você só é cobrado pelo uso da instância quando ela está no estado `running`.

Forçar a parada da instância

Force a interrupção da instância usando o console ou a AWS CLI.

> **Note**
>
> É possível forçar uma instância a parar de usar o console somente enquanto ela estiver no estado `stopping`. É possível forçar uma instância a parar de usar o AWS CLI enquanto a instância estiver em qualquer estado, exceto `shutting-down` e `terminated`.

Console

Para forçar a parada da instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Instance state (Estado da instância), Force stop instance (Forçar parada da parada), Stop (Parar).

   A opção Force stop instance (Forçar interrupção de instância) estará disponível no console somente se a instância estiver no estado `stopping`. Se a instância estiver em outro estado (exceto `shutting-down` e `terminated`), você poderá usar AWS CLI para forçar a interrupção da instância.

AWS CLI

Para forçar a parada da instância usando a AWS CLI

Use o comando stop-instances e a opção `--force` da seguinte forma:

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Se, após dez minutos, a instância não tiver sido interrompida, publique uma solicitação de ajuda em AWS re:Post. Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que você já realizou. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no Atendimento ao cliente.

Para criar uma instância de substituição

Para tentar resolver o problema enquanto espera pela assistência do AWS re:Post ou do Support Center, crie uma instância de substituição. Crie uma AMI da instância travada e execute uma nova instância usando a nova AMI.

> **Important**
>
> A criação de uma instância substituta é recomendada se ela estiver registrando somente as verificações de status do sistema, pois as verificações de status da instância resultarão na cópia da AMI sobre uma réplica exata do sistema operacional com problema. Depois de confirmar a mensagem de status, crie a AMI e execute uma nova instância usando a nova AMI.

Console

Para criar uma instância de substituição usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Na página Create image (Criar imagem), faça o seguinte:

   a. Digite um nome e uma descrição para a AMI.

   b. Escolha Sem reinicialização.

   c. Escolha Create Image (Criar imagem).

   Para ter mais informações, consulte the section called “Criação de uma AMI usando uma instância”.
5. Execute uma nova instância a partir da AMI e verifique se a instância nova está funcionando.
6. Selecione a instância travada e escolha Actions (Ações), Instance state (Estado da instância) e Terminate (Encerrar). Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

AWS CLI

Para criar uma instância de substituição usando a CLI

1. Crie uma AMI da instância travada usando o comando create-image (AWS CLI) e a opção `--no-reboot` da seguinte forma:

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. Execute uma nova instância da AMI usando o comando run-instances (AWS CLI) da seguinte forma:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large
 --key-name MyKeyPair --security-groups MySecurityGroup
```

3. Verifique se a nova instância está funcionando.
4. Encerre a instância travada usando o comando terminate-instances (AWS CLI) da seguinte forma:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Caso você não consiga criar uma AMI a partir da instância, conforme descrito no procedimento anterior, configure uma instância de substituição da seguinte forma:

(Alternativa) Para criar uma instância de substituição usando o console

1. Selecione a instância e escolha Description (Descrição), Block devices (Dispositivos de bloco). Selecione cada volume e anote o ID do volume. Note qual é o volume do dispositivo raiz.
2. No painel de navegação, escolha Volumes. Selecione cada volume para a instância e escolha Ações, Criar snapshot.
3. No painel de navegação, selecione Snapshots. Selecione o snapshot que você acabou de criar, e escolha Ações, Criar volume.
4. Execute uma instância com o mesmo sistema operacional da instância travada. Observe o ID do volume e o nome do dispositivo de seu volume do dispositivo raiz.
5. No painel de navegação, escolha Instances (Instâncias), selecione a instância que acabou de executar e escolha Instance state (Estado da instância) e Stop instance (Parar instância).

6. No painel de navegação, selecione Volumes, selecione o volume do dispositivo raiz da instância parada e escolha Ações, Separar volume.
7. Selecione o volume do dispositivo raiz de que você criou usando a instância presa, selecione Actions (Actions), Attach Volume (Associar volume) e associe-o à nova instância como volume raiz (usando o nome do dispositivo que você anotou). Associe todos os volumes adicionais não raiz à instância.
8. No painel de navegação, selecione Instâncias e selecione a instância de substituição. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Verifique se a instância está trabalhando.
9. Selecione a instância travada e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância). Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

Solucionar problemas de encerramento (desativação) da instância

Você não paga por nenhum uso de instância enquanto ela não estiver no estado `running`. Em outras palavras, ao encerrar uma instância, você para de ser cobrado por ela assim que o estado mudar para `shutting-down`.

A instância é encerrada imediatamente

Vários problemas podem fazer com que a sua instância seja encerrada imediatamente na inicialização. Consulte A instância é encerrada imediatamente para obter mais informações.

Encerramento atrasado da instância

Se sua instância permanecer no estado `shutting-down` por mais do que alguns minutos, ela poderá ser atrasada porque os scripts de desativação estão sendo executados pela instância.

Outra causa possível é um problema com o computador host subjacente. Se sua instância permanecer no estado `shutting-down` por várias horas, o Amazon EC2 a tratará como uma instância travada e a encerrará à força.

Se parecer que sua instância está travada no término e tiverem se passado muitas horas, publique uma solicitação de ajuda no AWS re:Post. Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que já tomou. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no Atendimento ao cliente.

Instância encerrada ainda sendo exibida

Depois de encerrar uma instância, ela permanecerá visível por um breve período antes de ser excluída. O estado mostra `terminated`. Se a entrada não for excluída depois de várias horas, entre em contato com o Suporte.

Erro: a instância não pode ser encerrada. Modifique seu atributo de instância 'disableApiTermination'

Se você tentar encerrar uma instância e receber a mensagem de erro `The instance instance_id may not be terminated. Modify its 'disableApiTermination' instance attribute`, isso indica que a instância foi habilitada para proteção contra encerramento. A proteção contra encerramento impede que a instância seja encerrada acidentalmente. Para ter mais informações, consulte Habilitar a proteção contra encerramento.

Você deve desativar a proteção contra encerramento antes de encerrar a instância.

Para desativar a proteção contra encerramento usando o console do Amazon EC2, selecione a instância e escolha Ações, Configurações da instância, Alterar proteção contra encerramento.

Para desabilitar a proteção contra encerramento via AWS CLI, use o comando a seguir.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-
termination
```

Instâncias executadas ou encerradas automaticamente

De modo geral, os comportamentos a seguir indicam que você usou o Amazon EC2 Auto Scaling, a frota do EC2 ou a frota spot para escalar os recursos de computação automaticamente com base nos critérios que você definiu.

- Você encerra uma instância e uma nova instância é iniciada automaticamente.
- Você inicia uma instância e uma de suas instâncias é encerrada automaticamente.
- Você interrompe uma instância e ela é encerrada e uma nova instância é iniciada automaticamente.

Para interromper a escalabilidade automática, consulte o Guia do usuário do Amazon EC2 Auto Scaling, EC2 Fleet ou Criar uma solicitação de frota spot.

Solução de problemas de instâncias do Linux com falhas nas verificações de status

> **Note**
>
> Este tópico se aplica somente a instâncias do Linux.

As informações apresentadas a seguir podem ajudar você a solucionar problemas caso sua instância do Linux apresente falhas em uma verificação de status. Determine primeiro se seus aplicativos exibem quaisquer problemas. Se você verificar que a instância não está executando seus aplicativos como esperado, analise as informações de verificação de status e os logs do sistema.

Para obter exemplos de problemas que podem causar falha nas verificações de status, consulte Verificações de status para as instâncias.

Tópicos

- Analisar informações de verificação de status
- Recuperar os logs do sistema
- Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux
- Sem memória: encerrar processo
- ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)
- Erro de E/S (falha de dispositivo de blocos)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)
- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)
- "FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)
- ERRO Kernel inválido (kernel incompatível com EC2)
- fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado)
- Erro geral ao montar os sistemas de arquivos (falha na montagem)

- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)
- XENBUS: Dispositivo sem driver…
- …dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)
- O fsck morreu com status de saída… (Dispositivo ausente)
- Prompt do GRUB (grubdom>)
- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

Analisar informações de verificação de status

Para investigar instâncias prejudicadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. No painel de detalhes, escolha Status e alarmes para ver os resultados individuais de todas as Verificações de status do sistema e as Verificações de status da instância.

Se uma verificação do status do sistema falhar, é possível tentar uma das opções a seguir:

- Crie um alarme de recuperação da instância. Para obter mais informações, consulte Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância.
- Se você alterou o tipo de instância para uma instância desenvolvida no AWS Nitro System, as verificações de status apresentarão falhas se você migrar de uma instância que não tenha os drivers ENA e NVMe necessários. Para obter mais informações, consulte Compatibilidade para alterar o tipo de instância.
- Para uma instância usando AMI baseada no Amazon EBS, pare e reinicie a instância.
- Para uma instância usando uma AMI com armazenamento de instâncias, encerre a instância e execute uma substituição.

- Espere o Amazon EC2 resolver o problema.
- Publique seu problema no AWS re:Post.
- Se sua instância está em um grupo do Auto Scaling, o serviço do Amazon EC2 Auto Scaling executa uma instância de substituição automaticamente. Para obter mais informações, consulte Verificações de integridade de instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.
- Recupere o log do sistema e procure erros.

Recuperar os logs do sistema

Se uma verificação de status da instância falhar, será possível reinicializar a instância e recuperar os logs do sistema. Os logs podem revelar um erro que pode ajudar você a resolver o problema. Reinicializar limpa as informações desnecessária dos logs.

Para reinicializar uma instância e recuperar o log do sistema

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Escolha Instance state (Estado da instância) e Reboot instance (Reinicializar instância). Pode demorar alguns minutos para a instância reinicializar.
4. Verifique o problema ainda existe; em alguns casos, reinicializar pode resolver o problema.
5. Quando a ação estiver no estado `running`, escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
6. Revise o log que aparece na tela e use a lista de declarações conhecidas de erro do log do sistema, abaixo, para solucionar seu problema.
7. Se seu problema não for resolvido, você pode publicar seu problema no AWS re:Post.

Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux

Para instâncias do Linux que apresentaram falhas na verificação de status da instância, como a verificação de acessibilidade da instância, verifique se você seguiu as etapas acima para recuperar o log do sistema. A lista a seguir contém alguns erros comuns no log do sistema e ações sugeridas que é possível utilizar para resolver o problema de cada erro.

Erros de memória

- Sem memória: encerrar processo
- ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)

Erros do dispositivo

- Erro de E/S (falha de dispositivo de blocos)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)

Erros de kernel

- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)
- "FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)
- ERRO Kernel inválido (kernel incompatível com EC2)

Erros do sistema de arquivos

- fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado)
- Erro geral ao montar os sistemas de arquivos (falha na montagem)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)
- XENBUS: Dispositivo sem driver…
- …dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)
- O fsck morreu com status de saída… (Dispositivo ausente)

Erros do sistema operacional

- Prompt do GRUB (grubdom>)

- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

Sem memória: encerrar processo

O erro de falta de memória é indicado por uma entrada no log de sistema semelhante à exibida abaixo.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Possível causa

Memória exaurida

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseada no Amazon EBS	Execute um destes procedimentos: • Pare a instância, modifique-a para usar um tipo de instância diferente e inicie-a novamente. Por exemplo, um tipo de instância maior ou otimizado para memória. • Reinicialize a instância para ela retornar ao status não prejudicado. O problema provavelmente ocorrerá outra vez, a menos que você altere o tipo de instância.
Com armazenamento de instâncias	Execute um destes procedimentos:

Para este tipo de instância	Faça o seguinte
	• Encerre a instância e execute uma nova instância, especificando um tipo de instância diferente. Por exemplo, um tipo de instância maior ou otimizado para memória. • Reinicialize a instância para ela retornar ao status não prejudicado. O problema provavelmente ocorrerá outra vez, a menos que você altere o tipo de instância.

ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)

As falhas de atualização do gerenciamento de memória são indicadas por uma entrada no logo do sistema semelhante à seguinte:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Possível causa

Problema com Amazon Linux

Ação sugerida

Publique seu problema nos Fóruns de desenvolvedores ou entre em contato com o AWS Support.

Erro de E/S (falha de dispositivo de blocos)

Um erro de entrada/saída é indicado por uma entrada no log do sistema semelhante ao exemplo a seguir:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	Um volume do Amazon EBS com falha
Com armazenamento de instâncias	Uma unidade física com falha

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume. 3. Tentativa de recuperar o volume. **Note** É boa prática tirar um snapshot dos seus volumes do Amazon EBS com frequência. Isso diminui drasticam ente o risco de perda de dados como resultado da falha. 4. Reassocie o volume à instância. 5. Inicie a instância.
Com armazenamento de instâncias	Encerre a instância e execute uma nova instância. **Note** Os dados não podem ser recuperados. Recupere os backups. **Note** É uma boa prática usar Amazon S3 ou Amazon EBS para backup. Os volumes de armazenamento de instâncias estão

Para este tipo de instância	Faça o seguinte
	diretamente vinculados a um único host e a falhas únicas de disco.

ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)

Um erro de entrada/saída no dispositivo é indicado por uma entrada no log do sistema semelhante ao exemplo a seguir:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	Um volume do Amazon EBS com falha
Com armazenamento de instâncias	Uma unidade física com falha

Ação sugerida

Encerre a instância e execute uma nova instância.

Para uma instância baseada no Amazon EBS, é possível recuperar os dados de um snapshot recente ao criar uma imagem a partir de deles. Alguns dados adicionados depois do snapshot não podem ser recuperados.

request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo. Usar um kernel instável ou antigo do Linux (por exemplo, 2.6.16-xenU) pode causar uma condição de loop interminável no startup.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use um kernel mais novo, baseado em GRUB ou estático, usando uma das seguintes opções:

Para este tipo de instância	Faça o seguinte
	Opção 1: Encerre a instância e execute uma nova, especificando os parâmetros `-kernel` e `-ramdisk`. Opção 2: 1. Pare a instância. 2. Modifique os atributos de kernel e ramdisk para usar um kernel mais recente. 3. Inicie a instância.
Com armazenamento de instâncias	Encerre a instância e execute uma nova, especificando os parâmetros `-kernel` e `-ramdisk`.

"FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Possíveis causas

Kernel e userland incompatíveis

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir:

Para este tipo de instância	Faça o seguinte
	1. Pare a instância. 2. Modifique a configuração para usar um kernel mais recente. 3. Inicie a instância.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Crie uma AMI que use um kernel mais recente. 2. Encerre a instância. 3. Execute uma nova instância com base na AMI criada.

"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
```

```
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Possíveis causas

Uma ou mais das condições a seguir podem causar esse problema:

- Ramdisk ausente
- Módulos corretos do ramdisk ausentes
- Volume do dispositivo raiz do Amazon EBS não associado corretamente como `/dev/sda1`

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Selecione o ramdisk corrigido para o volume do Amazon EBS. 2. Pare a instância. 3. Desanexe o volume e repare-o. 4. Associe o volume à instância.

Para este tipo de instância	Faça o seguinte
	5. Inicie a instância. 6. Modifique a AMI para usar o ramdisk corrigido.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Encerre a instância e execute uma nova instância com o ramdisk correto. 2. Crie uma nova AMI com o ramdisk correto.

ERRO Kernel inválido (kernel incompatível com EC2)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Possíveis causas

Uma ou ambas as condições a seguir podem causar esse problema:

- O kernel fornecido não é compatível com GRUB
- O kernel de fallback não existe

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância. 2. Substitua por um kernel em funcionamento. 3. Instale um kernel de fallback. 4. Modifique a AMI corrigindo o kernel.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Encerre a instância e execute uma nova instância com o kernel correto. 2. Crie uma AMI com o kernel correto. 3. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]
```

```
Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Possíveis causas

- Existe um bug nas definições de /etc/fstab do sistema de arquivos do ramdisk
- Definições do sistema de arquivos com configuração errada em /etc/fstab
- Unidade ausente/com falha

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância, separe o volume do dispositivo raiz, repare/modifique /etc/fstab o volume, associe o volume à instância e inicie a instância. 2. Corrija o ramdisk para incluir o /etc/fstab modificado (se aplicável). 3. Modifique as AMIs para usar um ramdisk mais recente. O sexto campo do fstab define os requisitos de disponibilidade da montagem – um valor diferente de zero implica que um fsck será feito nesse volume e deve ter sucesso. Usar esse campo pode ser problemático no Amazon EC2, pois a falha tipicamente resulta em um prompt do console interativo que não está disponíve l atualmente no Amazon EC2. Tenha cuidado com esse recurso e leia a man page do Linux para fstab.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Encerre a instância e execute uma nova instância. 2. Separe todos os volumes do Amazon EBS com erro e a instância de reinicialização. 3. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

Erro geral ao montar os sistemas de arquivos (falha na montagem)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	• Volume do Amazon EBS destacado ou com falha. • Sistema de arquivos corrompido. • Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).
Com armazenamento de instâncias	• Uma unidade com falha. • Um sistema de arquivos corrompido. • Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume de raiz. 3. Associe o volume do dispositivo raiz a uma instância de trabalho conhecida. 4. Execute uma verificação no sistema de arquivos (fsck -a /dev/...). 5. Corrija todos os erros. 6. Separe o volume de instância de trabalho conhecida. 7. Associe o volume à instância parada. 8. Inicie a instância.

Para este tipo de instância	Faça o seguinte
	9. Verifique novamente o status da instância.
Com armazenamento de instâncias	Faça uma das coisas a seguir: • Execute uma nova instância. • (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	• Dispositivo não associado corretamente. • O dispositivo raiz não foi associado no ponto correto do dispositivo. • O sistema de arquivos não está no formato esperado. • Uso do kernel de legado (por exemplo, 2.6.16-XenU).

Tipo de instância	Possível causa
	• Uma atualização de kernel recente na sua instância (atualização defeituosa ou bug de atualização)
Com armazenamento de instâncias	Falha no dispositivo de hardware.

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseada no Amazon EBS	Execute um destes procedimentos: • Pare e reinicie a instância. • Modifique o volume do dispositivo raiz para associar no ponto correto do dispositivo, possível /dev/sda1 em vez de /dev/sda. • Pare e modifique para usar o kernel moderno. • Consulte a documentação para sua distribui ção Linux para verificar bugs conhecidos da atualização. Altere ou reinstale o kernel.
Com armazenamento de instâncias	Encerre a instância e execute uma nova instância usando um kernel moderno.

Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
```

```
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Possíveis causas

- Driver do dispositivo de blocos virtual ausente ou configurado incorretamente
- Conflito de enumeração de dispositivos (sda versus xvda ou sda em vez de sda1)
- Escolha incorreta do kernel da instância

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume. 3. Corrija o problema de mapeamento de dispositivos. 4. Inicie a instância. 5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.
Com armazenamento de instâncias	Use o procedimento a seguir:

Para este tipo de instância	Faça o seguinte
	1. Crie nova AMI com a correção apropriada (mapeie o dispositivo de blocos corretame nte). 2. Encerre a instância e execute uma nova a partir da AMI criada.

XENBUS: Dispositivo sem driver…

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Possíveis causas

- Driver do dispositivo de blocos virtual ausente ou configurado incorretamente
- Conflito de enumeração de dispositivos (sda versus xvda)
- Escolha incorreta do kernel da instância

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume. 3. Corrija o problema de mapeamento de dispositivos. 4. Inicie a instância. 5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Crie uma AMI com a correção apropriada (mapeie o dispositivo de blocos corretame nte). 2. Encerre a instância e execute uma nova usando a AMI criada.

…dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Possíveis causas

Tempo de verificação do sistema de arquivos passado; uma verificação do sistema de arquivos está sendo forçada.

Ações sugeridas

- Espere até que a verificação do sistema de arquivos seja concluída. Uma verificação do sistema de arquivos pode demorar bastante, dependendo do tamanho do sistema de arquivos raiz.
- Modifique seus sistemas de arquivos para remover a obrigatoriedade de verificação do sistema de arquivos (fsck) usando tune2fs ou ferramentas apropriadas para seu sistema de arquivos.

O fsck morreu com status de saída… (Dispositivo ausente)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Possíveis causas

- Ramdisk procurando unidade ausente
- Verificação de consistência do sistema de arquivos forçada
- Unidade falha ou separada

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Teste uma ou mais das opções a seguir para resolver o problema: • Pare a instância, associe o volume a uma instância em execução existente. • Execute manualmente verificações de consistência.

Para este tipo de instância	Faça o seguinte
	• Conserte o ramdisk para incluir utilitários relevantes. • Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados).
Com armazenamento de instâncias	Teste uma ou mais das opções a seguir para resolver o problema: • Reempacote o ramdisk com as ferramentas corretas. • Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados). • Encerre a instância e execute uma nova instância. • (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

Prompt do GRUB (grubdom>)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]
```

```
grubdom>
```

Possíveis causas

Tipo de instância	Possíveis causas
Baseado em Amazon EBS	• Arquivo de configuração do GRUB ausente. • Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente. • Sistema de arquivos não compatível usado para armazenar seu arquivo de configuração de GRUB (por exemplo, convertendo o sistema de arquivos raiz a um tipo que não é compatível com uma versão anterior do GRUB).
Com armazenamento de instâncias	• Arquivo de configuração do GRUB ausente. • Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente. • Sistema de arquivos não compatível usado para armazenar seu arquivo de configuração de GRUB (por exemplo, convertendo o sistema de arquivos raiz a um tipo que não é compatível com uma versão anterior do GRUB).

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Opção 1: Modifique a AMI e reexecute a instância:

Para este tipo de instância	Faça o seguinte
	1. Modifique as AMIs de origem para criar um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst). 2. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário. 3. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição). 4. Encerre a instância e execute uma nova usando a AMI criada. Opção 2: Corrija a instância existente: 1. Pare a instância. 2. Separe o sistema de arquivos-raiz. 3. Associe o sistema de arquivos raiz para uma instância de trabalho conhecida. 4. Monte o sistema de arquivos. 5. Crie o arquivo de configuração do GRUB. 6. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário. 7. Separe o sistema de arquivos. 8. Associe à instância original. 9. Modifique o atributo do kernel para usar a imagem adequada do GRUB (1º disco ou 1ª partição no 1ª disco). 10. Inicie a instância.

Para este tipo de instância	Faça o seguinte
Com armazenamento de instâncias	Opção 1: Modifique a AMI e reexecute a instância: 1. Crie a nova AMI com um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst). 2. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição). 3. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário. 4. Encerre a instância e execute uma nova usando a AMI criada. Opção 2: Encerre a instância e execute uma nova, especificando o kernel correto. **Note** Para recuperar dados da instância existente, entre em contato com o AWS Support.

Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
```

```
[FAILED]

Starting auditd: [  OK  ]
```

Possíveis causas

Há uma interface MAC hard-coded na configuração da AMI

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseada no Amazon EBS	Execute um destes procedimentos: • Modifique a AMI para remover o hard code e reexecute a instância. • Modifique a instância para remover o endereço MAC hard-coded. OU Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume de raiz. 3. Associe o volume a outra instância e modifique o volume para remover o endereço MAC hard-coded. 4. Associe o volume à instância original. 5. Inicie a instância.
Com armazenamento de instâncias	Execute um destes procedimentos: • Modifique a instância para remover o endereço MAC hard-coded. • Encerre a instância e execute uma nova instância.

Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Possíveis causas

O SELinux foi habilitado por engano:

- O kernel fornecido não é compatível com GRUB
- O kernel de fallback não existe

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 1. Pare a instância com falha. 2. Separe o volume do dispositivo raiz da instância com falha. 3. Associe o volume do dispositivo raiz a outra instância do Linux em execução (posterio rmente chamada de instância de recuperaç ão). 4. Conecte-se à instância de recuperação e monte o volume do dispositivo raiz da instância falha. 5. Desabilite o SELinux no volume do dispositi vo raiz montado. Esse processo varia nas distribuições de Linux; para obter mais

Para este tipo de instância	Faça o seguinte
	informações, consulte a documentação específica do seu SO. **Note** Em alguns sistemas, você desabilita o SELinux configurando `SELINUX=disabled` no arquivo `/mount_point/etc/sysconfig/selinux`, onde *mount_point* é o local onde você montou o volume da sua instância de recuperação. 6. Desmonte e separe o volume do dispositivo raiz da instância de recuperação e reassocie-o à instância original. 7. Inicie a instância.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Encerre a instância e execute uma nova instância. 2. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
```

```
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Possíveis causas

- O dispositivo de blocos não está conectado à instância
- Essa instância está usando um kernel de uma instância antiga

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseada no Amazon EBS	Execute um destes procedimentos: • Modifique a AMI e a instância para usar um kernel moderno e reexecutar a instância. • Reinicialize a instância.
Com armazenamento de instâncias	Execute um destes procedimentos: • Encerre a instância. • Modifique as AMIs para usar um kernel moderno e execute uma nova instância usando essa AMI.

Solução de problemas de inicialização da instância do Linux usando o volume errado

> **Note**
>
> Este tópico de solução de problemas se aplica somente a instâncias do Linux.

Em algumas situações, é possível descobrir que um volume além do volume associado a `/dev/xvda` ou `/dev/sda` tornou-se o volume do dispositivo raiz da sua instância. Isso pode acontecer quando você associar o volume do dispositivo raiz de outra instância, ou um volume criado a partir

do snapshot de um volume do dispositivo raiz, a uma instância com um volume do dispositivo raiz existente.

Isso ocorre por conta de como funciona o ramdisk inicial no Linux. O volume definido como `/` em `/etc/fstab` é escolhido e, em algumas distribuições, isso é determinado pelo rótulo anexado à partição do volume. Mais especificamente, você descobrirá que seu `/etc/fstab` parece com o seguinte:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Se você verificar os rótulos dos dois volumes, verá que ambos contêm o rótulo `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

Neste exemplo, pode acontecer de `/dev/xvdf1` acabar sendo o dispositivo raiz no qual sua instância se inicia após a execução inicial do ramdisk, em vez de o volume `/dev/xvda1` do qual você pretendeu inicializar. Para resolver isso, use o mesmo comando e2label para alterar o rótulo do volume associado do qual você não deseja inicializar.

Em alguns casos, especificar um UUID em `/etc/fstab` pode resolver isso. No entanto, se ambos os volumes vierem do mesmo snapshot ou o secundário for criado a partir de um snapshot do volume primário, eles compartilharão um UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Para alterar a identificação de um volume ext4 associado

1. Use o comando e2label para alterar a identificação do volume para outra coisa além de `/`.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1 old/
```

2. Verifique se o volume tem a nova identificação.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1
old/
```

Para alterar a identificação de um volume xfs associado

- Use o comando xfs_admin para alterar a identificação do volume para outra coisa além de /.

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

Depois de alterar a identificação do volume como mostrado, será possível reiniciar a instância e selecionar o volume adequado pelo ramdisk inicial quando a instância for inicializada.

> **Important**
>
> Se você pretende desanexar o volume com o novo rótulo e devolvê-lo a outra instância para ser usado como o volume raiz, deverá executar novamente o procedimento acima e alterar o rótulo do volume de volta ao seu valor original. Caso contrário, a outra instância não é inicializada porque o disco ramdisk não consegue encontrar o volume com o rótulo /.

Solução de problemas de Sysprep com instâncias do Windows

> **Note**
>
> Este tópico de solução de problemas se aplica somente a instâncias do Windows.

Se você tiver problemas ou receber mensagens de erro durante as preparações da imagem, veja os logs a seguir. A localização do log depende se você está executando EC2Config, EC2Launch v1 ou EC2Launch v2 com Sysprep.

- `%WINDIR%\Panther\Unattendgc`(EC2Config, EC2Launch v1 e EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther`(EC2Config, EC2Launch v1 e EC2Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (somente EC2Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs` (somente EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (somente EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (somente EC2Launch v2)

Se você receber uma mensagem de erro durante a preparação de imagem com Sysprep, o SO poderá não ser alcançável. Para analisar os arquivos de log, é preciso primeiro parar a instância, associar o volume do dispositivo raiz a outra instância íntegra como volume secundário e analisar os logs mencionados anteriormente no volume secundário. Para obter mais informações sobre a finalidade dos arquivos de log por nome, consulte Arquivos de log relacionados à configuração do Windows na documentação da Microsoft.

Se você encontrar erros no arquivo de log Unattendgc, use a Ferramenta de pesquisa de erro da Microsoft para obter mais detalhes sobre o erro. O problema a seguir relatado no arquivo de log Unattendgc é geralmente o resultado de um ou mais perfis de usuário corrompidos na instância:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Há duas opções para resolver o problema:

Opção 1

Use o Regedit na instância para pesquisar pela chave a seguir. Verifique se não há chaves do registro de perfil para um usuário excluído.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
\ProfileList\
```

Opção 2

1. Edite o arquivo relevante da seguinte forma:

- Windows Server 2012 R2 e anterior – Edite o arquivo de resposta do EC2Config (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
- Windows Server 2016 e 2019 – Edite o arquivo de resposta unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
- Windows Server 2022 – Edite o arquivo de resposta unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).

2. Fazer `<CopyProfile>true</CopyProfile>` alteração `<CopyProfile>false</CopyProfile>`.
3. Execute novamente o Sysprep. Observe que essa mudança de configuração excluirá o perfil de usuário do administrador incorporado após o Sysprep concluir.

Usar o EC2Rescue para Linux

O EC2Rescue para Linux é uma ferramenta de código aberto fácil de usar que pode ser executada na instância Linux do Amazon EC2 para diagnosticar e resolver problemas comuns usando sua biblioteca de mais de 100 módulos. Alguns casos de uso generalizados para o EC2Rescue para Linux incluem reunir syslog e logs do gerenciador de pacotes, coletar dados de utilização de recursos e diagnosticar/corrigir parâmetros problemáticos de kernel conhecidos e problemas comuns de OpenSSH.

O runbook `AWSSupport-TroubleshootSSH` instala oEC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Para obter mais informações e para executar essa automação, consulte AWS Support-TroubleshootSSH.

Se você estiver usando uma instância do Windows, consulte the section called “EC2Rescue for Windows Server”.

Conteúdo

- Instalar o EC2Rescue para Linux
- Trabalhar com EC2Rescue para Linux
- Desenvolver módulos do EC2Rescue

Instalar o EC2Rescue para Linux

A ferramenta EC2Rescue para Linux pode ser instalada em uma instância Linux do Amazon EC2 que atenda aos seguintes pré-requisitos.

Pré-requisitos

- Sistemas operacionais com suporte:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Requisitos de software:
  - Python 2.7.9+ ou 3.2+

O runbook `AWSSupport-TroubleshootSSH` instala oEC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Para obter mais informações e para executar essa automação, consulte AWS Support-TroubleshootSSH.

Se o seu sistema tem a versão necessária do Python, você pode instalar a compilação padrão. Caso contrário, você pode instalar a compilação do pacote, incluindo uma cópia mínima do Python.

Para instalar a compilação padrão

1. Em uma instância Linux de trabalho, faça download da ferramenta EC2Rescue para Linux:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
   ```

2. (Opcional) Antes de continuar, você também pode verificar a assinatura do arquivo de instalação do EC2Rescue para Linux. Para obter mais informações, consulte (Opcional) Verifique a assinatura de EC2Rescue para Linux.
3. Faça download do arquivo hash sha256:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
   ```

4. Verifique a integridade do tarball:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Desembale o tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verifique instalação listando o arquivo de ajuda:

```
cd ec2rl-<version_number>
./ec2rl help
```

Para instalar a compilação do pacote

Para obter um link para download e uma lista de limitações, consulte EC2Rescue para Linux no GitHub.

(Opcional) Verifique a assinatura de EC2Rescue para Linux

Veja a seguir o processo recomendado para verificação da validade do pacote do EC2Rescue para Linux para sistemas operacionais Linux.

Sempre que baixar um aplicativo da Internet, recomendamos que você autentique a identidade do fornecedor do software e verifique se o aplicativo não foi alterado ou corrompido desde que foi publicado. Isso protege você contra a instalação de uma versão do aplicativo que contenha um vírus ou outro código mal-intencionado.

Se depois de executar as etapas neste tópico, você determinar que o software do EC2Rescue para Linux está alterado ou corrompido, não execute o arquivo de instalação. Em vez disso, entre em contato com o Amazon Web Services.

Os arquivos do EC2Rescue para Linux para os sistemas operacionais baseados em Linux são assinados usando o GnuPG, uma implementação de código aberto do padrão OpenPGP (Pretty Good Privacy) para assinaturas digitais seguras. O GnuPG (também conhecido como GPG) fornece autenticação e verificação de integridade por meio de uma assinatura digital. A AWS publica uma chave pública e assinaturas que você pode usar para verificar o pacote EC2Rescue para Linux que foi obtido por download. Para obter mais informações sobre o PGP e o GnuPG (GPG), consulte http://www.gnupg.org.

A primeira etapa é estabelecer confiança com o fornecedor do software. Faça download da chave pública do fornecedor do software, verifique se o proprietário da chave pública é quem afirma ser e, em seguida, adicione a chave pública ao seu keyring. O keyring é um conjunto de chaves públicas conhecidas. Após estabelecer a autenticidade da chave pública, você pode usá-la para verificar a assinatura do aplicativo.

Tarefas

- Instalar as ferramentas do GPG
- Autenticar e importar a chave pública
- Verificar a assinatura do pacote

Instalar as ferramentas do GPG

Se o seu sistema operacional for Linux ou Unix, as ferramentas do GPG já poderão estar instaladas. Para testar se as ferramentas estão instaladas no sistema, digite gpg2 em um prompt de comando. Se as ferramentas do GPG estiverem instaladas, um prompt de comando do GPG será exibido. Se as ferramentas do GPG não estiverem instaladas, uma mensagem de erro será exibida informando que o comando não pode ser encontrado. Você pode instalar o pacote GnuPG a partir de um repositório.

Para instalar as ferramentas do GPG no Linux baseado em Debian

- Em um terminal, execute o comando a seguir:

```
apt-get install gnupg2
```

Para instalar as ferramentas do GPG no Linux baseado em Red Hat

- Em um terminal, execute o comando a seguir:

```
yum install gnupg2
```

Autenticar e importar a chave pública

A próxima etapa do processo é autenticar a chave pública do EC2Rescue para Linux e adicioná-la como uma chave confiável ao seu keyring do GPG.

Para autenticar e importar a chave pública do EC2Rescue para Linux

1. Em um aviso de comando, use o seguinte comando para obter uma cópia de nossa chave de compilação de público GPG:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. Em um prompt de comando no diretório onde você salvou `ec2rl.key`, use o comando a seguir para importar a chave pública do EC2Rescue para Linux para seu keyring:

   ```
   gpg2 --import ec2rl.key
   ```

   O comando retorna resultados semelhantes a:

   ```
   gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
   gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
    imported
   gpg: Total number processed: 1
   gpg:               imported: 1  (RSA: 1)
   ```

Verificar a assinatura do pacote

Depois de instalar as ferramentas do GPG, autenticar e importar a chave pública do EC2Rescue para Linux e verificar se a chave pública do EC2Rescue para Linux é confiável, você estará pronto para verificar a assinatura do script de instalação do EC2Rescue para Linux.

Para verificar o script de instalação da assinatura do EC2Rescue para Linux

1. Em um prompt de comando, execute o comando a seguir para baixar o arquivo de assinatura para o script de instalação:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifique a assinatura executando o comando a seguir em um prompt no diretório onde você salvou o `ec2rl.tgz.sig` e o arquivo de instalação EC2Rescue para Linux. Ambos os arquivos devem estar presentes.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

A saída deve parecer com algo semelhante ao seguinte:

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
     Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Se a saída contém a frase `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, isso significa que a assinatura foi confirmada com êxito e você pode dar continuidade à execução do script de instalação do EC2Rescue para Linux.

Se a saída inclui a frase `BAD signature`, verifique se você executou o procedimento corretamente. Se você continuar a receber essa resposta, entre em contato com o Amazon Web Services e não execute o arquivo de instalação que baixou anteriormente.

Veja a seguir os detalhes sobre as advertências que talvez sejam exibidas:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Isso se refere ao seu nível pessoal de confiança de que você tem uma chave pública autêntica para o EC2Rescue para Linux. A situação ideal seria você visitar um escritório do Amazon Web Services e receber uma chave em pessoa. No entanto, é mais frequente você baixá-la de um site. Nesse caso, o site é um Amazon Web Services.
- gpg2: no ultimately trusted keys found. Isso significa que a chave específica não é "essencialmente confiável" (por você ou por outras pessoas que você confia).

Para obter mais informações, consulte http://www.gnupg.org.

Trabalhar com EC2Rescue para Linux

Veja a seguir as tarefas comuns que você pode realizar para começar a usar essa ferramenta.

Tarefas

- Executar EC2Rescue para Linux
- Fazer upload dos resultados
- Criar backups

- Obter ajuda

Executar EC2Rescue para Linux

Você pode executar o EC2Rescue para Linux conforme mostrado nos exemplos a seguir.

Example Exemplo: executar todos os módulos

Para executar todos os módulos, execute o EC2Rescue para Linux sem opções:

```
./ec2rl run
```

Alguns módulos exigem o acesso raiz. Se você não é um usuário raiz, use o comando sudo para executar esses módulos da seguinte maneira:

```
sudo ./ec2rl run
```

Example Exemplo: executar um módulo específico

Para executar apenas módulos específicos, use o parâmetro --only-modules:

```
./ec2rl run --only-modules=module_name --arguments
```

Por exemplo, este comando executa o módulo dig para consultar o domínio `amazon.com`:

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example Exemplo: visualizar os resultados

Você pode visualizar os resultados em `/var/tmp/ec2rl`:

```
cat /var/tmp/ec2rl/logfile_location
```

Por exemplo, visualize o arquivo de log para o módulo dig:

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

Fazer upload dos resultados

Se o AWS Support solicitou os resultados, ou para compartilhar os resultados de um bucket do S3, carregue-os usando a ferramenta da CLI EC2Rescue para Linux. A saída dos comandos do EC2Rescue para Linux devem fornecer os comandos que você precisa usar.

Example Exemplo: Carregar resultados para AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example Exemplo: carregar os resultados em um bucket do S3

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

Para obter mais informações sobre como gerar pre-signed URLs para o Amazon S3, consulte Fazer upload de objetos usando pre-signed URLs.

Criar backups

Crie um backup para sua instância, um ou mais volumes, ou um ID de dispositivo específico usando os seguintes comandos.

Example Exemplo: fazer backup de uma instância usando uma imagem de máquina da Amazon (AMI)

```
./ec2rl run --backup=ami
```

Example Exemplo: fazer backup de todos os volumes associados à instância

```
./ec2rl run --backup=allvolumes
```

Example Exemplo: fazer backup de um volume específico

```
./ec2rl run --backup=volumeID
```

Obter ajuda

O EC2Rescue para Linux inclui um arquivo de ajuda que fornece informações e a sintaxe para cada comando disponível.

Example Exemplo: exibir a ajuda geral

```
./ec2rl help
```

Example Exemplo: listar os módulos disponíveis

```
./ec2rl list
```

Example Exemplo: exibir a ajuda para um módulo específico

```
./ec2rl help module_name
```

Por exemplo, use o comando a seguir para mostrar o arquivo de ajuda do módulo dig:

```
./ec2rl help dig
```

Desenvolver módulos do EC2Rescue

Os módulos são gravados em YAML, um padrão de serialização de dados. O arquivo YAML de um módulo consiste em um único documento, representando o módulo e seus atributos.

Adicionar atributos de módulo

A tabela a seguir lista os atributos de módulo disponíveis.

Atributo	Descrição
name	O nome do módulo. O nome precisa ter 18 caracteres ou menos.
versão	O número da versão do módulo.
title	Um título curto e descritivo para o módulo. Esse valor precisa ter 50 caracteres ou menos.

Atributo	Descrição

helptext	A descrição estendida do módulo. Cada linha precisa ter 75 caracteres ou menos. Se o módulo utilizar argumentos, obrigatórios ou opcionais, inclua-os no valor helptext.
	
	Por exemplo:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

posicionamento	O estágio no qual o módulo deve ser executado. Valores com suporte: • pré-diagnóstico • executar • pós-diagnóstico
linguagem	A linguagem em que o código do módulo está escrito. Valores com suporte: • bash • python **Note** O código Python deve ser compatível com o Python 2.7.9+ e o Python 3.2+.

Atributo	Descrição
correção	Indica se o módulo dá suporte a correão. Os valores compatíveis são `True` ou `False`. Os padrões do módulo de `False` se estiver ausente, tornando-o um atributo opcional para esses módulos que não dão suporte a correção.
conteúdo	A totalidade do código do script.
restrição	O nome do objeto que contém os valores de limite.
domínio	Um descritor de como o módulo é agrupado ou classificado. O conjunto de módulos incluídos usa os seguintes domínios: • aplicativo • net • os • desempenho
classe	Um descritor do tipo da tarefa executada pelo módulo. O conjunto de módulos incluídos usa as seguintes classes: • coletar (coleta a saída dos programas) • diagnosticar (é aprovado/falha com base em um conjunto de critérios) • recolher (copia os arquivos e grava em um arquivo específico)

Atributo	Descrição
distro	A lista de distribuições Linux às quais esse módulo oferece suporte. O conjunto de módulos usa as seguintes distribuições: • alami (Amazon Linux) • rhel • ubuntu • suse
obrigatório	Os argumentos necessários que o módulo está consumindo das opções de CLI.
opcional	Os argumentos opcionais que o módulo pode usar.
software	Os executáveis de software usados no módulo. Esse atributo deve especificar o software que não é instalado por padrão. A lógica do EC2Rescue para Linux garante que esses programas estejam presentes e executáveis antes de executar o módulo.
pacote	O pacote de software de origem para um executável. Esse atributo deve fornecer detalhes estendidos sobre o pacote com o software, incluindo uma URL para fazer download ou obter mais informações.
sudo	Indica se o acesso raiz é necessário para executar o módulo. Não é necessário implementar verificações sudo no script do módulo. Se o valor for verdadeiro, a lógica do EC2Rescue para Linux só executará o módulo quando o usuário que estiver executando tiver acesso raiz.

Atributo	Descrição
perfimpact	Indica se o módulo pode ter impacto significativo no desempenho no ambiente no qual ele está sendo execução. Se o valor for verdadeiro e o argumento `--perfimpact=true` não estiver presente, o módulo será ignorado.
parallelexclusive	Especifica um programa que exija exclusividade mútua. Por exemplo, todos os módulos que especificam "bpf" executados de maneira serial.

Adicionar variáveis de ambiente

A tabela a seguir lista as variáveis de ambiente disponíveis.

Variável de ambiente	Descrição
`EC2RL_CALLPATH`	O caminho para `ec2rl.py`. Esse caminho pode ser usado para encontrar o diretório lib e utilizar os módulos Python do fornecedor.
`EC2RL_WORKDIR`	O diretório tmp principal para a ferramenta de diagnóstico. Valor padrão: `/var/tmp/ec2rl` .
`EC2RL_RUNDIR`	O diretório no qual a saída é armazenada. Valor padrão: `/var/tmp/ec2rl/<date&timestamp>` .
`EC2RL_GATHEREDDIR`	O diretório raiz para colocar os dados de módulo reunidos.

Variável de ambiente	Descrição
	Valor padrão:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
`EC2RL_NET_DRIVER`	O driver em uso na primeira interface de rede não virtual, ordenada alfabeticamente, na instância. Exemplos: • xen_netfront • ixgbevf • ena
`EC2RL_SUDO`	Verdadeiro se EC2Rescue para Linux estiver em execução como raiz; caso contrário, falso.
`EC2RL_VIRT_TYPE`	O tipo de virtualização conforme fornecido pelos metadados da instância. Exemplos: • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Uma lista enumerada de interfaces no sistema. O valor é uma string que contém nomes, como `eth0eth1`, etc. É gerada pelo `functions.bash` e está disponível somente para os módulos que a originaram.

Usar sintaxe de YAML

Os seguintes itens devem ser observados ao construir os arquivos YAML do módulo:

- O hífen triplo (`---`) denota o início explícito de um documento.

- A tag `!ec2rlcore.module.Module` indica para o analisador YAML qual construtor chamar ao criar o objeto do fluxo de dados. Você pode localizar o construtor no arquivo `module.py`.
- A tag `!!str` diz para o analisador YAML não tentar determinar o tipo de dados e, em vez disso, interpretar o conteúdo como um literal de string.
- O caractere pipe (`|`) informa ao analisador YAML que o valor é um escalar de estilo literal. Nesse caso, o analisador inclui todos os espaços em branco. É importante para os módulos porque o recuo e os caracteres de nova linha são mantidos.
- O recuo padrão YAML é dois espaços, que podem ser vistos nos exemplos a seguir. Certifique-se de manter o recuo padrão (por exemplo, quatro espaços para Python) para o script e, em seguida, defina o recuo de dois espaços para todo o conteúdo no arquivo do módulo.

Exemplos de módulos

Exemplo 1 (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
```

```
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Usar o EC2Rescue for Windows Server

O EC2Rescue for Windows Server é uma ferramenta fácil de usar que você executa em uma instância do Windows Server do Amazon EC2 para diagnosticar e solucionar os possíveis problemas. A ferramenta é valiosa para coletar arquivos de log e solucionar problemas e também para pesquisar proativamente possíveis áreas de preocupação. Ele pode até examinar volumes raiz do Amazon EBS de outras instâncias e coletar logs relevantes para solucionar problemas de instâncias do Windows Server que usam esse volume.

A ferramenta EC2Rescue for Windows Server tem dois módulos diferentes: um módulo coletor de dados que coleta dados de todas as diferentes origens, e um módulo analisador que analisa os dados coletados em relação a uma série de regras predefinidas para identificar problemas e fornecer sugestões.

A ferramenta EC2Rescue para Windows Server apenas é executada em instâncias do Amazon EC2 executando o Windows Server 2012 e versões posteriores. Quando a ferramenta é iniciada, ela verifica se está sendo executada em uma instância do Amazon EC2.

O runbook `AWSSupport-ExecuteEC2Rescue` usa a ferramenta EC2Rescue para solucionar problemas e, quando possível, reparar problemas comuns de conectividade com a instância do EC2 especificada. Para obter mais informações e para executar essa automação, consulte AWSSupport-ExecuteEC2Rescue.

Se você estiver usando uma instância do Linux, consulte the section called “EC2Rescue for Linux”.

Conteúdo

- Usar a GUI EC2Rescue for Windows Server
- Usar o EC2Rescue for Windows Server com a linha de comando
- Usar o EC2Rescue for Windows Server com o Run Command do Systems Manager

Usar a GUI EC2Rescue for Windows Server

O EC2Rescue for Windows Server pode executar as seguintes análises em instâncias offline :

Opção	Descrição

Diagnostico e resgate	O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:
	• Hora do sistema
	  • RealTimeisUniversal: detecta se a chave do registro `RealTimeisUniversal` está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.
	• Firewall do Windows
	  • Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
	  • Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
	  • Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do

Opção	Descrição

	Firewall do Windows está habilitado ou desabilitado.
	
	• Desktop remoto
	  • Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado.
	  • Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada.
	  • TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo.
	
	• EC2Config (Windows Server 2012 R2 e anteriores)
	  • Installation (Instalação): detecta qual versão do EC2Config está instalada.
	  • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado.
	  • Ec2SetPassword: gera uma nova senha de administrador.
	  • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicialização da instância.
	
	• EC2Launch (Windows Server 2016 e posterior)
	  • Installation (Instalação): detecta qual versão do EC2Launch está instalada.
	  • Ec2SetPassword: gera uma nova senha de administrador.

Opção	Descrição

	• Interface de rede
	  • DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado.
	  • Ethernet detail (Detalhes da Ethernet): exibe informações sobre a versão do driver de rede, se detectado.
	  • DHCP on Ethernet (DHCP na Ethernet): detecta se o DHCP está habilitado.
	• Status da assinatura no disco
	  • Signature on disk (Assinatura em disco) e Signature on Boot Configuration Database (BCD) (Assinatura em banco de dados de configuração de inicialização): detectam se a assinatura no disco e a assinatura no BCD são iguais. Se os valores forem diferentes, o EC2Rescue tentará substitui r a assinatura no disco pela assinatura no BCD.

Restaurar	Execute uma das seguintes ações: • Last Known Good Configuration (Última configuração válida conhecida): tenta inicializ ar a instância no estado inicializável mais recente conhecido. • Restore registry from backup (Restaura r registro do backup): restaura o registro de `\Windows\System32\config\Re gBack` .
Capturar logs	Permite que você capture logs na instância para análise.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline:

Item	Descrição
Log de eventos	Coleta logs do aplicativo, do sistema e de eventos do EC2Config.
Registro	Coleta os hives `SYSTEM` e `SOFTWARE`.
Log do Windows Update	Coleta arquivos de log gerados pelo Windows Update. **Note** No Windows Server 2016 e posterior, o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).
Log do Sysprep	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
Registro de configuração da unidade	Coleta os logs da SetupAPI do Windows (`setupapi.dev.log` e `setupapi.setup.log`).
Configuração da inicialização	Coleta o hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Despejo de memória	Coleta todos os arquivos de despejo de memória existentes na instância.
Arquivo do EC2Config	Coleta os arquivos de log gerados pelo serviço EC2Config.
Arquivo do EC2Launch	Coleta os arquivos de log gerados pelos scripts do EC2Launch.

Item	Descrição
Arquivo do SSM Agent	Coleta arquivos de log gerados pelo SSM Agent e pelos logs do Patch Manager.
Arquivo ElasticGPUs do EC2	Recolhe os logs de eventos relacionados a GPUs elásticas.
ECS	Coleta logs relacionados ao Amazon ECS.
CloudEndure	Coleta arquivos de log relacionados ao agente CloudEndure.

EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas:

Item	Descrição
Informações do sistema	Coleta MSInfo32.
Resultado da política de grupo	Coleta um relatório de políticas de grupo.

Analisar uma instância offline

A opção Offline Instance é útil para a depuração de problemas de inicialização com instâncias do Windows.

Para executar uma ação em uma instância off-line

1. Em uma instância do Windows Server em execução, faça download da ferramenta EC2Rescue for Windows Server e extraia os arquivos.

   Você pode executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

2. Pare a instância com falha, se ela ainda não estiver parada.
3. Desanexe o volume raiz do EBS da instância com falha e anexe o volume a uma instância do Windows em funcionamento que tenha a EC2Rescue for Windows Server instalada.
4. Execute a ferramenta EC2Rescue for Windows Server na instância em funcionamento e escolha Offline Instance.
5. Selecione o disco do volume recém-montado e escolha Next.
6. Confirme a seleção do disco e escolha Yes.
7. Escolha a opção de instância off-line a ser executada e escolha Next.

A ferramenta EC2Rescue for Windows Server verifica o volume e coleta informações para solução de problemas com base nos arquivos de log selecionados.

Coletar dados de uma instância ativa

Você pode coletar logs e outros dados de uma instância ativa.

Para coletar dados de uma instância ativa

1. Conecte-se à sua instância do Windows.
2. Faça download da ferramenta EC2Rescue for Windows Server na instância do Windows e extraia os arquivos.

Você pode executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. Você pode habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

3. Abra o aplicativo da EC2Rescue for Windows Server e aceite o contrato de licença.
4. Escolha Next, Current instance, Capture logs.
5. Selecione os itens de dados a serem coletados e escolha Collect.... Leia o aviso e escolha Yes para continuar.
6. Escolha um nome de arquivo e um local do arquivo ZIP e escolha Save.
7. Depois que a EC2Rescue for Windows Server for concluída, escolha Open Containing Folder para visualizar o arquivo ZIP.
8. Escolha Finish.

Usar o EC2Rescue for Windows Server com a linha de comando

A interface de linha de comando (CLI) do EC2Rescue for Windows Server permite executar um plug-in do EC2Rescue for Windows Server (conhecido como “ação”) de forma programada.

O ferramenta EC2Rescue for Windows Server tem dois modos de execução:

- /online — Permite agir na instância em que o EC2Rescue for Windows Server está instalado, como coletar arquivos de log.
- /offline:<device_id>—Permite agir no volume raiz offline que está associado a uma instância separada do Amazon EC2 do Windows em que você instalou o EC2Rescue for Windows Server.

Faça download da ferramenta EC2Rescue for Windows Server na instância do Windows e extraia os arquivos. É possível visualizar o arquivo de ajuda usando o seguinte comando:

