aws

Guida per l'utente

AWS Systems Manager Riferimento al runbook di automazione

AWS Systems Manager Riferimento al runbook di automazione: Guida per l'utente

Table of Contents

Riferimento al runbook del servizio di automazione di Systems Manager

Per aiutarti a iniziare rapidamente, AWS Systems Manager fornisce runbook predefiniti. Questi runbook sono gestiti da Amazon Web Services AWS Support e AWS Config. Il riferimento al runbook descrive ciascuno dei runbook predefiniti forniti da Systems Manager e. AWS Support AWS Config

> **Important**
>
> Se esegui un flusso di lavoro di automazione che richiama altri servizi utilizzando un ruolo di servizio AWS Identity and Access Management (IAM), tieni presente che il ruolo di servizio deve essere configurato con l'autorizzazione a richiamare tali servizi. Questo requisito si applica a tutti i runbook di automazione di AWS (runbook di `AWS-*`) come i runbook di `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup`, e `AWS-RestartEC2Instance`, per citarne alcuni. Questo requisito si applica anche a tutti i runbook di automazione personalizzati creati dall'utente che richiamano altri AWS servizi utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, allora dovrai configurare il ruolo di servizio con l'autorizzazione per richiamare questi servizi. È possibile abilitare le autorizzazioni per altri AWS servizi aggiungendo una policy IAM in linea al ruolo. Per ulteriori informazioni, consulta Aggiungere una policy in linea di automazione per richiamare altri servizi. AWS

Questo riferimento include argomenti che descrivono ciascuno dei runbook di Systems Manager di proprietà di AWS AWS Support, e AWS Config. I runbook sono organizzati in base ai pertinenti. AWS servizio Ogni pagina fornisce una spiegazione dei parametri obbligatori e facoltativi che è possibile specificare quando si utilizza il runbook. Ogni pagina elenca anche i passaggi del runbook e l'eventuale output dell'automazione.

Questo riferimento non include una pagina separata per i runbook che richiedono l'approvazione, come il runbook `AWS-CreateManagedLinuxInstanceWithApproval` o`AWS-StopEC2InstanceWithApproval`. Qualsiasi nome di runbook che include `WithApproval` significa che il runbook include l'azione. `aws:approve` Questa azione sospende temporaneamente un'automazione fino a quando i responsabili designati non approvano o rifiutano l'azione. Una volta raggiunto il numero richiesto di approvazioni, viene ripresa l'automazione.

Per informazioni sull'esecuzione delle automazioni, consulta Esecuzione di un'automazione semplice. Per informazioni sull'esecuzione di automazioni su più destinazioni, consulta Esecuzione di automazioni che utilizzano obiettivi e controlli di frequenza.

Argomenti

- EventBridge
- Amazon FSx
- GuardDuty
- IAM
- Flusso di dati Amazon Kinesis
- AWS KMS
- Lambda
- Amazon Managed Workflows for Apache Airflow
- Neptune
- Amazon RDS
- Amazon Redshift
- Amazon S3
- SageMaker
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- Terze parti
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

Visualizza il contenuto del runbook

È possibile visualizzare il contenuto dei runbook nella console Systems Manager.

Per visualizzare il contenuto dei runbook

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel pannello di navigazione, scegliere Documents (Documenti).

   oppure

   Se la AWS Systems Manager home page si apre per prima, scegli l'icona del menu (☰) per aprire il riquadro di navigazione, quindi scegli Documenti nel riquadro di navigazione.
3. Nella sezione Categorie, scegli Documenti di automazione.
4. Scegliere un documento, quindi scegliere View details (Visualizza dettagli).
5. Scegliere la scheda Content (Contenuti).

APIGateway

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon API Gateway. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-DeleteAPIGatewayStage
- AWSConfigRemediation-EnableAPIGatewayTracing
- AWSConfigRemediation-UpdateAPIGatewayMethodCaching

`AWSConfigRemediation-DeleteAPIGatewayStage`

Descrizione

Il `AWSConfigRemediation-DeleteAPIGatewayStage` runbook elimina una fase di Amazon API Gateway (API Gateway). AWS Configdeve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- StageArn

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della fase API Gateway che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `apigateway:GET`
- `apigateway:DELETE`

Fasi del documento

- `aws:executeScript`- Elimina la fase API Gateway specificata nel `StageArn` parametro.