```
EC2RescueCmd.exe /help
```

O EC2Rescue for Windows Server pode executar as seguintes ações na instância do Windows do Amazon EC2:

- Ação de coleta
- Ação de salvamento
- Ação de restauração

Ação de coleta

> **Note**
>
> Você pode coletar todos os logs, um grupo inteiro de log ou um log individual dentro de um grupo.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline.

Grupo de logs	Logs disponíveis	Descrição
`all`		Coleta todos os logs disponíveis.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Coleta logs do aplicativo, do sistema e de eventos do EC2Config.

Grupo de logs	Logs disponíveis	Descrição
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Coleta todos os arquivos de despejo de memória existente s na instância.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Coleta os arquivos de log gerados pelo serviço EC2Config.
`ec2launch`	• `'Logs'` • `'Config'`	Coleta os arquivos de log gerados pelos scripts do EC2Launch.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Coleta arquivos de log gerados pelo Agente SSM e pelos logs do Patch Manager.
`sysprep`	`'Log Files'`	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Coleta os logs da SetupAPI do Windows (`setupapi.dev.log` e `setupapi.setup.log`).
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Coleta os hives `SYSTEM` e `SOFTWARE`.
`egpu`	• `'Event Log'` • `'System Files'`	Recolhe os logs de eventos relacionados a GPUs elásticas .

Grupo de logs	Logs disponíveis	Descrição
`boot-config`	`'BCDEDIT Output'`	Coleta o hive `HKEY_LOCAL_MACHINE\BCD00000000` .
`windows-update`	`'Log Files'`	Coleta arquivos de log gerados pelo Windows Update. **Note** No Windows Server 2016 e posterior, o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Coleta arquivos de log relacionados ao agente CloudEndure.

O EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas.

Grupo de logs	Logs disponíveis	Descrição
`system-info`	`'MSInfo32 Output'`	Coleta `MSInfo32`.
`gpresult`	`'GPResult Output'`	Coleta um relatório de políticas de grupo.

As seguintes opções estão disponíveis:

- /output:<outputFilePath>: localização do caminho de arquivo de destino obrigatório para salvar arquivos de log coletados no formato zip.
- /no-offline: atributo opcional usado no modo offline. Não define o volume offline após completar a ação.
- /no-fix-signature: atributo opcional usado no modo offline. Não conserta uma possível colisão de assinatura de disco após concluir a ação.

Exemplos

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server.

Exemplos de modo online

Coleta todos os logs disponíveis:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Coleta logs individuais dentro de um grupo de log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Exemplos de modo offline

Coleta todos os logs disponíveis de um volume do EBS. O volume é especificado pelo valor device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Ação de salvamento

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
`all`		
`system-time`	`'RealTimeIsUniversal'`	Hora do sistema • RealTimeisUniversal: detecta se a chave do registro `RealTimeisUniversal` está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Firewall do Windows • Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado. • Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado. • Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do Firewall do

Grupo de serviço	Ações disponíveis	Descrição
		Windows está habilitado ou desabilitado.
rdp	• 'Service Start' • 'Remote Desktop Connections' • 'TCP Port'	Desktop remoto • Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado. • Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada. • TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo.
ec2config	• 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData'	EC2Config • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado. • Ec2SetPassword: gera uma nova senha de administrador. • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicialização da instância.

Grupo de serviço	Ações disponíveis	Descrição
`ec2launch`	`'Reset Administrator Password'`	Gera uma nova senha de administrador do Windows.
`network`	`'DHCP Service Startup'`	Interface de rede • DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado.

As seguintes opções estão disponíveis:

- /level:<level>: atributo opcional para o nível de verificação que a ação deve acionar. Os valores permitidos são: `information`, `warning`, `error`, `all`. Por padrão, ele é definido como `error`.
- /check-only atributo opcional que gera um relatório, mas não faz nenhuma modificação no volume offline.

> **Note**
>
> Se o EC2Rescue para Windows Server detectar uma possível colisão de assinatura de disco, ele corrigirá a assinatura após a conclusão do processo off-line por padrão, mesmo quando você usa a opção `/check-only`. Use a opção `/no-fix-signature` para evitar a correção.

- /no-offline atributo opcional que impede que o volume seja definido como offline após concluir a ação.
- /no-fix-signature: atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de salvamento

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor device_id.

Tentar corrigir todos os problemas identificados em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Tentar corrigir todos os problemas dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Tentar corrigir um item específico dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Especificar vários problemas para tentar corrigir em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Ação de restauração

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
Restaurar a última boa configuração conhecida	`lkgc`	Last Known Good Configura tion (Última configuração válida conhecida): tenta inicializar a instância no estado inicializável mais recente conhecido.
Restaurar o registro do Windows do backup mais recente	`regback`	Restore registry from backup (Restaurar registro do backup): restaura o registro de `\Windows\System32\ config\RegBack` .

As seguintes opções estão disponíveis:

- /no-offline—Atributo opcional que impede que o volume seja definido offline após concluir a ação.
- /no-fix-signature—Atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de restauração

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor device_id.

Restaurar a última boa configuração conhecida em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Restaurar o último backup de registro do Windows em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Usar o EC2Rescue for Windows Server com o Run Command do Systems Manager

O AWS Support fornece um documento Run Command do Systems Manager para interagir com a instância habilitada para Systems Manager a fim de executar o EC2Rescue for Windows Server. O documento Run Command é chamado `AWSSupport-RunEC2RescueForWindowsTool`.

Este documento Run Command do Systems Manager realiza as seguintes tarefas:

- Baixa e verifica o EC2Rescue for Windows Server.
- Importa um módulo do PowerShell para facilitar a interação com a ferramenta.
- Executa EC2RescueCmd com o comando e os parâmetros fornecidos.

O documento Run Command do Systems Manager aceita três parâmetros:

- Comando—A EC2Rescue for Windows Server ação. Os valores atuais permitidos são:
  - ResetAccess—Restaura a senha do administrador local. A senha de administrador local da instância atual será restaurada e uma senha gerada aleatoriamente será armazenada com segurança no Parameter Store como `/EC2Rescue/Password/<INSTANCE_ID>`. Se você selecionar essa ação e não fornecer um parâmetro, as senhas serão criptografadas

automaticamente com a chave padrão Chave do KMS. Opcionalmente, você pode especificar um ID de chave Chave do KMS em Parameters (Parâmetros) para criptografar a senha com sua própria chave.

- CollectLogs—Executa o EC2Rescue for Windows Server com a ação `/collect:all`. Se você selecionar essa ação, `Parameters` deverá incluir um nome de bucket Amazon S3 no qual carregar os logs.
- FixAlll—Executa o EC2Rescue for Windows Server com a ação `/rescue:all`. Se você selecionar essa ação, `Parameters` deverá incluir o nome de dispositivo de bloco para salvar.

- Parameters—Os parâmetros do PowerShell para passar para o comando especificado.

> **Note**
>
> Para que a ação ResetAccess funcione, sua instância do Amazon EC2 precisa ter a seguinte política vinculada para gravar a senha criptografada no Parameter Store. Espere alguns minutos antes de tentar recuperar senha de uma instância depois de anexar essa política na função IAM relativa a ela.
> Usando a Chave do KMS padrão:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

> Usar uma Chave do KMS personalizada:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
        ]
      },
      {
      "Effect": "Allow",
      "Action": [
      "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:region:account_id:key/<kmskeyid>"
      ]
    }
  ]
}
```

O procedimento a seguir descreve como visualizar o JSON para este documento no console do Amazon EC2.

Para visualizar o JSON para o documento Run Command do Systems Manager

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/home.
2. No painel de navegação, expanda Shared Services e escolha Documents.
3. Na barra de pesquisa, defina o Proprietário como Meu ou da Amazon e defina o Prefixo de nome do documento como `AWSSupport-RunEC2RescueForWindowsTool`.
4. Selecione o documento `AWSSupport-RunEC2RescueForWindowsTool`, escolha Contents, e visualize o JSON.

Exemplos

Veja alguns exemplos sobre como usar o documento Run Command do Systems Manager para executar o EC2Rescue for Windows Server usando a AWS CLI. Para obter mais informações sobre o envio de comandos com a AWS CLI, consulte a Referência de comandos da AWS CLI.

Tentar corrigir todos os problemas identificados em um volume raiz offline

Tente corrigir todos os problemas identificados em um volume raiz off-line associado a uma instância do Windows do Amazon EC2:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters
 "Command=FixAll, Parameters='xvdf'" --output text
```

Coletar logs da instância atual do Windows do Amazon EC2

Colete todos os logs da instância atual do Windows do Amazon EC2 online e carregue-os em um bucket do Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --
parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Coletar logs de um volume de instância do Windows do Amazon EC2 offline

Colete todos os logs de um volume offline associado a uma instância do Windows do Amazon EC2 e carregue-os no Amazon S3 com um URL pré-assinado:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3"
 --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -
S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Redefinir a senha do administrador local

Os seguintes exemplos mostram os métodos que você pode usar para restaurar a senha de administrador local. A saída fornece um link para o Parameter Store, onde você encontra a senha segura gerada aleatoriamente para usar o RDP para sua instância do Windows do Amazon EC2 como administrador local.

Restaurar a senha de administrador local de uma instância online usando a chave padrão AWS KMS key alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess" --output text
```

Restaurar a senha de administrador local de uma instância online usando uma Chave do KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> Nesse exemplo, a Chave do KMS é `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

Console de Série do EC2 para as instâncias do Amazon EC2

Com o Console de Série do EC2, você tem acesso à porta serial da instância do Amazon EC2, que pode ser usada para solucionar problemas de lançamento, configuração de rede e outros problemas. O console de série não exige que sua instância tenha recursos de rede. Com o console de série, você pode inserir comandos para uma instância como se o teclado e o monitor estivessem conectados diretamente à porta serial da instância. A sessão do console de série tem a duração do período de reinicialização e de parada da instância. Durante a reinicialização, você pode visualizar todas as mensagens de inicialização desde o início.

O acesso ao console de série não está disponível por padrão. Sua organização deve conceder acesso da conta ao console de série e configurar políticas do IAM para conceder aos usuários acesso ao console de série. O acesso ao console serial pode ser controlado em um nível granular usando IDs de instância, tags de recursos e outras alavancas do IAM. Para obter mais informações, consulte Configurar o acesso ao Console de Série do EC2.

O console de série pode ser acessado usando o console do EC2 ou a AWS CLI.

O console de série está disponível sem qualquer custo adicional.

Tópicos

- Pré-requisitos do Console de Série do EC2
- Configurar o acesso ao Console de Série do EC2
- Conectar-se ao Console de Série do EC2
- Desconecte-se do Console de Série do EC2
- Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2

Pré-requisitos do Console de Série do EC2

Para se conectar ao Console de Série do EC2 e usar sua ferramenta preferida para solucionar problemas, os seguintes pré-requisitos devem estar em vigor:

- Regiões da AWS
- Zonas do Wavelength e AWS Outposts
- Zonas Locais
- Tipos de instância
- Concessão de acesso
- Suporte para cliente baseado em navegador
- Estado da instância
- Amazon EC2 Systems Manager
- Configurar a ferramenta de solução de problemas escolhida

Regiões da AWS

Compatível em todas as Regiões da AWS, exceto Oeste do Canadá (Calgary).

Zonas do Wavelength e AWS Outposts

Sem suporte.

Zonas Locais

Compatível em todas as zonas locais.

Tipos de instância

Tipos de instâncias compatíveis:

- Linux
  - Todas as instâncias virtualizadas criadas no Nitro System.
  - Todas instâncias bare metal, exceto:
    - Uso geral: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Computação acelerada: `g5g.metal`
    - Otimizadas para memória: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Todas as instâncias virtualizadas criadas no Nitro System. Não há suporte para instâncias bare metal.

Concessão de acesso

Você deve concluir as tarefas de configuração para conceder acesso ao Console de Série do EC2. Para ter mais informações, consulte Configurar o acesso ao Console de Série do EC2.

Suporte para cliente baseado em navegador

Para se conectar ao console de sérieUsando o cliente com base em navegador, seu navegador deve suportar WebSocket. Se o navegador não suportar WebSocket, conecte-se ao console de sérieUsando sua própria chave e um cliente SSH.

Estado da instância

Deve ser `running`.

Você não poderá se conectar ao console de série se a instância estiver no estado `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`.

Para obter mais informações sobre os estados da instância, consulte Ciclo de vida da instância.

Amazon EC2 Systems Manager

Se a instância usar o Amazon EC2 Systems Manager, o SSM Agent versão 3.0.854.0 ou posterior deve ser instalado na instância. Para obter mais informações sobre o SSM Agent, consulte Trabalhar com o SSM Agent no Guia do usuário do AWS Systems Manager.

Configurar a ferramenta de solução de problemas escolhida

Para solucionar problemas em sua instância via console de série, é possível usar o GRUB ou SysRq em instâncias do Linux e o Special Admin Console (SAC) em instâncias do Windows. Antes de usar essas ferramentas, é necessário executar as etapas de configuração em cada instância em que elas serão usadas.

Use as instruções para o sistema operacional da sua instância para configurar a ferramenta de solução de problemas escolhida.

(Instâncias do Linux) Configurar o GRUB

Para configurar o GRUB, escolha um dos seguintes procedimentos com base na AMI que foi usada para executar a instância.

Amazon Linux 2

Para configurar o GRUB em uma instância do Amazon Linux 2

1. Conecte-se à sua instância do Linux
2. Adicione ou altere as seguintes opções em `/etc/default/grub`:
   - Defina `GRUB_TIMEOUT=1`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub`. Você pode precisar alterar a configuração com base na configuração do seu sistema.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Aplique a configuração atualizada executando o comando a seguir.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

Para configurar o GRUB em uma instância do Ubuntu

1. Conecte-se à sua instância.
2. Adicione ou altere as seguintes opções em `/etc/default/grub.d/50-cloudimg-settings.cfg`:

   - Defina `GRUB_TIMEOUT=1`.
   - Adicionar `GRUB_TIMEOUT_STYLE=menu`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Remover `GRUB_HIDDEN_TIMEOUT`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub.d/50-cloudimg-settings.cfg`. Você pode precisar alterar a configuração com base na configuração do seu sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Para configurar o GRUB em uma instância do RHEL

1. Conecte-se à sua instância.
2. Adicione ou altere as seguintes opções em `/etc/default/grub`:
   - Remover `GRUB_TERMINAL_OUTPUT`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub`. Você pode precisar alterar a configuração com base na configuração do seu sistema.

   ```
   GRUB_TIMEOUT=1
   GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
   GRUB_DISABLE_RECOVERY="true"
   GRUB_ENABLE_BLSCFG=true
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Aplique a configuração atualizada executando o comando a seguir.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

CentOS

Para instâncias executadas usando uma AMI do CentOS, o GRUB é configurado para o console de série por padrão.

Veja a seguir um exemplo de `/etc/default/grub`. Sua configuração pode ser diferente com base na configuração do sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
```

```
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(Instâncias do Linux) Configurar o SysRq

Para configurar o SysRq, habilite os comandos do SysRq para o ciclo de inicialização atual. Para tornar a configuração persistente, você também pode habilitar os comandos SysRq para inicializações subsequentes.

Para habilitar todos os comandos SysRq para o ciclo de inicialização atual

1. Conecte-se à sua instância.
2. Execute o seguinte comando.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

> **Note**
>
> Essa configuração será limpa na próxima reinicialização.

Para habilitar todos os comandos do SysRq para inicializações subsequentes

1. Crie o arquivo `/etc/sysctl.d/99-sysrq.conf` e abra-o no seu editor favorito.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Adicione a seguinte linha.

```
kernel.sysrq=1
```

3. Reinicie a instância para aplicar as alterações.

```
[ec2-user ~]$ sudo reboot
```

4. No prompt `login`, insira o nome do usuário com senha que você configurou anteriormentee, a seguir, pressione Enter.
5. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

(Instâncias do Windows) Habilitar o SAC e o menu de inicialização

> **Note**
>
> Se você habilitar o SAC em uma instância, os serviços do EC2 que dependem de recuperação de senha não funcionarão no console do Amazon EC2. Os agentes de execução do Windows no Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) dependem do console de série para executar várias tarefas. Essas tarefas não são executadas com êxito quando você habilita o SAC em uma instância. Para obter mais informações sobre o Windows nos agentes de inicialização do Amazon EC2, consulte the section called “Configuração da instância do Windows”. Se você habilitar o SAC, poderá desabilitá-lo posteriormente. Para ter mais informações, consulte Desabilitar o SAC e o menu de inicialização.

Use um dos métodos a seguir para habilitar o SAC e o menu de inicialização em uma instância.

PowerShell

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas na linha de comando do PowerShell.
2. Habilite o SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Command prompt

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas no prompt de comando.
2. Habilite o SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Configurar o acesso ao Console de Série do EC2

Para configurar o acesso ao console de série, você deve conceder acesso ao console de série no nível da conta e, em seguida, configurar políticas do IAM para conceder acesso aos seus usuários. Para instâncias do Linux, você também deve configurar um usuário baseado em senha em cada instância com a finalidade de que os usuários possam usar o console de série para obter a solução de problemas.

Antes de começar, certifique-se de verificar os pré-requisitos.

Tópicos

- Níveis de acesso ao Console de Série do EC2
- Gerenciar o acesso da conta ao Console de Série do EC2
- Configurar políticas do IAM para acesso ao Console de Série do EC2

- Definição de uma senha do usuário do sistema operacional em uma instância do Linux

Níveis de acesso ao Console de Série do EC2

Por padrão, não há acesso ao console de série no nível da conta. Você precisa explicitamente conceder acesso ao console de série no nível da conta. Para obter mais informações, consulte Gerenciar o acesso da conta ao Console de Série do EC2.

Você pode usar uma política de controle de serviço (SCP) para permitir o acesso ao console de série dentro de sua organização. Em seguida, você pode ter controle de acesso granular no nível de usuário usando uma política do IAM para controlar o acesso. Usando uma combinação de políticas de SCP e do IAM, você tem diferentes níveis de controle de acesso ao console de série.

Nível da organização

Você pode usar uma política de controle de serviço (SCP) para permitir o acesso ao console de série para contas de membros dentro da sua organização. Para obter mais informações sobre SCPs, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Nível da instância

Você pode configurar as políticas de acesso ao console de série usando as construções IAM PrincipalTag e ResourceTag e especificando instâncias pelo ID delas. Para ter mais informações, consulte Configurar políticas do IAM para acesso ao Console de Série do EC2.

Nível de usuário

Você pode configurar o acesso no nível do usuário configurando uma política do IAM para permitir ou negar a um usuário especificado a permissão para enviar a chave pública SSH ao serviço de console de série de uma instância específica. Para ter mais informações, consulte Configurar políticas do IAM para acesso ao Console de Série do EC2.

Nível do sistema operacional (somente para instâncias do Linux)

Você pode definir uma senha de usuário no nível do SO convidado. Isso fornece acesso ao console de série para alguns casos de uso. No entanto, para monitorar os logs, você não precisa de um usuário com senha. Para obter mais informações, consulte Definição de uma senha do usuário do sistema operacional em uma instância do Linux.

Gerenciar o acesso da conta ao Console de Série do EC2

Por padrão, não há acesso ao console de série no nível da conta. Você precisa explicitamente conceder acesso ao console de série no nível da conta.

Tópicos

- Conceder permissão a usuários para gerenciar acesso à conta
- Exibir status de acesso da conta no console de série
- Conceder acesso da conta ao console de série
- Negar acesso da conta ao console de série

Conceder permissão a usuários para gerenciar acesso à conta

Para permitir que os usuários gerenciem o acesso da conta ao Console de Série do EC2, você precisa conceder a eles as permissões necessárias do IAM.

A política a seguir concede permissões para visualizar o status da conta e para permitir e impedir o acesso da conta ao Console de Série do EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

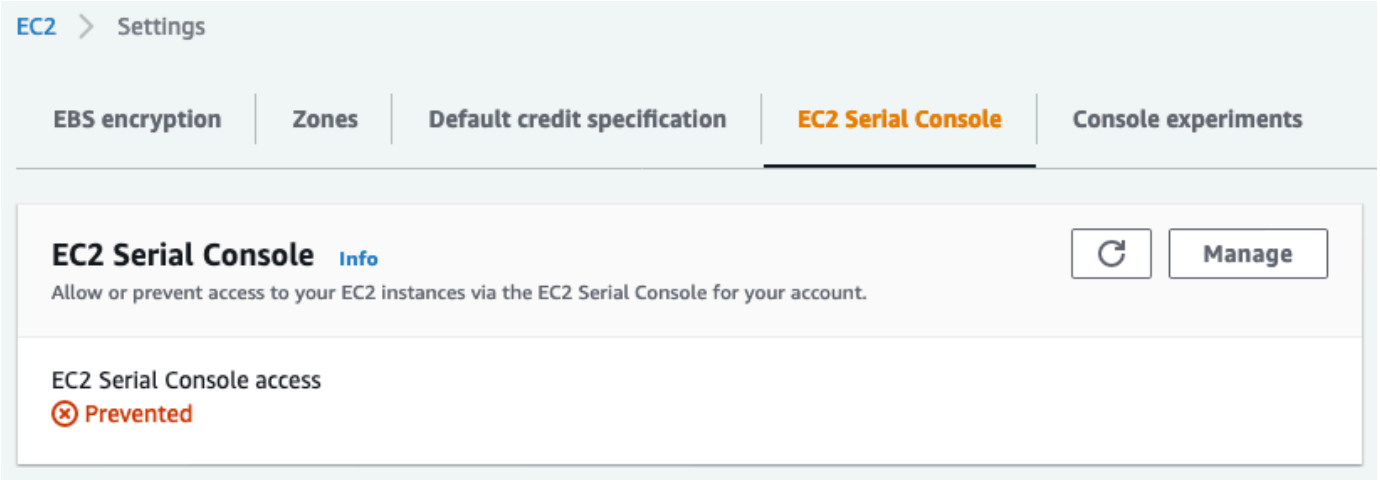
Exibir status de acesso da conta no console de série

Para exibir o status do acesso da conta no console de série (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).

   O campo de acesso ao Console serial do EC2 indica se o acesso da conta é Allowed (Permitido) ou Prevented (Impedido).

   A captura de tela a seguir mostra que a conta está impedida de usar o Console de Série do EC2.



Para exibir o status do acesso da conta ao console de série (AWS CLI)

Use o comando get-serial-console-access-status para exibir o status de acesso da conta ao console de série.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

Na saída a seguir, `true` indica que a conta tem permissão para acessar o console de série.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Conceder acesso da conta ao console de série

Para conceder acesso da conta ao console de série (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para permitir acesso de todas as instâncias da conta ao Console de Série do EC2, marque a caixa de seleção Allow (Permitir).
6. Escolha Update (Atualizar).

Para conceder acesso da conta ao console de série (AWS CLI)

Use o comando enable-serial-console-access para permitir o acesso da conta ao console de série.

```
aws ec2 enable-serial-console-access --region us-east-1
```

Na saída a seguir, `true` indica que a conta tem permissão para acessar o console de série.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Negar acesso da conta ao console de série

Para negar acesso da conta ao console de série (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para evitar o acesso de todas as instâncias da conta ao Console de Série do EC2, desmarque a caixa de seleção Allow (Permitir).
6. Escolha Update (Atualizar).

Para negar acesso da conta ao console de série (AWS CLI)

Use o comando disable-serial-console-access para impedir o acesso da conta ao console de série.

```
aws ec2 disable-serial-console-access --region us-east-1
```

Na saída a seguir, `false` indica que a conta tem acesso negado ao console de série.

```
{
    "SerialConsoleAccessEnabled": false
}
```

Configurar políticas do IAM para acesso ao Console de Série do EC2

Por padrão, seus usuários não têm acesso ao console de série. Sua organização deve configurar políticas do IAM para conceder aos usuários o acesso necessário. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

Para acessar o console de série, crie um documento de política JSON que inclua a ação `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Essa ação concede a um usuário permissão para enviar a chave pública para o serviço de console de série, que inicia uma sessão de console de série. Recomendamos restringir o acesso a instâncias do EC2 específicas. Caso contrário, todos os usuários com essa permissão poderão se conectar ao console de série de todas as instâncias do EC2.

Políticas de exemplo do IAM.

- Permitir explicitamente o acesso ao console de série
- Explicitamente negar acesso ao console de série
- Usar tags de recursos para controlar o acesso ao console de série

Permitir explicitamente o acesso ao console de série

Por padrão, ninguém tem acesso ao console de série. Para conceder acesso ao console de série, é preciso configurar uma política para permitir explicitamente o acesso. Recomendamos configurar uma política que restrinja o acesso a instâncias específicas.

A política a seguir permite o acesso ao console de série de uma instância específica, identificada pelo ID da instância.

Observe que as ações `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` não são compatíveis com permissões no nível do recurso e, portanto, todos os recursos, indicados por * (asterisco), devem ser especificados para essas ações.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Explicitamente negar acesso ao console de série

A política do IAM a seguir permite o acesso ao console de série de todas as instâncias, denotado pelo * (asterisco) e nega explicitamente o acesso ao console de série de uma instância específica, identificado por seu ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Usar tags de recursos para controlar o acesso ao console de série

Você pode usar tags de recursos para controlar o acesso ao console de série de uma instância.

O controle de acesso por atributo é uma estratégia de autorização que define permissões de acordo com tags que podem ser anexadas a usuários e a recursos da AWS. Por exemplo, a política a seguir só permite que um usuário inicie uma conexão de console de série para uma instância se a tag de recurso desta instância e a tag da entidade principal tiverem o mesmo valor do `SerialConsole` para a chave de tag.

Para obter mais informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte Controle do acesso aos recursos da AWS no Guia do usuário do IAM.

Observe que as ações `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` não são compatíveis com permissões no nível do recurso e, portanto, todos os recursos, indicados por `*` (asterisco), devem ser especificados para essas ações.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Definição de uma senha do usuário do sistema operacional em uma instância do Linux

> **Note**
>
> Esta seção se aplica somente a instâncias do Linux.

Você pode se conectar ao console de série sem uma senha. No entanto, para usar o console de série com a finalidade de solucionar problemas de uma instância do Linux, a instância deve ter um usuário do sistema operacional baseado em senha.

Você pode definir a senha para qualquer usuário do sistema operacional, incluindo o usuário raiz. Observe que o usuário raiz pode modificar todos os arquivos, enquanto cada usuário do sistema operacional pode ter permissões limitadas.

Você deve definir uma senha de usuário para cada instância para a qual você usará o console de série. Essa é uma exigência única de cada instância.

> **Note**
>
> As instruções apresentadas a seguir serão aplicáveis somente se você iniciar a instância usando uma AMI do Linux fornecida pela AWS porque, por padrão, as AMIs fornecidas pela AWS não são configuradas com um usuário baseado em senha. Se você tiver executado a instância usando uma AMI que já tenha a senha do usuário raiz configurada, poderá ignorar essas instruções.

Para definir uma senha do usuário do sistema operacional em uma instância do Linux

1. Conecte-se à sua instância. Você pode usar qualquer método para se conectar à instância, exceto o método de conexão do Console de Série do EC2.
2. Para definir a senha para um usuário, use o comando passwd. No exemplo a seguir, o usuário é `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   A seguir está um exemplo de saída.

   ```
   Changing password for user root.
   New password:
   ```
3. No prompt `New password`, digite a nova senha.
4. No prompt, digite novamente a senha.

Conectar-se ao Console de Série do EC2

Você pode se conectar ao console de série da instância do EC2 usando o console do Amazon EC2 ou por SSH. Depois de se conectar ao console de série, você pode usá-lo para solucionar problemas de inicialização, configuração de rede e outros problemas. Para obter mais informações sobre solução de problemas, consulte Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2.

Considerações

- Há suporte para somente uma conexão ativa do console de série por instância.

- A conexão do console de série geralmente dura uma hora, a menos que você se desconecte. No entanto, durante a manutenção do sistema, o Amazon EC2 desconectará a sessão do console de série.
- Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.
- Portas do console de série com suporte: `ttyS0` (instâncias do Linux) e `COM1` (instâncias do Windows)
- Quando você se conecta ao console de série, pode observar uma pequena queda na taxa de throughput da instância.

Tópicos

- Conectar-se usando o cliente com base em navegador
- Conectar-se usando sua própria chave e cliente SSH
- Endpoints e impressões digitais do console serial EC2

Conectar-se usando o cliente com base em navegador

Você pode se conectar ao console de série da instância do EC2 usando o cliente com base em navegador. Faça isso selecionando a instância no console do Amazon EC2 e escolhendo conectar-se ao console de série. O cliente com base em navegador lida com as permissões e fornece uma conexão bem-sucedida.

O Console de Série do EC2 funciona a na maioria dos navegadores e suporta entrada de teclado e mouse.

Antes de realizar a conexão, certifique-se de ter concluído os pré-requisitos.

Para se conectar à porta serial da instância usando o cliente com base em navegador (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolher Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), EC2 Serial Console (Console de Série do EC2), Connect (Conectar).

Ou selecione a instância e escolha Connect (Conectar), EC2 Serial Console (Console de Série do EC2), Connect (Conectar).

Uma janela de terminal no navegador é aberta.

4. Pressione Enter. Se for exibido um prompt de login, significará que você está conectado ao console de série.

   Se a tela permanecer preta, você poderá usar as seguintes informações para ajudar a resolver problemas com a conexão ao console de série:

   - Verifique se você configurou o acesso ao console de série. Para ter mais informações, consulte Configurar o acesso ao Console de Série do EC2.
   - (Somente para instâncias do Linux) Use SysRq para realizar a conexão com o console de série. O SysRq não exige que você se conecte por meio do cliente com base em navegador. Para ter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância.
   - (Somente para instâncias do Linux) Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Reinicialize sua instância. É possível reinicializar a instância ao usar SysRq (instâncias do Linux), o console do EC2 ou a AWS CLI. Para obter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância (instâncias do Linux) ou Reinicializar a instância.

5. (Somente para instâncias do Linux) Na solicitação `login`, insira o nome do usuário baseado em senha que você configurou anteriormente e, em seguida, pressione Enter.
6. (Somente para instâncias do Linux) Na solicitação `Password`, insira a senha e, em seguida, pressione Enter.

Agora, você está conectado à instância e pode usar o console de série para solucionar problemas.

Conectar-se usando sua própria chave e cliente SSH

Você pode usar sua própria chave do SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do console de série. Isso permite que você se beneficie da capacidade do console de série de enviar por push uma chave pública para a instância.

Antes de realizar a conexão, certifique-se de ter concluído os pré-requisitos.

Para se conectar ao console de série de uma instância usando SSH

1. Envie por push a chave pública do SSH para a instância para iniciar uma sessão de console de série

   Use o comando send-serial-console-ssh-public-key para enviar por push a chave pública do SSH para a instância. Isso inicia uma sessão de console de série.

   Se uma sessão de console de série já tiver sido iniciada para essa instância, o comando falhará porque você só pode ter uma sessão aberta de cada vez. Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Conecte-se ao console de série usando sua chave privada

   Use o comando ssh para se conectar ao console de série antes que a chave pública seja removida do serviço de console de série. Você tem 60 segundos antes que ela seja removida.

   Use a chave privada que corresponde à chave pública.

   O formato do nome de usuário é `instance-id.port0`, que abrange o ID da instância e a porta 0. No exemplo a seguir, o nome de usuário é `i-001234a4bf70dec41EXAMPLE.port0`.

   O endpoint do serviço de console de série é diferente para cada região. Veja a Endpoints e impressões digitais do console serial EC2 tabela do endpoint de cada região. No exemplo a seguir, o serviço de console de série está na região *us-east-1*.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
   connect.us-east-1.aws
   ```

3. (Opcional) Verificar a impressão digital

   Quando você se conecta pela primeira vez ao console de série, é solicitado a verificar a impressão digital. Você pode comparar a impressão digital do console de série com a impressão

digital exibida para verificação. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se elas corresponderem, você poderá se conectar com confiança ao console de série.

A seguinte impressão digital corresponde ao serviço de console de série na região us-east-1. Para obter as impressões digitais de cada região, consulte Endpoints e impressões digitais do console serial EC2.

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
```

> **Note**
>
> A impressão digital só aparece na primeira vez que você se conecta ao console de série.

4. Pressione Enter. Se for exibido um prompt, significará que você está conectado ao console de série.

   Se a tela permanecer preta, você poderá usar as seguintes informações para ajudar a resolver problemas com a conexão ao console de série:

   - Verifique se você configurou o acesso ao console de série. Para ter mais informações, consulte Configurar o acesso ao Console de Série do EC2.
   - (Somente para instâncias do Linux) Use SysRq para realizar a conexão com o console de série. O SysRq não exige que você se conecte via SSH. Para ter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância.
   - (Somente para instâncias do Linux) Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Reinicialize sua instância. É possível reinicializar a instância ao usar SysRq (somente para instâncias do Linux), o console do EC2 ou a AWS CLI. Para obter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância (somente para instâncias do Linux) ou Reinicializar a instância.

5. (Somente para instâncias do Linux) Na solicitação `login`, insira o nome do usuário baseado em senha que você configurou anteriormente e, em seguida, pressione Enter.

6. (Somente para instâncias do Linux) Na solicitação `Password`, insira a senha e, em seguida, pressione Enter.

Agora, você está conectado à instância e pode usar o console de série para solucionar problemas.

Endpoints e impressões digitais do console serial EC2

A seguir estão os endpoints de serviço e as impressões digitais do EC2 Serial Console. Para se conectar programaticamente ao console de série de uma instância, você usa um endpoint do console de série EC2. Os endpoints e impressões digitais do console serial do EC2 são exclusivos para cada região AWS.

Nome da região	Região	Endpoint	Impressão digital
Leste dos EUA (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256:EhwPkTzRtTY7TRSzz26XbB0/HvV9jRM7mCZN0xw/d/0
Leste dos EUA (Norte da Virgínia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
Oeste dos EUA (N. da Califórnia)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
Oeste dos EUA (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
África (Cidade do Cabo)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256:RMWWZ2fVePe

Nome da região	Região	Endpoint	Impressão digital
			JUqzjO5jL2KIgXsczo Hlz21Ed00biiWI
Ásia-Pacífico (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1lpiXxCh oZHplnAkjbP7tkm2xX ViC9bJFsjYnifk
Ásia-Pacífico (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256:WJ gPBSwV4/shN +OPITValoewAuYj1 5DVW845JEhDKRs
Ásia-Pacífico (Jacarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256:5ZwgrCh+lfn s32XITqL/4O0zIfbx4 bZgsYFqy3o8mIk
Ásia-Pacífico (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Av aq27hFgLv jn5gTSShZ 0oV7h90p0 GG46wfOeT6ZJvM
Ásia-Pacífico (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:oB LXcYmklqH HEbliARxEgH8IsO51r ezTPiSM35BsU40
Ásia-Pacífico (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:Am0/ jiBKBnBuFnHr9aXs gEV3G8Tu/ vVHFXE/3UcyjsQ
Ásia-Pacífico (Seul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++GuNTztg9 PK49WYMqBX +FrcZM2dSrqrI

Nome da região	Região	Endpoint	Impressão digital
Ásia-Pacífico (Singapura)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256:PLFNn7WnCQDHx3qmwLu1Gy/O8TUX7LQgZuaC6L45CoY
Ásia-Pacífico (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256:yFvMwUK9lEUQjQTRoXXzuN+cW9/VSe9W984Cf5Tgzo4
Ásia-Pacífico (Tóquio)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256:RQfsDCZTOfQawewTRDV1t9Em/HMrFQe+CRlIOT5um4k
Canadá (Central)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256:P2O2jOZwmpMwkpO6YW738FIOTHdUTyEv2gczYMMO7s4
China (Pequim)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA256:2gHVFy4H7uU3+WaFUxD28v/ggMeqjvSlgngpgLgGT+Y
China (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA256:TdgrNZkiQOdVfYEBUhO4SzUA09VWI5rYOZGTogpwmiM

Nome da região	Região	Endpoint	Impressão digital
Europa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:aCMFS/yIcOdOlkXvOl8AmZ1Toe+bBnrJJ3Fy0k0De2c
Europa (Irlanda)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E
Europa (Londres)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
Europa (Milão)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:IC0kOVJnpgFyBVrxn0A7n99ecLbXSX95cuuS7X7QK30
Europa (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeEWs
Europa (Espanha)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:GoCW2DFRlu669QNxqFxEcsR6fZUz/4F4n7T45ZcwoEc
Europa (Estocolmo)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84

Nome da região	Região	Endpoint	Impressão digital
Europa (Zurique)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256:8Ppx2mBMf6WdCw0NUlzKfwM4/IfRz4OaXFutQXWp6mk
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256:JR6q8v6kNNPi8+QSFQ4dj5dimNmZPTgwgsM1SNvtYyU
Oriente Médio (Barém)	me-south-1	ec2-serial-console.me-south-1.api.aws	SHA256:nPjLLKHu2QnLdUq2kVArsoK5xvPJOMRJKCBzCDqC3k8
Oriente Médio (Emirados Árabes Unidos)	me-central-1	ec2-serial-console.me-central-1.api.aws	SHA256:zpb5duKiBZ+l0dFwPeyykB4MPBYhI/XzXNeFSDKBvLE
América do Sul (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256:rd2+/32Ognjew1yVIemENaQzC+Botbih62OqAPDq1dI
AWS GovCloud (Leste dos EUA)	us-gov-east-1	serial-console.ec2-instance-connect.us-gov-east-1.amazonaws.com	SHA256:tIwe19GWsoyLClrtvu38YEEh+DHIkqnDcZnmtebvF28
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	serial-console.ec2-instance-connect.us-gov-west-1.amazonaws.com	SHA256:kfOFRWLaOZfB+utbd3bRf8OlPf8nGO2YZLqXZiIw5DQ

Desconecte-se do Console de Série do EC2

Se você não precisa mais estar conectado ao Console de Série do EC2 da sua instância, pode se desconectar dele. Quando você se desconecta do console de série, as sessões de shell em execução na instância continuarão sendo executadas. Se desejar encerrar a sessão do shell, será necessário encerrá-la antes de se desconectar do console de série.

Considerações

- A conexão do console de série geralmente dura uma hora, a menos que você se desconecte. No entanto, durante a manutenção do sistema, o Amazon EC2 desconectará a sessão do console de série.
- Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.

A forma de se desconectar do console de série depende do cliente.

Cliente com base em navegador

Para se desconectar do console de série, feche a janela de terminal no navegador do console de série.

Cliente OpenSSH padrão

Para se desconectar do console de série, use o comando a seguir para fechar a conexão SSH. Esse comando deve ser executado imediatamente após uma nova linha.

```
~.
```

O comando que você usa para fechar uma conexão SSH pode ser diferente, dependendo do cliente SSH que você está usando.

Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2

Ao usar o Console de Série do EC2, você pode solucionar problemas de inicialização, configuração de rede e outros problemas ao se conectar à porta serial da instância.

Use as instruções para o sistema operacional da sua instância e para a ferramenta que você configurou em sua instância.

> **Note**
>
> Antes de começar, certifique-se de ter concluído os pré-requisitos, inclusive a configuração da sua ferramenta de solução de problemas escolhida.

(Instâncias do Linux) Usar o GRUB para solucionar problemas na sua instância

O GNU GRUB (abreviatura de GNU GRand Unified Bootloader) é o carregador de inicialização padrão para a maioria dos sistemas operacionais Linux. No menu do GRUB, você pode selecionar em qual kernel inicializar ou modificar entradas de menu para alterar a forma como o kernel irá inicializar. Isso pode ser útil ao solucionar problemas de uma instância com falha.

O menu do GRUB é exibido durante o processo de inicialização. O menu não é acessível via SSH normal, mas você pode acessá-lo por meio do Console de Série do EC2.

É possível inicializar no modo de usuário único ou no modo de emergência. O modo de usuário único inicializará o kernel em um nível de execução inferior. Por exemplo, ele pode montar o sistema de arquivos, mas não ativar a rede, dando a você a oportunidade de realizar a manutenção necessária para corrigir a instância. O modo de emergência é semelhante ao modo de usuário único, exceto que o kernel é executado no nível de execução mais baixo possível.

Para inicializar no modo de usuário único

1. Connect (Conecte-se) ao console de série da instância.
2. Execute a instância usando o seguinte comando.

   ```
   [ec2-user ~]$ sudo reboot
   ```
3. Durante a reinicialização, quando o menu do GRUB aparecer, pressione qualquer tecla para interromper o processo de inicialização.
4. No menu do GRUB, use as teclas de seta para selecionar o kernel para inicializar e pressione e no teclado.
5. Use as teclas de seta para posicionar o cursor na linha que contém o kernel. A linha começa com um `linux` ou `linux16`, dependendo da AMI usada para executar a instância. Para o Ubuntu, duas linhas começam com `linux`, que devem ser modificadas na próxima etapa.
6. No final da linha, adicione a palavra `single`.

   Veja um exemplo a seguir para Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Pressione Ctrl+X para inicializar no modo de usuário único.
8. No prompt `login`, insira o nome do usuário com senha que você configurou anteriormente, a seguir, pressione Enter.
9. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

Para inicializar no modo de emergência

Siga as mesmas etapas do modo de usuário único, mas na etapa 6, adicione a palavra `emergency` em vez de `single`.

(Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância

A chave System Request (SysRq), que, às vezes, é denominada “SysRq mágica”, pode ser usada para enviar diretamente ao kernel um comando, fora de um shell, e o kernel responderá, independentemente do que o kernel está fazendo. Por exemplo, se a instância tiver parado de responder, você poderá usar a chave SysRq para dizer ao kernel para falhar ou reiniciar. Para obter mais informações, consulte Chave SysRq mágica na Wikipédia.

Você pode usar comandos SysRq no cliente com base em navegador do Console de Série do EC2 ou em um cliente SSH. O comando que enviará uma solicitação de interrupção é diferente para cada cliente.

Para usar o SysRq, escolha um dos seguintes procedimentos com base no cliente que você está usando.

Browser-based client

Para usar o SysRq no cliente com base em navegador do console de série

1. Connect (Conecte-se) ao console de série da instância.

2. Para enviar uma solicitação de interrupção, pressione `CTRL+0` (zero). Se o teclado suportá-la, você também poderá enviar uma solicitação de interrupção usando a tecla Pause ou Break.

```
[ec2-user ~]$ CTRL+0
```

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

```
[ec2-user ~]$ h
```

O comando h gera algo semelhante ao seguinte.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

Para usar o SysRq em um cliente SSH

1. Connect (Conecte-se) ao console de série da instância.
2. Para enviar uma solicitação de interrupção, pressione `~B` (til, seguido de maiúsculas `B`).

```
[ec2-user ~]$ ~B
```

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

```
[ec2-user ~]$ h
```

O comando h gera algo semelhante ao seguinte.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
```

```
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> O comando que você usa para enviar uma solicitação de interrupção pode ser diferente, dependendo do cliente SSH que você está usando.

(Instâncias do Windows) Usar o SAC para solucionar problemas na sua instância

O recurso Special Admin Console (SAC) do Windows fornece uma maneira de solucionar problemas de uma instância do Windows. Ao se conectar ao console de série da instância e usando o SAC, você pode interromper o processo de inicialização e inicializar o Windows no modo de segurança.

> **Note**
>
> Se você habilitar o SAC em uma instância, os serviços do EC2 que dependem de recuperação de senha não funcionarão no console do Amazon EC2. Os agentes de execução do Windows no Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) dependem do console de série para executar várias tarefas. Essas tarefas não são executadas com êxito quando você habilita o SAC em uma instância. Para obter mais informações sobre o Windows nos agentes de inicialização do Amazon EC2, consulte the section called “Configuração da instância do Windows”. Se você habilitar o SAC, poderá desabilitá-lo posteriormente. Para ter mais informações, consulte Desabilitar o SAC e o menu de inicialização.

Tópicos

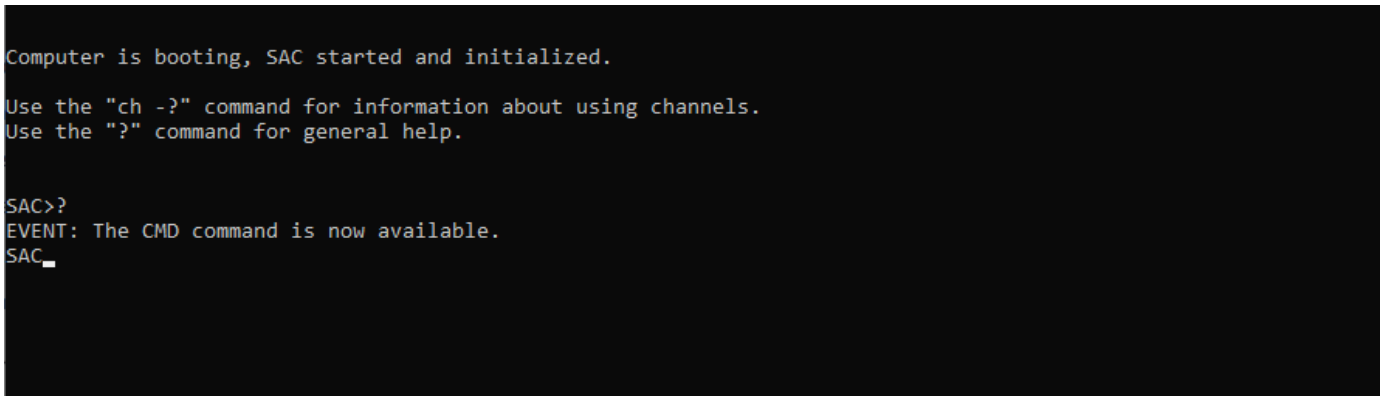
- Usar o SAC
- Usar o menu de inicialização
- Desabilitar o SAC e o menu de inicialização

Usar o SAC

Para usar o SAC

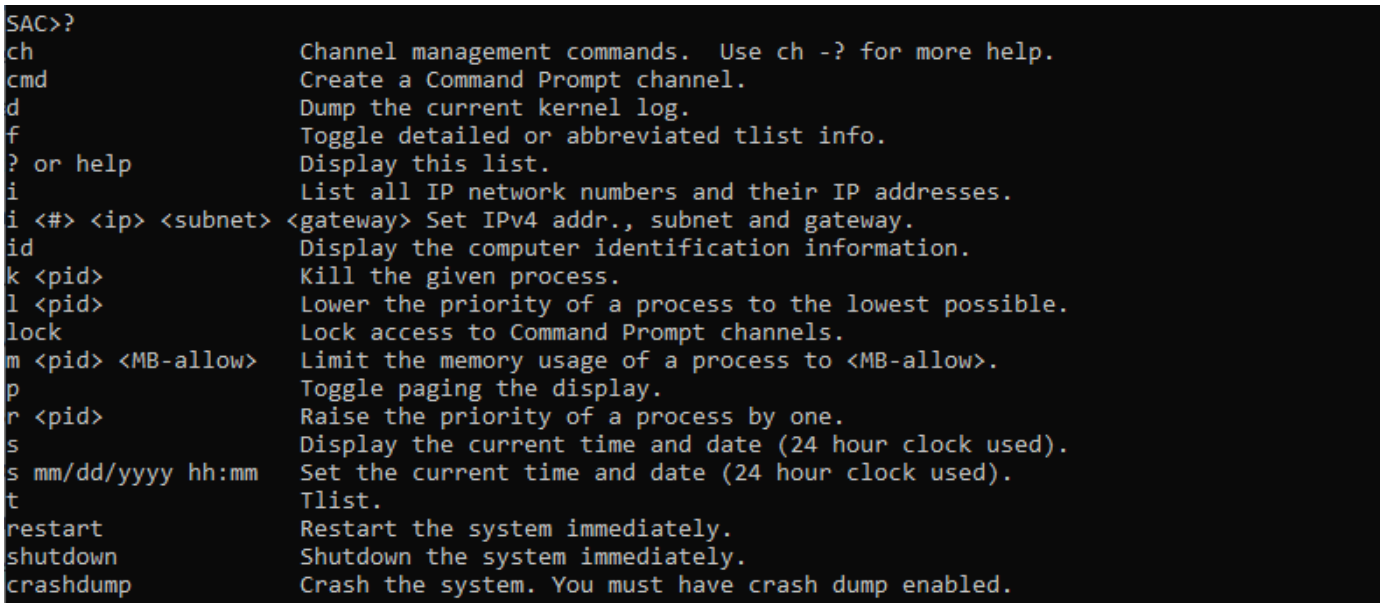
1. Conecte-se ao console de série.

   Se o SAC estiver habilitado na instância, o console de série exibirá oSAC>editor.exe?".



2. Para exibir os comandos do SAC, digite**?**E pressioneDigite.

   Saída esperada



3. Para criar um canal de linha de comandos (comocmd0001oucmd0002), insira**cmd**E pressioneDigite.
4. Para ver o canal do prompt de comando, pressioneESCE pressioneTAB.

   Saída esperada

```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Para trocar de canais, pressioneESC+tab+número do canaljunto. Por exemplo, para alternar para o`cmd0002`(se tiver sido criado), pressioneESC+TABA+2.
6. Insira as credenciais exigidas pelo canal do prompt de comando.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

O prompt de comando é o mesmo shell de comando completo que você obtém em um desktop, mas com a exceção de que ele não permite a leitura de caracteres que já foram emitidos.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online           46 GB    46 GB

DISKPART>
```

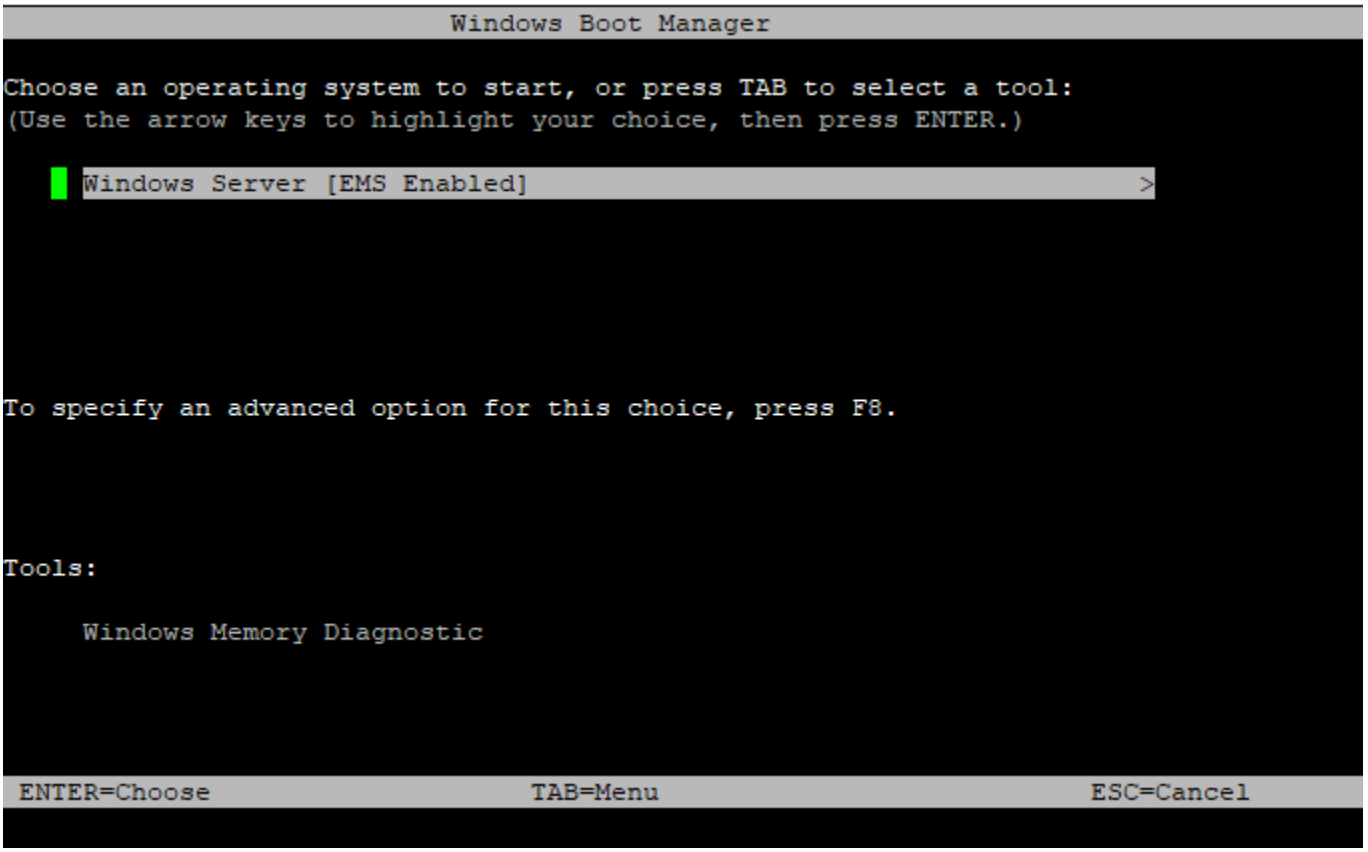
O PowerShell também pode ser usado a partir do prompt de comando.

Observe que talvez seja necessário definir a preferência do progresso para o modo silencioso.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Usar o menu de inicialização

Se a instância tiver o menu de inicialização habilitado e for reiniciado após a conexão via SSH, você verá o menu de inicialização, como a seguir.



Comandos do menu de inicialização

ENTER

Inicia a entrada selecionada do sistema operacional.

TAB

Alterna para o menu Tools (Ferramentas).

ESC

Cancela e reinicia a instância.

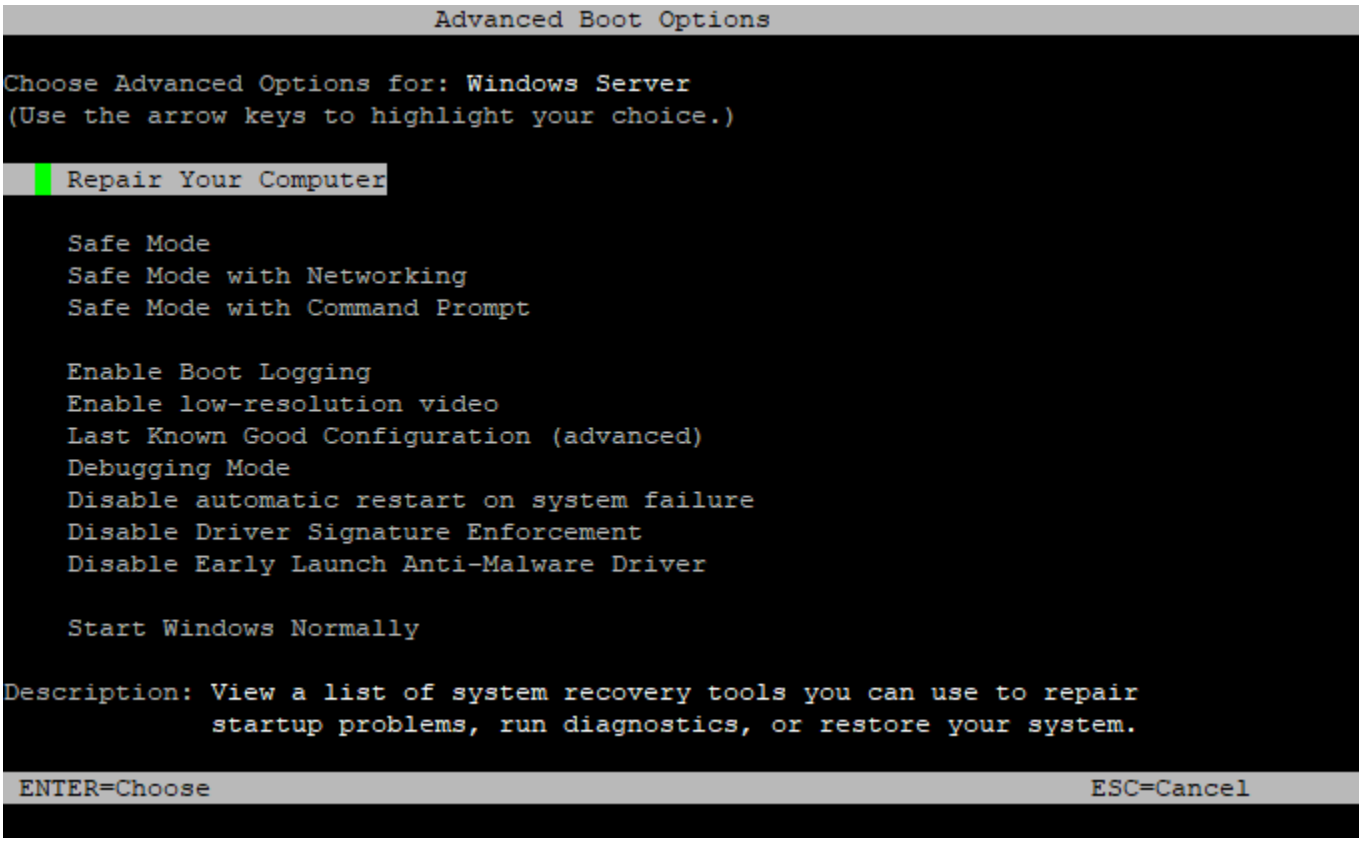
ESC seguido por 8

Equivalente a pressionar F8. Mostra opções avançadas para o item selecionado.

Tecla ESC + seta para a esquerda

Volta para o menu de inicialização inicial.

> **Note**
>
> A tecla ESC por si só não leva você de volta ao menu principal porque o Windows está aguardando para ver se uma sequência de escape está em andamento.



Desabilitar o SAC e o menu de inicialização

Se você habilitar o SAC e o menu de inicialização, poderá desabilitar esses recursos posteriormente.

Use um dos métodos a seguir para desabilitar o SAC e o menu de inicialização em uma instância.

PowerShell

Para desabilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas na linha de comando do PowerShell.
2. Primeiro, desabilite o menu de inicialização alterando o valor para `no`.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Em seguida, desabilite o SAC alterando o valor para `off`.

```
bcdedit /ems '{current}' off
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Command prompt

Para desabilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas no prompt de comando.
2. Primeiro, desabilite o menu de inicialização alterando o valor para `no`.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Em seguida, desabilite o SAC alterando o valor para `off`.

```
bcdedit /ems {current} off
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Enviar uma interrupção para diagnóstico (para usuários avançados)

> **Warning**
>
> As interrupções de diagnóstico são destinadas ao uso de usuários avançados. O uso incorreto pode ter um impacto negativo sobre sua instância. Enviar uma interrupção de diagnóstico para uma instância pode acionar uma instância para travar e reinicializar, o que pode levar à perda de dados.

É possível enviar uma interrupção de diagnóstico para uma instância inacessível ou que não responde com a finalidade de acionar manualmente um kernel panic para uma instância do Linux ou um erro de parada (comumente chamado de erro de tela azul) para uma instância do Windows.

Instâncias do Linux

Os sistemas operacionais Linux normalmente falham e reinicializam quando ocorre um pânico de kernel. O comportamento específico do sistema operacional depende de sua configuração. Um pânico de kernel também pode ser usado para fazer com que o kernel do sistema operacional da instância execute tarefas, como a geração de um arquivo de despejo de falha. É possível usar as informações no arquivo de despejo da falha para conduzir uma análise de causa raiz e depurar a instância. Os dados do despejo da falha são gerados localmente pelo sistema operacional na própria instância.

Instâncias do Windows

Em geral, os sistemas operacionais Windows falham e reinicializam quando ocorre um erro de parada, mas o comportamento específico depende de sua configuração. Um erro de parada também pode fazer com que o sistema operacional grave informações de depuração, como um despejo de memória de kernel, em um arquivo. É possível usar essas informações para conduzir análises de causa raiz para depurar a instância. Os dados do despejo da memória são gerados localmente pelo sistema operacional na própria instância.

Antes de enviar uma interrupção de diagnóstico para sua instância, recomendamos que você consulte a documentação do seu sistema operacional e, em seguida, faça as alterações de configuração necessárias.

Tópicos

- Tipos de instâncias compatíveis
- Pré-requisitos
- Enviar uma interrupção para diagnóstico

Tipos de instâncias compatíveis

A interrupção do diagnóstico é compatível com todos os tipos de instância baseadas em Nitro, exceto as que são ativadas pelos processadores AWS Graviton. Para obter mais informações, consulte Instances built on the AWS Nitro System e AWS Graviton.

Pré-requisitos

Antes de usar uma interrupção para diagnóstico, configure o sistema operacional da instância. Isso garantirá que o sistema operacional execute as ações necessárias quando ocorrer um kernel panic (instâncias do Linux) ou um erro de parada (instâncias do Windows).

Instâncias do Linux

Para configurar o Amazon Linux 2 para gerar um despejo de falha quando ocorrer um pânico de kernel

1. Conecte-se à sua instância.
2. Instale kexec e kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Configure o kernel para reservar uma quantidade de memória para o kernel secundário. A quantidade de memória a ser reservada depende da memória disponível total de sua instância. Abra o arquivo `/etc/default/grub` usando o editor de texto de sua preferência, localize a linha que começa com `GRUB_CMDLINE_LINUX_DEFAULT` e adicione o parâmetro `crashkernel` no seguinte formato: `crashkernel=`*`memory_to_reserve`*. Por exemplo, para reservar `160MB`, modifique o arquivo `grub` da seguinte forma:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
    net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
    rd.shell=0"
   GRUB_TIMEOUT=0
   GRUB_DISABLE_RECOVERY="true"
   ```

4. Salve as alterações e feche o arquivo `grub`.
5. Recompile o arquivo de configuração do GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Abra o arquivo `/etc/sysctl.conf` usando o editor de texto de sua preferência e adicione o seguinte.

```
kernel.unknown_nmi_panic=1
```

7. Reinicialize e reconecte-se a sua instância.
8. Verifique se o kernel foi inicializado com o parâmetro `crashkernel` correto.

```
$ grep crashkernel /proc/cmdline
```

A saída do seguinte exemplo indica uma configuração bem-sucedida.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Verifique se o serviço kdump está em execução.

```
[ec2-user ~]$ systemctl status kdump.service
```

A saída do seguinte exemplo mostrará o resultado se o kdump estiver em execução.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Por padrão, o arquivo de dump da falha é salvo em `/var/crash/`. Para alterar o local, modifique o arquivo `/etc/kdump.conf` usando o editor de texto de sua preferência.

Para configurar o Amazon Linux para gerar um despejo de falha quando ocorrer um pânico de kernel

1. Conecte-se à sua instância.
2. Instale kexec e kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Configure o kernel para reservar uma quantidade de memória para o kernel secundário. A quantidade de memória a ser reservada depende da memória disponível total de sua instância.

   ```
   $ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
   ```

   Por exemplo, para reservar `160MB` para o kernel de falha, use o seguinte comando.

   ```
   $ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
   ```

4. Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Abra o arquivo `/etc/sysctl.conf` usando o editor de texto de sua preferência e adicione o seguinte.

   ```
   kernel.unknown_nmi_panic=1
   ```

5. Reinicialize e reconecte-se a sua instância.
6. Verifique se o kernel foi inicializado com o parâmetro `crashkernel` correto.

   ```
   $ grep crashkernel /proc/cmdline
   ```

   A saída do seguinte exemplo indica uma configuração bem-sucedida.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
 LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Verifique se o serviço kdump está em execução.

```
[ec2-user ~]$ sudo service kdump status
```

Se o serviço estiver em execução, o comando retornará a resposta `Kdump is operational`.

> **Note**
>
> Por padrão, o arquivo de dump da falha é salvo em `/var/crash/`. Para alterar o local, modifique o arquivo `/etc/kdump.conf` usando o editor de texto de sua preferência.

Para configurar o SUSE Linux Enterprise, o Ubuntu ou o Red Hat Enterprise Linux

Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando ele receber a NMI desconhecida. Para fazer isso, ajuste o arquivo de configuração para o seu sistema operacional. Para obter mais informações sobre como configurar o kernel para falhar, consulte a documentação do sistema operacional.

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Instâncias do Windows

Para configurar o Windows para gerar um despejo de memória quando ocorrer um erro de parada.

1. Conecte-se à sua instância.
2. Abra o Control Panel (Painel de controle) e escolha System (Sistema), Advanced system settings (Configurações avançadas do sistema).

3. Na caixa de diálogo System Properties (Propriedades do sistema), escolha a guia Advanced (Avançado).
4. Na seção Startup and Recovery (Inicialização e recuperação), escolha Settings... (Configurações...).
5. Na seção System failure (Falha do sistema), defina as configurações conforme necessário e escolha OK.

Para obter mais informações sobre como configurar os erros de parada do Windows, consulte Visão geral das opções do arquivo de despejo de memória do Windows.

Enviar uma interrupção para diagnóstico

Depois de concluir as alterações necessárias na configuração, é possível enviar uma interrupção de diagnóstico para a instância usando a AWS CLI ou a API do Amazon EC2.

AWS CLI

Para enviar uma interrupção para diagnóstico para sua instância (AWS CLI)

Use o comando send-diagnostic-interrupt e especifique o ID da instância.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Para enviar uma interrupção para diagnóstico para sua instância (AWS Tools for Windows PowerShell)

Use o cmdlt Send-EC2DiagnosticInterrupt e especifique o ID da instância.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Histórico do documento

A tabela apresentada a seguir descreve adições importantes ao Guia do usuário do Amazon EC2 a partir de 2019. Além disso, atualizamos o guia com frequência para abordar os comentários enviados por você.

Alteração	Descrição	Data
Tipos de instância adicionais compatíveis com o Credential Guard	Agora é possível habilitar o Credential Guard para instâncias C7i, C7-flex, M7i, M7i-flex, R7i, R7i-flex e T3.	26 de junho de 2024
Instâncias Mac M1 Ultra do EC2	Novo tipo de instância de uso geral que conta com processadores Apple M1 Ultra.	17 de junho de 2024
Assistente de seleção de tipo de instância do EC2: parâmetros adicionais	Agora, o assistente de seleção de tipo de instância do EC2 fornece parâmetros adicionais para você especificar requisitos mais detalhados para a workload.	5 de junho de 2024
Instâncias U7i-12tb, U7in-16tb, U7in-24tb e U7in-32tb	Novos tipos de instâncias de alta memória com processadores Intel Xeon Scalable de 4ª geração.	28 de maio de 2024
Nova política gerenciada para o EC2 Fast Launch	Adicionada a política de EC2FastLaunchFullAccess para realizar ações de API relacionadas ao atributo EC2 Fast Launch em uma instância.	14 de maio de 2024
Proteção contra cancelamento de registro da AMI	É possível ativar a proteção contra cancelamento de	23 de abril de 2024

	registro em uma AMI para evitar sua exclusão acidental ou mal-intencionada.	
Relógio de hardware PTP: suporte ao tipo de instância	O relógio de hardware PTP agora está disponível nos tipos de instância C7a, C7i, M7a, M7g, M7i, R7a e R7i.	22 de abril de 2024
Adição de considerações de performance sobre o Nitro para redes aprimoradas	Esta página se concentra em considerações de rede para ajudar no ajuste de performance de instâncias do Amazon EC2 baseadas no Nitro.	4 de abril de 2024
Nova política gerenciada para snapshots do EBS habilitados para o VSS	O VSS do Amazon EC2 tem uma nova política gerenciada pelo IAM disponível que você pode adicionar à sua função do perfil de instância para garantir que as permissões permaneçam atualizadas e sigam as práticas recomendadas.	28 de março de 2024
Relógio de hardware PTP: Leste dos EUA (Norte da Virgínia)	O relógio de hardware PTP agora está disponível na região Leste dos EUA (Norte da Virgínia).	26 de março de 2024
Definir o IMDSv2 como o padrão da conta	É possível definir todas as execuções de novas instâncias do EC2 em sua conta para usar o Instance Metadata Service Version 2 (IMDSv2) por padrão.	25 de março de 2024

Marcar novas AMIs do Linux criadas com base em um snapshot	Ao criar uma AMI do Linux com base em um snapshot, é possível marcar a nova AMI.	7 de março de 2024
Marcar novas AMIs e snapshots ao copiar	Ao copiar uma AMI, é possível marcar a nova AMI e os novos snapshots com as mesmas tags ou com tags diferentes.	7 de março de 2024
Remoção de páginas do AWS Management Pack	O AWS Management Pack foi usado, principalmente, com o Windows Server 2012 e com versões anteriores. Não há mais suporte para essas versões da plataform a do sistema operacional herdadas. Para gerenciar e solucionar problemas relacionados à sua frota de servidores em execução na AWS e on-premises, consulte AWS Systems Manager Fleet Manager.	12 de fevereiro de 2024
EC2 Instance Connect pré-instalado em AMIs do macOS	Agora, o EC2 Instance Connect vem pré-instalado nas AMIs do macOS Sonoma 14.2.1 ou posterior, macOS Ventura 13.6.3 ou posterior e macOS Monterey 12.7.2 ou posterior.	26 de janeiro de 2024
EC2 Instance Connect support for CentOS, macOS, and RHEL	Agora é possível instalar o EC2 Instance Connect em AMIs compatíveis do CentOS, do macOS e do RHEL.	6 de dezembro de 2023

Compatibilidade com hibernação de C7a, C7i, R7a, R7i e R7iz	Coloque em hibernação as instâncias recém-iniciadas em execução nos tipos de instância C7a, C7i, R7a, R7i e R7iz.	1.º de dezembro de 2023
Seletor de tipo de instância do EC2 Amazon Q	O seletor de tipo de instância do EC2 Amazon Q considera o caso de uso, o tipo de workload e a preferência do fabricante da CPU, e também como você prioriza preço e performance. Depois, ele usa esses dados para fornecer orientações e sugestões sobre os tipos de instância do Amazon EC2 que são mais adequados para as novas workloads.	28 de novembro de 2023
Nível gratuito do EC2	Você pode acompanhar o seu uso do nível gratuito do EC2 no painel do EC2.	26 de novembro de 2023
Console-to-Code	O Console-to-Code pode ajudar você a começar a usar o seu código de automação. O Console-to-Code registra as suas ações feitas no console e depois usa IA generativa para sugerir código no formato de infraestrutura como código de sua preferência. Você pode usar o código como ponto de partida, personalizando-o para deixá-lo pronto para produção no seu caso de uso específico.	26 de novembro de 2023

Tempos limites configuráveis de rastreamento de conexão ociosa	As conexões do grupo de segurança que permanecem ociosas podem levar à exaustão do rastreamento da conexão e fazer com que as conexões não sejam rastreadas e os pacotes sejam descartados. Você agora pode definir em segundos o tempo limite para rastreamento de conexões do grupo de segurança em uma interface de rede do Elastic.	17 de novembro de 2023
Relógio PTP físico	As instâncias compatíveis agora têm um relógio Precision Time Protocol (PTP) físico. O relógio PTP físico é compatível tanto com uma conexão NTP como com uma conexão PTP direta.	16 de novembro de 2023
Alterar o tipo de instância de uma instância habilitada para hibernação	Você não pode alterar o tipo de instância de uma instância habilitada para hibernação quando ela está no estado `stopped`.	16 de novembro de 2023
Topologia da instância	Você pode usar a API DescribeInstanceTopology para detectar a localização das suas instâncias e depois usar essas informações para otimizar trabalhos de HPC e ML executando-os em instâncias fisicamente mais próximas umas das outras.	13 de novembro de 2023

Compatibilidade com AMI compartilhada do EC2 Fast Launch	Agora você pode habilitar o EC2 Fast Launch em uma AMI que seja compartilhada com você. Quando você habilita o EC2 Fast Launch em uma AMI compartilhada, snapshots pré-provisionados para uma inicialização mais rápida são criados na sua conta.	6 de novembro de 2023
Blocos de capacidade para ML	Você agora pode reservar instâncias de GPU para uma data futura a fim de lidar com workloads de machine learning (ML) de curta duração.	31 de outubro de 2023
Hibernação de instância spot	Agora você pode colocar instâncias spot em hibernação usando a mesma experiência de hibernação e as mesmas famílias de instâncias que estão atualmente disponíveis para instâncias sob demanda.	24 de outubro de 2023
Configurações padrão de bloquear acesso público para AMIs	O bloqueio do acesso público para AMIs agora é habilitado por padrão em todas as contas novas e nas contas existentes sem AMIs públicas.	20 de outubro de 2023
Amazon EC2 Global View	A Visualização Global do Amazon EC2 é compatível com tipos de recursos adicionais e opções de exibição personalizáveis.	18 de outubro de 2023

Suporte à hibernação para o Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Hiberne suas instâncias executadas recentemente pela AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 de outubro de 2023
Desabilitar uma AMI	Você pode desabilitar uma AMI para evitar que ela seja usada em execuções de instâncias.	12 de outubro de 2023
Verificações de status do EBS anexado	Você pode usar as verificaç ões de status do EBS anexado para monitorar se os volumes do Amazon EBS anexados a uma instância estão acessívei s.	11 de outubro de 2023
Suporte de hibernação para o Red Hat Enterprise Linux 9	Coloque em hibernação as instâncias recém-iniciadas que foram executadas na AMI do Red Hat Enterprise Linux 9.	2 de outubro de 2023
Suporte de hibernação para o Microsoft Windows Server 2022	Coloque em hibernação as instâncias recém-iniciadas que foram executadas no AMI do Microsoft Windows Server 2022.	2 de outubro de 2023
Suporte para hibernação do AL2023	Coloque em hibernação as instâncias recém-iniciadas que foram executadas na AMI do AL2023.	2 de outubro de 2023

Iniciar a interrupção das instâncias spot em uma frota spot	Você pode selecionar uma Frota Spot no console da Amazon EC2 e iniciar uma interrupção das Instância s Spot na frota para testar como as aplicações nas suas Instâncias Spot lidam com a interrupção.	21 de setembro de 2023
Bloqueie o acesso público às AMIs	Você pode ativar o bloqueio de acesso público para AMIs no nível da conta para bloquear qualquer tentativa de tornar suas AMIs públicas.	12 de setembro de 2023
Compatibilidade com hibernação para M7i e M7i-flex	Hiberne as instâncias recém-iniciadas em execução nos tipos de instância M7i e M7i-flex.	22 de agosto de 2023
O EC2-Classic foi descontinuado	Com o EC2-Classic, suas instâncias do EC2 executadas em uma única rede simples compartilhada com outros clientes. A Amazon VPC substitui o EC2-Classic. Com a Amazon VPC, suas instâncias são executadas em uma nuvem privada virtual (VPC) que é isolada logicamente na conta da AWS.	8 de agosto de 2023
Hosts dedicados	Você pode alocar hosts dedicados em ativos de hardware específicos em um Outpost.	20 de junho de 2023

Endpoint do EC2 Instance Connect	Agora é possível conectar-se a uma instância via SSH ou RDP sem exigir que a instância tenha um endereço IPv4 público.	13 de junho de 2023
IMDS Package Analyzer	Agora você pode usar o IMDS Packet Analyzer para identificar origens de chamadas IMDSv1 em suas instâncias do EC2.	1.º de junho de 2023
Instâncias bare metal do Console de Série do EC2	O Console de Série do EC2 agora oferece suporte à conectividade com a porta de série de instâncias bare metal selecionadas.	11 de abril de 2023
Cotas do modelo de execução	É possível visualizar as cotas para os modelos de execução e as versões de modelos de execução no console do Service Quotas e usando a CLI do Service Quotas.	3 de abril de 2023
Notificações de utilização da reserva de capacidade	O AWS Health enviará notificações quando a utilização da capacidade para reservas de capacidade em sua conta estiver abaixo de 20%.	3 de abril de 2023
Grupos de Reserva de capacidade	É possível adicionar reservas de capacidade compartilhadas com você aos grupos de reserva de capacidade de sua propriedade.	30 de março de 2023

Modificar opções de metadados da instância	É possível usar o console Amazon EC2 para modificar as opções de metadados da instância.	20 de março de 2023
Atualizações do sistema operacional macOS no local	Agora, é possível realizar atualizações do sistema operacional no local em instâncias M1 do Mac.	14 de março de 2023
UEFI preferencial	Agora, é possível criar uma única AMI que suporte ambos os modos de inicialização, Unified Extensible Firmware Interface (UEFI) e BIOS legado.	3 de março de 2023
Modificar uma AMI para IMDSv2	Modifique sua AMI existente de modo que as instância s iniciadas a partir da AMI exijam o IMDSv2 por padrão.	28 de fevereiro de 2023
Segurança baseada na virtualização do Windows - Credential Guard	Você pode habilitar o Credential Guard, um recurso de segurança baseada em virtualização (VBS), em instâncias compatíveis do Amazon EC2.	31 de janeiro de 2023
Alias de AMI em modelos de inicialização	Você pode especificar um parâmetro AWS Systems Manager em vez do ID da AMI nos modelos de inicialização para evitar ter que atualizar os modelos toda vez que o ID da AMI for alterada.	19 de janeiro de 2023

Compatibilidade com hibernação para C6i, I3en e M6i	Hiberne as instâncias recém-iniciadas em execução nos tipos de instância C6i, I3en e M6i.	19 de dezembro de 2022
Prevenção de gravação interrompida	Melhore a performance das workloads de banco de dados relacional com uso intenso de E/S e reduza a latência sem afetar negativamente a resiliência dos dados com a prevenção a gravação interrompida, um recurso de armazenamento de blocos.	29 de novembro de 2022
ENA Express	Aumente o throughput e minimize a latência final do tráfego de rede entre instâncias do EC2 com o ENA Express.	28 de novembro de 2022
Bloqueio de regra de retenção da lixeira	Você pode bloquear as regras de retenção para ajudar a protegê-las contra modificações e exclusões acidentais ou maliciosas.	23 de novembro de 2022
Copiar tags de AMI	Ao copiar uma AMI, você pode copiar as tags de AMI definidas pelo usuário ao mesmo tempo.	18 de novembro de 2022
Tamanho de AMI para armazenamento e restauração	O tamanho de uma AMI (antes da compactação) que pode ser armazenada e restaurada de e em um bucket do Amazon S3 agora pode ser de até 5.000 GB.	16 de novembro de 2022

Estratégia de alocação priceCapacityOptimized para instâncias spot	Uma frota spot que usa a estratégia de alocação `priceCapacityOptimized` examina o preço e a capacidade para selecionar os grupos de instâncias spot com menor probabilidade de interrupção e com o menor preço mais possível.	10 de novembro de 2022
Estratégia de alocação price-capacity-optimized para instâncias spot	Uma frota do EC2 que usa a estratégia de alocação `price-capacity-optimized` em preço e capacidade para selecionar os grupos de instâncias spot com menor probabilidade de interrupção e com o menor preço possível.	10 de novembro de 2022
Cancelar o compartilhamento de uma AMI com sua conta	Se uma AMI tiver sido compartilhada com sua Conta da AWS e você não quiser mais compartilhá-la com sua conta, poderá remover sua conta das permissões de execução da AMI.	4 de novembro de 2022
Transferir endereços IP elásticos	Agora, é possível transferir endereços IP elásticos de uma Conta da AWS para outra.	31 de outubro de 2022
Substituir volume raiz	Você pode substituir o volume raiz do Amazon EBS por uma instância em execução usando uma AMI.	27 de outubro de 2022

Conectar automaticamente a instância ao banco de dados	Use o recurso de conexão automática para conectar rapidamente uma ou mais instâncias do EC2 a um banco de dados do RDS para permitir o tráfego entre elas.	10 de outubro de 2022
Cotas de AMI	As cotas já se aplicam à criação e ao compartilhamento de AMIs.	10 de outubro de 2022
Configurar AMI para o IMDSv2	Configure a AMI de modo que as instâncias iniciadas a partir da AMI exijam o IMDSv2 por padrão.	3 de outubro de 2022
Iniciar interrupção de instância spot	Você pode selecionar uma instância spot no console do Amazon EC2 e iniciar uma interrupção para poder testar como as aplicações nessas instâncias spot lidam com interrupções.	26 de setembro de 2022
Provedor de AMI verificado	No console do Amazon EC2, AMIs públicas de propriedade da Amazon ou de um parceiro verificado da Amazon são marcadas como Provedor verificado.	22 de julho de 2022
Grupos de posicionamento no AWS Outposts	Foi adicionada uma estratégi a de distribuição de host para grupos de posicionamento em um Outpost.	30 de junho de 2022

Chaves de condição para a Recycle Bin (Lixeira)	Você pode usar as chaves de condição `rbin:RequestResourceType` e `rbin:Attribute/ResourceType` para filtrar o acesso nas solicitações da Recycle Bin (Lixeira).	14 de junho de 2022
Volumes `io2` do Block Express	Você pode modificar o tamanho e as IOPS provisionadas dos volumes do `io2` Block Express e pode habilitá-los para restauração rápida de snapshots.	31 de maio de 2022
Hosts dedicados no AWS Outposts	Você pode alocar hosts dedicados em AWS Outposts.	31 de maio de 2022
Proteção de instâncias contra interrupção	Para impedir que sua instância seja interrompida acidentalmente, habilite a proteção contra a interrupção da instância.	24 de maio de 2022
UEFI Secure Boot	O UEFI Secure Boot baseia-se no longo processo de inicialização segura do Amazon EC2 e fornece defesa adicional em profundidade que ajuda os clientes a proteger o software contra ameaças que persistem durante as reinicializações.	10 de maio de 2022

NitroTPM	O Nitro Trusted Platform Module (NitroTPM) é um dispositivo virtual fornecido pelo AWS Nitro System que está em conformidade com a especificação TPM 2.0.	10 de maio de 2022
Eventos de alteração de estado de AMI	O Amazon EC2 agora gera um evento quando uma AMI muda de estado. É possível usar o Amazon EventBridge para detectar e reagir a esses eventos.	9 de maio de 2022
Descrever as chaves públicas	É possível consultar a chave pública e a data de criação de um par de chaves do Amazon EC2.	28 de abril de 2022
Criar pares de chaves	É possível especificar o formato da chave (PEM ou PPK) ao criar um novo par de chaves.	28 de abril de 2022
Monte sistemas de arquivos Amazon FSx na inicialização	É possível montar um sistema de arquivos Amazon FSx novo ou existente para NetApp ONTAP ou Amazon FSx for OpenZFS na inicialização usando o novo assistente de inicialização de instância.	12 de abril de 2022

Novo assistente de inicialização de instância, versão beta	Uma nova e aprimorada experiência de lançamento no console do Amazon EC2, fornecendo uma maneira mais rápida e fácil de iniciar uma instância do EC2.	5 de abril de 2022
Descontinuar automaticamente as AMIs públicas	Por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos a partir da data de criação da AMI.	31 de março de 2022
Categoria de metadados de instância: autoescalabilidade/estado de destino do ciclo de vida	Ao usar grupos do Auto Scaling, é possível acessar o estado de destino do ciclo de vida de uma instância com base nos metadados de instância.	24 de março de 2022
Hora do último início da AMI	`lastLaunchedTime` indica quando sua AMI foi usada pela última vez para iniciar uma instância.	28 de fevereiro de 2022
Lixeira para AMIs	A Lixeira permite restaurar AMIs excluídas acidentalmente.	3 de fevereiro de 2022
Chaves ED25519	Agora há suporte para as chaves ED25519 para EC2 Instance Connect e Console de série do EC2.	20 de janeiro de 2022
Plataformas RHEL adicionais para reservas de capacidade	Plataformas Red Hat Enterprise Linux adicionais para reservas de capacidade sob demanda.	11 de janeiro de 2022

Configure AMIs do Windows para um início mais rápido	Configure AMIs do Windows para iniciar instâncias até 65% mais rápido, usando snapshots pré-provisionados.	10 de janeiro de 2022
Tags de instância em metadados de instância	É possível acessar as tags de uma instância a partir dos metadados da instância.	6 de janeiro de 2022
As Reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster	É possível criar reservas de capacidade em grupos de posicionamento de cluster.	6 de janeiro de 2022
Lixeira de snapshots do Amazon EBS	A lixeira de snapshots do Amazon EBS é um recurso de recuperação de snapshots que permite restaurar snapshots excluídos acidentalmente.	29 de novembro de 2021
Lançamento antes do término da frota spot	A frota spot pode terminar as instâncias spot que recebem uma notificação de rebalanceamento após o lançamento de novas Instâncias spot de substituição.	4 de novembro de 2021
Lançamento antes do término da frota do EC2	A frota do EC2 pode terminar as instâncias spot que recebem uma notificação de rebalanceamento após o início de novas instâncias spot de substituição.	4 de novembro de 2021

Compare os carimbos de data/hora	É possível determinar a hora real de um evento comparando o carimbo de data/hora da instância do Linux do Amazon EC2 com o ClockBound.	2 de novembro de 2021
Compartilhe AMIs com organizações e UOs	Agora é possível compartilhar AMIs com os seguintes recursos da AWS: organizações e unidades organizacionais (UOs).	29 de outubro de 2021
Pontuação de posicionamento de spot	Receba uma recomendação para uma região ou zona de disponibilidade da AWS com base nos requisitos de capacidade spot.	27 de outubro de 2021
Seleção de tipo de instância baseada em atributos para frota spot	Especifique os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos.	27 de outubro de 2021
Seleção de tipo de instância baseada em atributos para frota do EC2	Especifique os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos.	27 de outubro de 2021
Frota de reserva de capacidade sob demanda	É possível usar uma frota de reserva de capacidade para iniciar um grupo ou frota de reservas de capacidade.	5 de outubro de 2021

Compatibilidade com hibernação para Ubuntu 20.04 LTS - Focal	Coloque em hibernação suas instâncias recém-iniciadas que foram executadas no Ubuntu 20.04 LTS - Focal AMI.	4 de outubro de 2021
Reservas de Capacidade sob demanda e direcionadas para EC2 Fleet	O EC2 Fleet pode iniciar Instâncias sob demanda nas Reservas de Capacidade `targeted`.	22 de setembro de 2021
Instâncias T3 em hosts dedicados	Suporte para instâncias T3 no host dedicado Amazon EC2.	14 de setembro de 2021
Suporte de hibernação para RHEL, Fedora e CentOS	Coloque em hibernação suas instâncias recém-iniciadas que foram iniciadas a partir de AMIs RHEL, Fedora e CentOS.	9 de setembro de 2021
Amazon EC2 Global View	O Amazon EC2 Global View permite que você visualize VPCs, sub-redes, instância s, grupos de segurança e volumes em várias regiões do AWS em um único console.	1º de setembro de 2021
Suporte de defasagem de AMI para Amazon Data Lifecycle Manager	As políticas de AMI apoiadas pelo EBS do Amazon Data Lifecycle Manager podem defasar AMIs. A política gerenciada AWSDataLi fecycleManagerServiceRoleFo rAMIManagement da AWS foi atualizada para ser compatível com esse recurso.	23 de agosto de 2021

Suporte à hibernação para C5d, M5d e R5d	Coloque em hibernação suas instâncias recém-iniciadas em execução nos tipos de instância C5d, M5d e R5d.	19 de agosto de 2021
Pares de chaves do Amazon EC2	O Amazon EC2 agora é compatível com chaves ED25519 em instâncias Linux e Mac.	17 de agosto de 2021
Prefixos para interfaces de rede	É possível atribuir um intervalo de CIDR IPv4 ou IPv6 privado, de modo automático ou manual, às interfaces de rede.	22 de julho de 2021
Janelas de eventos	É possível definir janelas de eventos personalizadas e semanais para eventos programados que reinicial izam, interrompem ou terminam suas instâncias do Amazon EC2.	15 de julho de 2021
IDs de recursos e suporte a marcação para regras do grupo de segurança	É possível fazer referênci a a regras de grupo de segurança por ID de recurso. Também é possível adicionar tags a regras de grupos de segurança.	7 de julho de 2021
Descontinuar uma AMI	Agora é possível especificar quando uma AMI é defasada.	11 de junho de 2021
Cobrança do Windows por segundo	O Amazon EC2 cobra por segundo pela utilização baseada em Windows e SQL Server, com cobrança mínima de um minuto.	10 de junho de 2021

Reservas de Capacidade no AWS Outposts	Agora é possível usar as Reservas de Capacidade no AWS Outposts.	24 de maio de 2021
Compartilhamento de reserva de capacidade	Agora é possível compartilhar Reservas de Capacidade criadas em zonas locais e zonas do Wavelength.	24 de maio de 2021
Substituição do volume raiz	Agora é possível usar tarefas de substituição de volume raiz para substituir o volume raiz do EBS para instâncias em execução.	22 de abril de 2021
Armazenar e restaurar uma AMI usando o S3	Armazene AMIs baseadas em EBS no S3 e restaure-as a partir do S3 para permitir a cópia de AMIs entre partições.	6 de abril de 2021
Console serial do EC2	Solucione problemas de inicialização e conectividade de rede estabelecendo uma conexão com a porta serial de uma instância.	30 de março de 2021
Modos de inicialização	O Amazon EC2 agora é compatível com a inicialização UEFI em determinadas instâncias do EC2 baseadas em AMD e Intel.	22 de março de 2021
Crie um registro de DNS reverso	Agora é possível configurar a pesquisa de DNS reverso para os seus endereços IP elásticos.	3 de fevereiro de 2021

Marcar AMIs e snapshots na criação de AMI	Ao criar uma AMI, é possível marcar a AMI e os snapshots com as mesmas tags, ou pode marcá-los com tags diferentes.	4 de dezembro de 2020
Use o Amazon EventBridge para monitorar eventos de frota spot	Crie regras do EventBridge que acionem ações programáticas em resposta a alterações e erros de estado de frota spot.	20 de novembro de 2020
Use Amazon EventBridge para monitorar eventos de Frota do EC2	Crie regras de EventBridge que acionem ações programáticas em resposta a alterações e erros de estado de Frota do EC2.	20 de novembro de 2020
Excluir frotas de instant	Exclua uma Frota do EC2 do tipo `instant` e encerre todas as instâncias na frota em uma única chamada de API.	18 de novembro de 2020
Suporte à hibernação para T3 e T3a	Hiberne suas instâncias recém-executadas em execução em tipos de instância T3 e T3a.	17 de novembro de 2020
Criação rápida do Amazon EFS	É possível criar e montar um sistema de arquivos do Amazon EFS em uma instância na inicialização usando o Amazon EFS Quick Create.	9 de novembro de 2020

Categoria de metadados da instância: events/recommendations/rebalance	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalanceamento da instância do EC2 é emitida para a instância.	4 de novembro de 2020
Recomendação de rebalanceamento de instâncias do EC2	Um sinal que o notifica quando uma instância spot está em risco elevado de interrupção.	4 de novembro de 2020
Reservas de Capacidade em zonas Wavelength	Reservas de Capacidade agora podem ser criadas e usadas em zonas Wavelength.	4 de novembro de 2020
Rebalanceamento de capacidade	Configure a frota spot ou a EC2 Fleet para executar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento.	4 de novembro de 2020
Suporte à hibernação para I3, M5ad e R5ad	Hibernar suas instâncias recém-iniciadas em execução nos tipos de instância I3, M5ad e R5ad.	21 de outubro de 2020
Limites de vCPU da instância spot	Os limites da instância spot agora são gerenciados em termos do número de vCPUs que suas instâncias spot em execução estão usando ou usarão até o atendimento de solicitações abertas.	1º de outubro de 2020
Reservas de Capacidade em zonas locais	Reservas de Capacidade agora podem ser criadas e usadas em zonas locais.	30 de setembro de 2020

Suporte à hibernação para M5a e R5a	Hiberne suas instâncias recém-executadas em execução nos tipos de instância M5a e R5a.	28 de agosto de 2020
Os metadados da instância fornecem informações de posicionamento e localização da instância	Novos campos de metadados de instância na categoria `placement` : região, nome do grupo de posicionamento, número da partição, ID do host e ID da zona de disponibilidade.	24 de agosto de 2020
Grupos de Reserva de capacidade	É possível usar AWS Resource Groups para criar coleções lógicas de reservas de capacidade e, depois, direcionar execuções de instâncias nesses grupos.	29 de julho de 2020
EC2Launch v2	É possível usar o EC2Launch v2 para executar tarefas durante o startup da instância se uma instância for interrompida e iniciada posteriormente, se uma instância for reiniciada, e também sob demanda. O EC2Launch v2 é compatível com todas as versões do Windows Server e substitui o EC2Launch e o EC2Config.	30 de junho de 2020
Traga seus próprios endereços IPv6	É possível trazer parte ou todo o seu intervalo de endereços IPv6 da rede on-premises para sua conta da AWS.	21 de maio de 2020

Inicie instâncias usando um parâmetro do Systems Manager	É possível especificar um parâmetro do AWS Systems Manager em vez de uma AMI ao executar uma instância.	5 de maio de 2020
Personalizar notificações de eventos programados	É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail.	4 de maio de 2020
Kernel Live Patching para Amazon Linux 2	O Kernel Live Patching para Amazon Linux 2 permite que você aplique vulnerabilidades de segurança e patches de erros críticos a um kernel do Linux em execução, sem reinicializações ou interrupç ões a aplicativos de execução.	28 de abril de 2020
Windows Server no Hosts dedicados	É possível usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados.	7 de abril de 2020
Interromper e iniciar uma instância spot	Agora é possível interromp er suas instâncias spot com base no Amazon EBS e iniciá-las à vontade, em vez de depender do comportamento de interrupção.	13 de janeiro de 2020

Marcação de recursos	É possível marcar gateways da Internet somente de saída, gateways locais, tabelas de rotas de gateway, interfaces virtuais de gateway locais, grupos de interface virtual de gateway local, associações de VPC da tabela de rotas do gateway local e associações de grupo de interface virtual da tabela de rotas do gateway local	10 de janeiro de 2020
Conecte-se à sua instância usando o Gerenciador de sessões	É possível iniciar uma sessão do Gerenciador de sessões com uma instância no console do Amazon EC2.	18 de dezembro de 2019
Hosts dedicados e grupos de recursos de host	Hosts dedicados agora podem ser usados com grupos de recursos de host.	2 de dezembro de 2019
Compartilhamento de host dedicado	Agora é possível compartilhar os hosts dedicados entre contas da AWS.	2 de dezembro de 2019
Especificação de crédito padrão no nível da conta	É possível definir a especificação de crédito padrão por família de instâncias expansíveis no nível da conta, por região da AWS.	25 de novembro de 2019
Descoberta de tipo de instância	É possível encontrar um tipo de instância que atenda às suas necessidades.	22 de novembro de 2019

Hosts dedicados	Agora, é possível configurar um Host dedicado para oferecer suporte a vários tipos de instância em uma família de instâncias.	21 de novembro de 2019
Serviço de metadados da instância versão 2	É possível usar o Serviço de metadados da instância versão 2, que é um método orientado a sessão para solicitação de metadados da instância.	19 de novembro de 2019
Adaptador de malha elástica	O Adaptador de malha elástica agora pode ser usado com a Intel MPI 2019 Update 6.	15 de novembro de 2019
Suporte à hibernação de instâncias do Windows sob demanda	É possível hibernar instâncias do Windows sob demanda.	14 de outubro de 2019
Compras na fila de instâncias reservadas	É possível colocar a compra de uma Instância reservada na fila até três anos de maneira antecipada.	4 de outubro de 2019
Interrupção do diagnóstico	É possível enviar uma interrupção para diagnóstico a uma instância inacessível ou sem resposta para acionar um pânico de kernel.	14 de agosto de 2019

Estratégia de alocação otimizada por capacidade	Com o uso de EC2 Fleet ou de frota spot, agora é possível executar instâncias spot a partir de grupos spot com a capacidade ideal para o número de instâncias que estão sendo executadas.	12 de agosto de 2019
Compartilhamento de reservas de capacidade sob demanda	Agora é possível compartilhar as Reservas de Capacidade entre contas da AWS.	29 de julho de 2019
Adaptador de malha elástica	O EFA agora oferece suporte à Open MPI 3.1.4 e à Intel MPI 2019 Update 4.	26 de julho de 2019
EC2 Instance Connect	O EC2 Instance Connect é uma forma simples e segura de conectar-se com suas instâncias usando Secure Shell (SSH).	27 de junho de 2019
Recuperação do host	Reinicie automaticamente suas instâncias em um novo host no caso de uma falha inesperada do hardware em um Host dedicado.	5 de junho de 2019
Snapshots consistentes com a aplicação VSS	Crie snapshots consistentes com a aplicação de todos os volumes do Amazon EBS anexados às instâncias do Windows usando o Run Command do AWS Systems Manager.	13 de maio de 2019

Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server	Mover workloads existentes do Microsoft SQL Server de um sistema operacional Windows para Linux.	8 de maio de 2019
Atualização automatizada do Windows	Execute atualizações automatizadas de instâncias do EC2 do Windows usando o AWS Systems Manager.	6 de maio de 2019
Adaptador de malha elástica	É possível anexar um Elastic Fabric Adapter às suas instâncias para acelerar os aplicativos High Performance Computing (HPC).	29 de abril de 2019

Para obter informações sobre as liberações de tipo de instância do Amazon EC2, consulte Document history no Guia de tipos de instância do Amazon EC2.

Histórico para 2018 e para os anos anteriores

A tabela apresentada a seguir descreve adições importantes ao Guia do usuário do Amazon EC2 em 2018 e nos anos anteriores.

Atributo	Versão da API	Descrição	Data de lançamento
Grupos de posicionamento de partição	15/11/2016	Os grupos de posicionamento de partição distribuem instâncias entre partições lógicas, garantindo que instâncias em uma partição não compartilhem hardware subjacente com instâncias em outras partições. Para ter mais informações, consulte Placement groups de partição.	20 de dezembro de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Hibernar instâncias do EC2 do Linux	15/11/2016	É possível hibernar uma instância do Linux se ela estiver habilitada para hibernação e atender aos pré-requisitos de hibernação. Para ter mais informações, consulte Hibernar sua instância do Amazon EC2.	28 de novembro de 2018
Amazon Elastic Inference Accelerators	15/11/2016	É possível anexar um Amazon EI Accelerator a suas instâncias para adicionar aceleração da plataforma de GPU para reduzir o custo de inferência de deep learning.	28 de novembro de 2018
O console do Spot recomenda uma frota de instâncias	15/11/2016	O console do Spot recomenda uma frota de instâncias com base na melhor prática do Spot (diversificação de instâncias) para atender às especificações mínimas de hardware (vCPUs, memória e armazenamento) para a necessidade de sua aplicação. Para ter mais informações, consulte Criar uma solicitação de frota spot.	20 de novembro de 2018
Novo tipo de solicitação de Frota do EC2: instant	15/11/2016	Agora, o Frota do EC2 oferece suporte a um novo tipo de solicitação, `instant`, que pode ser usada para provisionar capacidade de forma síncrona entre tipos de instâncias e modelos de compra. A solicitação `instant` retorna as instâncias executadas na resposta da API e não toma nenhuma ação adicional permitindo que você controle se e quando as instâncias são executadas. Para ter mais informações, consulte Tipos de solicitação da Frota do EC2.	14 de novembro de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Informações sobre economias do Spot	15/11/2016	É possível visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. Para ter mais informações, consulte Economia na compra das Instâncias spot.	5 de novembro de 2018
Suporte do console para otimização de opções de CPU	15/11/2016	Ao executar uma instância, é possível otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas usando o console do Amazon EC2. Para ter mais informações, consulte Otimizar as opções de CPU.	31 de outubro de 2018
Suporte do console para criação de um modelo de execução usando uma instância	15/11/2016	É possível criar um modelo de execução usando uma instância como a base para um novo modelo de execução usando o console do Amazon EC2. Para ter mais informações, consulte Criar um modelo de inicialização.	30 de outubro de 2018
On-Demand Capacity Reservations	15/11/2016	É possível reservar capacidade para suas instâncias do Amazon EC2 em uma zona de disponibilidade específica por qualquer duração. Isso permite criar e gerenciar Reservas de Capacidade de forma independente dos descontos de faturamento oferecidos pelas Instâncias reservadas (RI - Reserved instances). Para ter mais informações, consulte On-Demand Capacity Reservations.	25 de outubro de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Traga seus próprios endereços IP (BYOIP)	15/11/2016	É possível trazer parte ou todo o seu intervalo de endereços IPv4 públicos da rede on-premises para sua conta da AWS. Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. É possível criar um endereço IP elástico de seu grupo de endereços e usá-lo com seus recursos da AWS. Para ter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no Amazon EC2.	23 de outubro de 2018
Tag de Host dedicado na criação e suporte do console	15/11/2016	É possível marcar seus Hosts dedicados na criação e gerenciar as tags de Host dedicado usando o console do Amazon EC2. Para ter mais informações, consulte Alocar Hosts dedicados.	08 de outubro de 2018
Suporte ao console para escalabilidade programada para a frota spot	15/11/2016	Aumentar ou diminuir a capacidade atual da frota com base em data e hora. Para ter mais informações, consulte Alterar a escala da frota spot usando a escalabilidade programada.	20 de setembro de 2018
Estratégias de alocação para Frotas do EC2	15/11/2016	É possível especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). É possível especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.	26 de julho de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Estratégias de alocação para Frotas spot	15/11/2016	É possível especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). É possível especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.	26 de julho de 2018
Automação do ciclo de vida do snapshot	15/11/2016	É possível usar o Amazon Data Lifecycle Manager para automatizar a criação e a exclusão de snapshots para seus volumes do EBS. Para obter mais informações, consulte Amazon Data Lifecycle Manager.	12 de julho de 2018
Opções de CPU em modelos de execução	15/11/2016	Quando você cria um modelo de execução usando as ferramentas da linha de comando, pode otimizar as opções de CPU para se adequarem a workloads ou necessidades de negócios específicos. Para ter mais informações, consulte Criar um modelo de inicialização.	11 de julho de 2018
Marcação de Hosts dedicados	15/11/2016	É possível marcar seus Hosts dedicados. Para ter mais informações, consulte Marcação de Hosts dedicados.	3 de julho de 2018
Obter a saída mais recente do console	15/11/2016	É possível recuperar a saída mais recente do console para alguns tipos de instância usando o comando get-console-output da AWS CLI.	9 de maio de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Otimizar as opções de CPU	15/11/2016	Ao executar uma instância, é possível otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas: Para ter mais informações, consulte Otimizar as opções de CPU.	8 de maio de 2018
EC2 Fleet	15/11/2016	É possível usar a EC2 Fleet para executar um grupo de instâncias em tipos de instância do EC2 e zonas de disponibilidade diferentes, e entre modelos de compra sob demanda, instância reservada e instância spot. Para ter mais informações, consulte EC2 Fleet.	2 de maio de 2018
Instâncias sob demanda em Frotas spot	15/11/2016	É possível incluir uma solicitação de capacidade sob demanda na solicitação de frota spot para garantir que você sempre tenha capacidade de instância. Para ter mais informações, consulte Frota spot.	2 de maio de 2018
Marcar snapshots do EBS na criação	15/11/2016	É possível aplicar tags a snapshots durante a criação.	2 de abril de 2018
Alterar grupos de posicionamento	15/11/2016	É possível mover uma instância para dentro ou para fora de um grupo de posicionamento, ou alterar o grupo de posicionamento da instância. Para ter mais informações, consulte Alterar o placement group de uma instância.	1 de março de 2018
IDs mais longos de recursos	15/11/2016	É possível habilitar o formato de ID mais longo para outros tipos de recursos. Para ter mais informações, consulte IDs de recursos.	9 de fevereiro de 2018

Atributo	Versão da API	Descrição	Data de lançamento
Melhorias na performance da rede	15/11/2016	As instâncias de fora de um grupo de posicionamento de cluster podem agora se beneficiar de uma maior largura de banda para enviar ou receber tráfego de rede entre as outras instâncias ou o Amazon S3.	24 de janeiro de 2018
Marcar endereços IP elásticos	15/11/2016	É possível marcar seus endereços IP elásticos. Para ter mais informações, consulte Aplicar uma tag em um endereço IP elástico.	21 de dezembro de 2017
Amazon Time Sync Service	15/11/2016	É possível usar o Amazon Time Sync Service para manter a precisão da hora na instância. Para ter mais informações, consulte Definição do horário para a instância do Amazon EC2.	29 de novembro de 2017
T2 ilimitada	15/11/2016	As instâncias T2 ilimitadas podem apresentar uma expansão acima da linha de base pelo tempo que for necessário. Para ter mais informações, consulte Instâncias expansíveis.	29 de novembro de 2017
Modelos de execução	15/11/2016	Um modelo de execução pode conter todos ou alguns parâmetros necessários à execução de uma instância, de modo que você não precise especificá-las todas as vezes que executar uma instância. Para ter mais informações, consulte Executar uma instância a partir de um modelo de execução.	29 de novembro de 2017
Posicionamento disseminado	15/11/2016	Os grupos de posicionamento de distribuição são recomendados para aplicações com uma pequena quantidade de instâncias críticas que devem ser mantidas separadas umas das outras. Para ter mais informações, consulte Grupos de posicionamento de distribuição.	29 de novembro de 2017

Atributo	Versão da API	Descrição	Data de lançamento
Hibernação da instância spot	15/11/2016	O serviço spot pode hibernar instâncias spot em caso de interrupção. Para ter mais informações, consulte Hibernar Instâncias spot interrompida.	28 de novembro de 2017
Monitoramento do objetivo da frota spot	15/11/2016	É possível configurar políticas de dimension amento com monitoramento do objetivo para a frota spot. Para ter mais informações, consulte Alterar a escala da frota spot usando as políticas de monitoramento do objetivo.	17 de novembro de 2017
A frota spot integra-se ao Elastic Load Balancing	15/11/2016	É possível associar um ou mais load balancers a uma frota spot.	10 de novembro de 2017
Mesclagem e divisão do Instâncias reservadas conversíveis	15/11/2016	É possível trocar (mesclar) dois ou mais Instâncias reservadas conversíveis por um novo Instância reservada convertível. Também é possível usar o processo de modificação para dividir um Instância reservada convertível em reservas menores. Para ter mais informaçõ es, consulte Trocar Instâncias reservadas conversíveis.	6 de novembro de 2017
Modificar a locação da VPC	15/11/2016	É possível alterar o atributo de locação da instância da VPC de `dedicated` para `default`. Para ter mais informações, consulte Alterar a locação de uma VPC.	16 de outubro de 2017
Cobrança por segundo	15/11/2016	O Amazon EC2 cobra por segundo pela utilização baseada em Linux, com uma cobrança mínima de um minuto.	2 de outubro de 2017

Atributo	Versão da API	Descrição	Data de lançamento
Parar em interrupção	15/11/2016	É possível especificar se o Amazon EC2 deve parar ou encerrar as Instâncias spot quando elas são interrompidas. Para ter mais informações, consulte Comportamento das interrupções de instâncias spot.	18 de setembro de 2017
Marcar gateways NAT	15/11/2016	É possível marcar o gateway NAT. Para ter mais informações, consulte Marcar com tag os recursos do .	7 de setembro de 2017
Descrições de regras do grupo de segurança	15/11/2016	É possível adicionar descrições às regras do grupo de segurança. Para ter mais informaçõ es, consulte Regras de grupos de segurança.	31 de agosto de 2017
Elastic Graphics	15/11/2016	Anexe aceleradores de Elastic Graphics a suas instâncias para acelerar a performance de gráficos de suas aplicações.	29 de agosto de 2017
Recuperar endereços IP elásticos	15/11/2016	Se você liberar um endereço IP elástico para usar em um VPC, poderá recuperá-lo. Para ter mais informações, consulte Recuperar um endereço IP elástico.	11 de agosto de 2017
Marcar instâncias de frota spot	15/11/2016	É possível configurar sua frota spot para marcar automaticamente as instâncias que ela executa.	24 de julho de 2017

Atributo	Versão da API	Descrição	Data de lançamento
Recursos de tags durante a criação	15/11/2016	É possível aplicar tags a instâncias e volumes durante a criação. Para ter mais informações, consulte Marcar com tag os recursos do . Além disso, é possível usar permissões em nível de recurso baseadas em tags para controlar as tags que são aplicadas. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.	28 de março de 2017
Executar modificações em volumes do EBS anexados	15/11/2016	Com a maioria dos volumes do EBS anexados à maioria das instâncias do EC2, é possível modificar o tamanho, o tipo e as IOPS do volume sem desanexar o volume ou parar a instância.	13 de fevereiro de 2017
Anexar uma função da IAM	15/11/2016	É possível anexar, desanexar ou substituir uma função da IAM para uma instância existente. Para ter mais informações, consulte Funções do IAM para Amazon EC2.	9 de fevereiro de 2017
Instâncias spot dedicadas	15/11/2016	É possível executar Instâncias spot em hardware de único locatário em uma nuvem privada virtual (VPC). Para ter mais informações, consulte Especificar uma locação para suas Instâncias spot.	19 de janeiro de 2017
Suporte a IPv6	15/11/2016	É possível associar um CIDR IPv6 às suas VPC e sub-redes e atribuir endereços IPv6 a instâncias em sua VPC. Para ter mais informações, consulte Endereçamento IP de instâncias do Amazon EC2.	1º de dezembro de 2016

Atributo	Versão da API	Descrição	Data de lançamento
Escalabilidade automática para frota spot		Agora é possível configurar políticas de escalabilidade para a frota spot. Para ter mais informações, consulte Escalabilidade automátia para frota spot.	1º de setembro de 2016
Elastic Network Adapter (ENA)	01/04/2016	Agora é possível usar o ENA para rede avançada. Para ter mais informações, consulte Suporte a redes avançadas.	28 de junho de 2016
Suporte avançado para visualização e modificação de IDs mais longos	01/04/2016	Agora é possível visualizar e modificar as configurações de IDs mais longos para outros usuários do IAM funções do IAM ou usuários root. Para ter mais informações, consulte IDs de recursos.	23 de junho de 2016
Copiar snapshots do Amazon EBS criptografados entre contas da AWS	01/04/2016	Agora é possível copiar snapshots do EBS criptografados entre contas da AWS.	21 de junho de 2016
Capturar uma captura de tela do console de uma instância	01/10/2015	Agora é possível obter informações adicionais ao depurar instâncias não acessíveis. Para ter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.	24 de maio de 2016
Dois novos tipos de volume do EBS	01/10/2015	Agora é possível criar HDD otimizado para throughput (st1) e volumes de disco rígido frio (sc1).	19 de abril de 2016
Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2		Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2. Para ter mais informações, consulte Métricas de instância.	23 de março de 2016

Atributo	Versão da API	Descrição	Data de lançamento
Métricas do CloudWatch para frota spot		Agora é possível obter as métricas do CloudWatch para sua frota spot. Para ter mais informações, consulte Métricas do CloudWatch para frota spot.	21 de março de 2016
Instâncias programadas	01/10/2015	As instâncias reservadas programadas (instâncias programadas) permitem adquirir Reservas de Capacidade que se repetem diariamente, semanalmente ou mensalmente, com uma hora de início e duração especificadas.	13 de janeiro de 2016
IDs mais longos de recursos	01/10/2015	Gradualmente, estamos introduzindo IDs de comprimento mais longo para alguns tipos de recursos do Amazon EC2 e do Amazon EBS. Durante o período de aceitação, é possível habilitar o formato mais longo de ID para tipos de recursos compatíveis. Para ter mais informações, consulte IDs de recursos.	13 de janeiro de 2016
Suporte do DNS para o ClassicLink	01/10/2015	Você pode habilitar o suporte a DNS do ClassicLink para sua VPC de forma que os hostnames de DNS sejam endereçados entre instâncias vinculadas do EC2-Classic e instâncias na resolução da VPC para endereços IP privados e não para endereços IP públicos.	11 de janeiro de 2016
Hosts dedicados	01/10/2015	Um host de Amazon EC2 dedicado é um servidor físico com capacidade de instância dedicado para seu uso. Para ter mais informações, consulte Dedicated Hosts.	23 de novembro de 2015

Atributo	Versão da API	Descrição	Data de lançamento
Duração da instância spot	01/10/2015	Agora é possível especificar uma duração para Instâncias spot. Bloqueios pontuais não são compatíveis (janeiro de 2023).	6 de outubro de 2015
Solicitação de modificação de frota spot	01/10/2015	Agora é possível modificar a capacidade de destino de sua solicitação de frota spot. Para ter mais informações, consulte Modificar uma solicitação de frota spot.	29 de setembro de 2015
Estratégia diversificada de alocação de frota spot	15/04/2015	Agora é possível alocar instâncias spot em vários grupos spot usando uma única solicitação de frota spot. Para ter mais informações, consulte Estratégias de alocação para Instâncias spot.	15 de setembro de 2015
Peso de instâncias de frotas spot	15/04/2015	Agora é possível definir as unidades de capacidade com que cada tipo de instância contribui para a performance de sua aplicação, e ajustar o valor a ser pago por Instâncias spot para cada grupo spot de forma correspondente. Para ter mais informações, consulte Peso de instâncias de frotas spot.	31 de agosto de 2015
Nova ação de alarme de reinicialização e nova função do IAM para uso com ações de alarme		Adicionada a ação de alarme de reinicialização e a nova função do IAM para uso com ações de alarme. Para ter mais informações, consulte Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância.	23 de julho de 2015
Spot Fleets	15/04/2015	É possível gerenciar uma coleção ou uma frota de instâncias spot em vez de gerenciar solicitações separadas de instância spot. Para ter mais informações, consulte Frota spot.	18 de maio de 2015

Atributo	Versão da API	Descrição	Data de lançamento
Migrar endereços IP elásticos para o EC2-Classic	15/04/2015	É possível migrar um endereço IP elástico alocado para uso no EC2-Classic para ser usado em uma VPC.	15 de maio de 2015
Importar VMs com vários discos como AMIs	01/03/2015	O processo de VM Import agora oferece suporte à importação de VMs com vários discos como AMIs. Para obter mais informações, consulte Como importar uma VM como uma imagem usando o VM Import/Export no Guia do usuário de VM Import/Export.	23 de abril de 2015
Systems Manager		O Systems Manager permite configurar e gerenciar as instâncias do EC2.	17 de fevereiro de 2015
Systems Manager para Microsoft SCVMM 1.5		Agora é possível usar o Systems Manager para Microsoft SCVMM para executar uma instância e para importar uma VM do SCVMM para o Amazon EC2.	21 de janeiro de 2015
Recuperação automática de instâncias do EC2		É possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e recupere-a automaticamente se ocorrer um problema devido a uma falha de hardware subjacente ou um problema que exija o envolvimento da AWS para repará-lo. Uma instância recuperada é idêntica à instância original incluindo o ID da instância, os endereços IP e todos os metadados da instância. Para ter mais informações, consulte Resiliência de instância.	12 de janeiro de 2015

Atributo	Versão da API	Descrição	Data de lançamento
ClassicLink	01/10/2014	O ClassicLink permite vincular sua instância do EC2-Classic a uma VPC em sua conta. É possível associar grupos de segurança da VPC à instância do EC2-Classic habilitando a comunicação entre sua instância do EC2-Classic e as instâncias em sua VPC usando endereços IP privados.	7 de janeiro de 2015
Notificações de encerramento de instância spot		A melhor maneira de proteger-se contra a interrupção de instância spot é configurar a aplicação para ser tolerante a falhas. Além disso, é possível aproveitar os avisos de encerramento de instância spot, que enviam um aviso dois minutos antes de o Amazon EC2 encerrar a instância spot. Para ter mais informações, consulte Avisos de interrupção de instância spot.	5 de janeiro de 2015
Systems Manager para Microsoft SCVMM		O Systems Manager para Microsoft SCVMM fornece uma interface simples e fácil de usar para gerenciamento de recursos da AWS, como instâncias do EC2, no Microsoft SCVMM.	29 de outubro de 2014
Suporte à paginação de `DescribeVolumes`	01/09/2014	A API `DescribeVolumes` agora oferece suporte à paginação dos resultados com os parâmetros `MaxResults` e `NextToken`. Para obter mais informações, consulte DescribeVolumes no Amazon EC2 API Reference.	23 de outubro de 2014

Atributo	Versão da API	Descrição	Data de lançamento
Adicionado o suporte para Amazon CloudWatch Logs		É possível usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar o sistema, a aplicação e os arquivos de log personalizados em suas instâncias ou em outras origens. Em seguida, é possível recuperar os dados de log associados do CloudWatch Logs usando o console do Amazon CloudWatch, os comandos do CloudWatch Logs na CLI da AWS ou o SDK do CloudWatch Logs.	10 de julho de 2014
Nova página EC2 Service Limits		Use a página EC2 Service Limits no console do Amazon EC2 para visualizar os limites atuais dos recursos fornecidos pelo Amazon EC2 e a Amazon VPC por região.	19 de junho de 2014
Volumes de Amazon EBS Finalidade geral (SSD)	01/05/2014	Os volumes Finalidade geral (SSD) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes proporcionam latências de milissegundos de um dígito, capacidade de expansão de 3.000 IOPS por períodos estendidos e uma performance básica de 3 IOPS/GiB. Os volumes SSD de uso geral podem variar de tamanho entre 1 GiB e 1 TiB.	16 de junho de 2014
AWS Management Pack		O AWS Management Pack agora oferece suporte para o System Center Operations Manager 2012 R2.	22 de maio de 2014

Atributo	Versão da API	Descrição	Data de lançamento
Amazon EBS encryption	01/05/2014	O Criptografia de Amazon EBS oferece criptografia sem interrupção dos volumes de dados do EBS, bem como de snapshots, eliminando a necessidade de criar e manter uma infraestrutura de gerenciamento de chaves de segurança. A criptografia do EBS ativa a segurança dos dados em repouso, criptografando os dados usando as Chaves gerenciadas pela AWS. A criptografia ocorre nos servidores que hospedam as instâncias do EC2, oferecendo criptografia de dados durante seu trânsito entre as instâncias do EC2 e armazenamento do EBS.	21 de maio de 2014
Relatórios de uso do Amazon EC2		Os relatórios de uso do Amazon EC2 são um conjunto de relatórios que mostram os custos e os dados de uso do EC2.	28 de janeiro de 2014
Importação de máquinas virtuais do Linux	15/10/2013	O processo de VM Import agora oferece suporte à importação de instâncias do Linux. Para obter mais informações, consulte o VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs).	16 de dezembro de 2013
Permissões em nível de recurso para RunInstances	15/10/2013	Agora é possível criar políticas no AWS Identity and Access Management para controlar permissões em nível de recurso para a ação da API RunInstances do Amazon EC2. Para obter mais informações e políticas de exemplo, consulte Identity and Access Management para o Amazon EC2.	20 de novembro de 2013

Atributo	Versão da API	Descrição	Data de lançamento
Execução de uma instância no AWS Marketplace		Agora é possível iniciar uma instância no AWS Marketplace usando o Launch Wizard do Amazon EC2. Para ter mais informações, consulte Executar uma instância AWS Marketplace.	11 de novembro de 2013
Novo assistente de execução		Há um novo assistente de execução reprojetado do EC2. Para ter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância.	10 de outubro de 2013
Modificação dos tipos de instância de instâncias reservadas	01/10/2013	Agora é possível modificar o tipo de instância de instâncias reservadas do Linux na mesma família (por exemplo, M1, M2, M3, C1). Para ter mais informações, consulte Modificar a Instâncias reservadas.	09 de outubro de 2013
Modificação de instâncias reservadas do Amazon EC2	15/08/2013	Agora é possível modificar instâncias reservadas em uma região. Para ter mais informações, consulte Modificar a Instâncias reservadas.	11 de setembro de 2013
Atribuição de um endereço IP público	15/07/2013	Agora é possível atribuir um endereço IP público ao executar uma instância em uma VPC. Para ter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância.	20 de agosto de 2013
Concessão de permissões em nível de recurso	15/06/2013	O Amazon EC2 oferece suporte aos novos Nomes de recurso da Amazon (ARNs) e a chaves de condição. Para ter mais informações, consulte Políticas do IAM no Amazon EC2.	8 de julho de 2013

Atributo	Versão da API	Descrição	Data de lançamento
Cópias incrementais de snapshot	01/02/2013	Agora é possível executar cópias incrementais de snapshot.	11 de junho de 2013
AWS Management Pack		O AWS Management Pack vincula as instâncias do Amazon EC2 e os sistemas operacionais Windows ou Linux que são executados nelas. O AWS Management Pack é uma extensão do Microsoft System Center Operations Manager.	8 de maio de 2013
Nova página Tags		Há uma nova página Tags no console do Amazon EC2. Para ter mais informações, consulte Marcar com tag os recursos do Amazon EC2.	04 de abril de 2013
Cópia de uma AMI de uma região para outra	01/02/2013	É possível copiar uma AMI de uma região para outra, o que permite executar instâncias consistentes em mais de uma região da AWS de maneira rápida e fácil. Para ter mais informações, consulte Copiar um AMI.	11 de março de 2013
Execução de instâncias em uma VPC padrão	01/02/2013	Sua conta da AWS é capaz de iniciar instâncias no EC2-Classic ou uma VPC ou somente em uma VPC, dependendo da região. Se você puder executar instâncias somente em uma VPC, criamos uma VPC padrão para você. Quando você executa uma instância, nós a executamos em sua VPC padrão, a menos que você crie uma VPC não padrão e a especifique ao executar a instância.	11 de março de 2013

Atributo	Versão da API	Descrição	Data de lançamento
Cópia de snapshot do EBS	01/12/2012	É possível usar cópias de snapshots para criar backups de dados, para criar novos volumes do Amazon EBS ou para criar Imagens de máquina da Amazon (AMIs).	17 de dezembro de 2012
Verificações de métricas e status do EBS atualizadas para volumes do Provisioned IOPS SSD	01/10/2012	Atualizadas as métricas do EBS para incluir duas novas métricas para volumes do Provisioned IOPS SSD. Novas verificações de status também adicionadas para volumes do Provisioned IOPS SSD.	20 de novembro de 2012
Status da solicitação de instância spot	01/10/2012	O status da solicitação da instância spot facilita a determinação do estado de suas solicitações spot.	14 de outubro de 2012
Marketplace de instâncias reservadas do Amazon EC2	15/08/2012	O Marketplace de instâncias reservadas correlaciona vendedores que têm instâncias reservadas do Amazon EC2 que não são mais necessárias a compradores que desejam adquirir capacidade adicional. As instâncias reservadas adquiridas e vendidas por meio do Marketplace de instâncias reservadas funcionam como qualquer outra instância reservada, com a exceção de que têm um período de vigência padrão menor que o período de vigência padrão total e podem ser vendidas a preços diferentes.	11 de setembro de 2012
Provisioned IOPS SSD para Amazon EBS	20/07/2012	Os volumes do Provisioned IOPS SSD fornecem alta performance previsível para workloads com uso intensivo de E/S, como aplicações de banco de dados que dependem de tempos de resposta consistentes e rápidos.	31 de julho de 2012

Atributo	Versão da API	Descrição	Data de lançamento
As funções do IAM em instâncias do Amazon EC2	01/06/2012	As funções do IAM para o Amazon EC2 fornecem: • Chaves de acesso da AWS para aplicações que executam em instâncias do Amazon EC2. • Rotação automática das chaves de acesso da AWS na instância do Amazon EC2. • Permissões granulares para aplicações que executam em instâncias do Amazon EC2 que fazem solicitações para seus serviços da AWS.	11 de junho de 2012

Atributo	Versão da API	Descrição	Data de lançamento
Os recursos de instâncias spot que facilitam a familiarização e o manuseio de possíveis interrupções.		Agora é possível gerenciar suas Instâncias spot da seguinte forma: • Especifique o valor que você está disposto a pagar por Instâncias spot usando as configurações de execução de Auto Scaling e configure um cronograma para especificar o valor que você está disposto a pagar por Instâncias spot. Para obter mais informações, consulte Como executar Instâncias spot no grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling. • Obter notificações quando as instâncias forem executadas ou encerradas. • Use modelos do AWS CloudFormation para iniciar instâncias spot em uma pilha com recursos da AWS.	7 de junho de 2012
Exportação de instâncias do EC2 e time stamps para verificações de status para o Amazon EC2	01/05/2012	Suporte adicionado para exportar instâncias do Windows Server que você importou originalmente para o EC2. Suporte adicionado para time stamps no status da instância e no status do sistema para indicar a data e a hora em que uma verificação de status falhou.	25 de maio de 2012

Atributo	Versão da API	Descrição	Data de lançamento
Exportação de instâncias do EC2 e time stamps em verificações do status de instâncias e do sistema para a Amazon VPC	01/05/2012	Suporte adicionado para a exportação de instâncias do EC2 ao Citrix Xen, ao Microsoft Hyper-V e ao VMware vSphere. Suporte adicionado para time stamps em verificações de status de instâncias e do sistema.	25 de maio de 2012
AWS Marketplace AMIs	01/04/2012	Suporte adicionado para AMIs do AWS Marketplace.	19 de abril de 2012
Níveis de definição de preço de instâncias reservadas	15/12/2011	Adicionada uma nova seção que discute como beneficiar-se da definição de preço com desconto que está embutido nos níveis de definição de preço de instâncias reservadas.	5 de março de 2012
Interfaces de rede elástica (ENIs) para instâncias do EC2 na Amazon Virtual Private Cloud	01/12/2011	Adicionada nova seção sobre interfaces de rede elástica (ENIs) para instâncias do EC2 em uma VPC. Para ter mais informações, consulte Interfaces de rede elástica.	21 de dezembro de 2011
Novos tipos de ofertas para instâncias reservadas do Amazon EC2	01/11/2011	É possível escolher entre várias ofertas de instâncias reservadas que atendem a seu uso projetado da instância.	01 de dezembro de 2011

Atributo	Versão da API	Descrição	Data de lançamento
Status das instâncias do Amazon EC2	01/11/2011	É possível visualizar detalhes adicionais sobre o status de suas instâncias, incluindo eventos programados planejados pela AWS que podem ter um impacto em suas instâncias. Essas atividades operacionais incluem reinicializações de instâncias necessárias para aplicar atualizações de software ou patches de segurança, ou a baixa de instâncias necessária quando há um problema de hardware. Para ter mais informações, consulte Monitorar o status das instâncias.	16 de novembro de 2011
Instâncias spot na Amazon VPC	15/07/2011	Adição de informações sobre o suporte para Instâncias spot na Amazon VPC. Com essa atualização, os usuários podem executar Instâncias spot em uma nuvem privada virtual (VPC). Ao executar Instâncias spot em uma VPC, os usuários de Instâncias spot podem aproveitar os benefícios da Amazon VPC.	11 de outubro de 2011
Processo de VM Import simplificado para usuários das ferramentas da CLI	15/07/2011	O processo de VM Import está simplificado com a funcionalidade avançada do `ImportInstance` e do `ImportVolume`, que agora executarão o upload das imagens no Amazon EC2 depois de criar a tarefa de importação. Além disso, com a introdução do `ResumeImport`, os usuários poderão reiniciar um upload incompleto no ponto em que a tarefa parou.	15 de setembro de 2011

Atributo	Versão da API	Descrição	Data de lançamento
Suporte para importação do formato de arquivo VHD		O VM Import agora pode importar arquivos de imagem de máquina virtual em formato VHD. O formato de arquivo VHD é compatível com as plataformas de virtualização Citrix Xen e Microsoft Hyper-V. Com essa versão, o VM Import agora oferece suporte aos formatos de imagem RAW, VHD e VMDK (compatível com o VMware ESX). Para obter mais informações, consulte o VM Import/Export User Guide (Guia do usuário para importação/exportação de VMs).	24 de agosto de 2011
Atualização do Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre a versão 1.1 do Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). Essa atualização inclui suporte de proxy para acesso à Internet, melhor manipulação de erros, barra de progresso de tarefas aprimorada e várias correções de erros.	27 de junho de 2011
Alterações na definição de preço de zonas de disponibilidade de Instâncias spot	15/05/2011	Adição de informações sobre o recurso de definição de preço de zonas de disponibilidade de Instâncias spot. Nessa versão, adicionamos novas opções de definição de preço de zonas de disponibilidade como parte das informações retornadas ao consultar as solicitações de instância spot e o histórico de preços spot. Essas adições facilitam a determinação do preço requerido para executar uma instância spot em uma zona de disponibilidade específica.	26 de maio de 2011

Atributo	Versão da API	Descrição	Data de lançamento
AWS Identity and Access Management		Adicionadas informações sobre o AWS Identity and Access Management (IAM), que permite que os usuários especifiquem quais ações do Amazon EC2 um usuário pode usar com recursos do Amazon EC2 em geral. Para ter mais informações, consulte Identity and Access Management para o Amazon EC2.	26 de abril de 2011
Instâncias dedicadas		Executadas em sua Amazon Virtual Private Cloud (Amazon VPC), as instâncias dedicadas são instâncias isoladas fisicamente no nível do hardware de host. As instâncias dedicadas permitem tirar proveito da Amazon VPC e da Nuvem AWS, com benefícios que incluem provisionamento elástico sob demanda e pagamento apenas pelo que você usa e, ao mesmo tempo, isolando suas instâncias de computação do Amazon EC2 no nível do hardware. Para ter mais informações, consulte Dedicated Instances.	27 de março de 2011
Atualizações nas instâncias reservadas para o Console de Gerenciamento da AWS		As atualizações no Console de Gerenciamento da AWS facilitam que os usuários visualizem suas instâncias reservadas e comprem instâncias reservadas adicionais, incluindo instâncias reservadas dedicadas.	27 de março de 2011
Informações de metadados	01/01/2011	Adicionadas informações sobre os metadados para refletir as alterações na versão 2011-01-01. Para ter mais informações, consulte Trabalhar com metadados de instância e Categorias de metadados da instância.	11 de março de 2011

Atributo	Versão da API	Descrição	Data de lançamento
Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre o Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). O conector é um plug-in para VMware vCenter que está integrado a VMware vSphere Client e fornece uma interface gráfica de usuário que pode ser usada para importar as máquinas virtuais do VMware para o Amazon EC2.	3 de março de 2011
Forçar desanexação de volume		Agora é possível usar o AWS Management Console para forçar o desapego de um volume do Amazon EBS de uma instância.	23 de fevereiro de 2011
Proteção contra encerramento de instância		Agora é possível usar o Console de Gerenciamento da AWS para impedir que uma instância seja encerrada. Para ter mais informações, consulte Habilitar a proteção contra encerramento.	23 de fevereiro de 2011
VM Import	15/11/2010	Adicionadas informações sobre o VM Import que permite importar uma máquina virtual ou um volume no Amazon EC2. Para obter mais informações, consulte o VM Import/Export User Guide (Guia do usuário para importação/exportação de VMs).	15 de dezembro de 2010
Monitoramento básico para instâncias	31/08/2010	Adicionadas informações sobre o monitoramento básico de instâncias do EC2.	12 de dezembro de 2010

Atributo	Versão da API	Descrição	Data de lançamento
Filtros e tags	31/08/2010	Adicionadas informações sobre recursos de listagem, filtragem e marcação. Para ter mais informações, consulte Listar e filtrar seus recursos e Marcar com tag os recursos do Amazon EC2.	19 de setembro de 2010
Execução de instância idempotente	31/08/2010	Adicionadas informações sobre garantia de idempotência ao executar instâncias.	19 de setembro de 2010
AWS Identity and Access Management para o Amazon EC2		O Amazon EC2 agora se integra ao AWS Identity and Access Management (IAM). Para ter mais informações, consulte Identity and Access Management para o Amazon EC2.	2 de setembro de 2010
Designação de endereço IP da Amazon VPC	15/06/2010	Os usuários do Amazon VPC agora podem especificar o endereço IP para atribuir uma instância executada em uma VPC.	12 de julho de 2010
Monitoramento de Amazon CloudWatch para volumes de Amazon EBS		Monitoramento de Amazon CloudWatch agora está disponível automaticamente para volumes de Amazon EBS.	14 de junho de 2010
Instâncias reservadas com Windows		O Amazon EC2 agora oferece suporte a instâncias reservadas com o Windows.	22 de fevereiro de 2010