AWSConfigRemediation-EnableAPIGatewayTracing

Descrizione

Il `AWSConfigRemediation-EnableAPIGatewayTracing` runbook consente il tracciamento su uno stage di Amazon API Gateway (API Gateway). AWS Configdeve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- StageArn

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della fase API Gateway su cui desideri abilitare il tracciamento.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `config:GetResourceConfigHistory`
- `apigateway:GET`
- `apigateway:PATCH`

Fasi del documento

- `aws:executeScript`- Abilita il tracciamento nella fase API Gateway specificata nel `StageArn` parametro.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descrizione

Il `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` runbook aggiorna l'impostazione del metodo di cache per una risorsa stage di Amazon API Gateway.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CachingAuthorizedMethods

  Tipo: StringList

  Descrizione: (Obbligatorio) I metodi autorizzati ad abilitare la memorizzazione nella cache. L'elenco deve essere una combinazione di `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, e`PUT`. La memorizzazione nella cache è abilitata per i metodi selezionati e disattivata per i metodi non selezionati. La memorizzazione nella cache è abilitata per tutti i metodi se `ANY` è selezionata e disattivata per tutti i metodi se `NONE` è selezionata.

- StageArn

  Tipo: String

  Descrizione: (Obbligatorio) Lo stadio API Gateway ARN per l'`RESTAPI`.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `apigateway:PATCH`
- `apigateway:GET`

Fasi del documento

- `aws:executeScript`- Accetta l'ID della risorsa dello stage come input, aggiorna l'impostazione del metodo di cache per una fase di `UpdateStage` API Gateway utilizzando l'azione API e verifica l'aggiornamento.

AWS Batch

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Batch Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

AWSSupport-TroubleshootAWSBatchJob

Descrizione

Il `AWSSupport-TroubleshootAWSBatchJob` runbook consente di risolvere i problemi che impediscono a un AWS Batch job di passare dallo stato precedente. `RUNNABLE` `STARTING`

Come funziona?

Questo runbook esegue i seguenti controlli:

- Se l'ambiente di calcolo è in uno stato `INVALID` or`DISABLED`.
- Se il `Max vCPU` parametro dell'ambiente di calcolo è sufficientemente grande da contenere il volume di lavori nella coda dei lavori.
- Se i processi richiedono più risorse vCPUs di memoria rispetto a quelle fornite dai tipi di istanza dell'ambiente di calcolo.
- Se i processi devono essere eseguiti su istanze GPU basate ma l'ambiente di calcolo non è configurato per utilizzare GPU istanze basate.
- Se il gruppo Auto Scaling per l'ambiente di calcolo non è riuscito ad avviare le istanze.
- Se le istanze avviate possono unirsi al cluster Amazon Elastic Container Service (AmazonECS) sottostante; in caso contrario, esegue il runbook AWSSupport-T roubleshootECSContainer Instance.
- Se c'è un problema di autorizzazioni che blocca azioni specifiche necessarie per eseguire il lavoro.

> **Important**
>
> - Questo runbook deve essere avviato nella stessa AWS regione del job il cui stato è bloccato. `RUNNABLE`
> - Questo runbook può essere avviato per i AWS Batch lavori pianificati su Amazon o ECS istanze AWS Fargate Amazon Elastic Compute Cloud (AmazonEC2). Se l'automazione viene avviata per un AWS Batch processo su Amazon Elastic Kubernetes Service EKS (Amazon), l'iniziazione si interrompe.

- Se le istanze sono disponibili per eseguire il job ma non riescono a registrare il ECS cluster Amazon, questo runbook avvia il runbook di `AWSSupport-TroubleshootECSContainerInstance` automazione per cercare di determinare il motivo. Per ulteriori informazioni, consulta il runbook -T InstanceAWSSupport. roubleshootECSContainer

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- JobId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del AWS Batch Job il cui `RUNNABLE` stato è bloccato.

  Modello consentito: `^[a-f0-9]{8}(-[a-f0-9]{4}){3}-[a-f0-9]{12}(:[0-9]+)?(#[0-9]+)?$`

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `batch:DescribeComputeEnvironments`
- `batch:DescribeJobs`
- `batch:DescribeJobQueues`
- `batch:ListJobs`
- `cloudtrail:LookupEvents`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetRequestHistory`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecs:DescribeClusters`
- `ecs:DescribeContainerInstances`
- `ecs:ListContainerInstances`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`

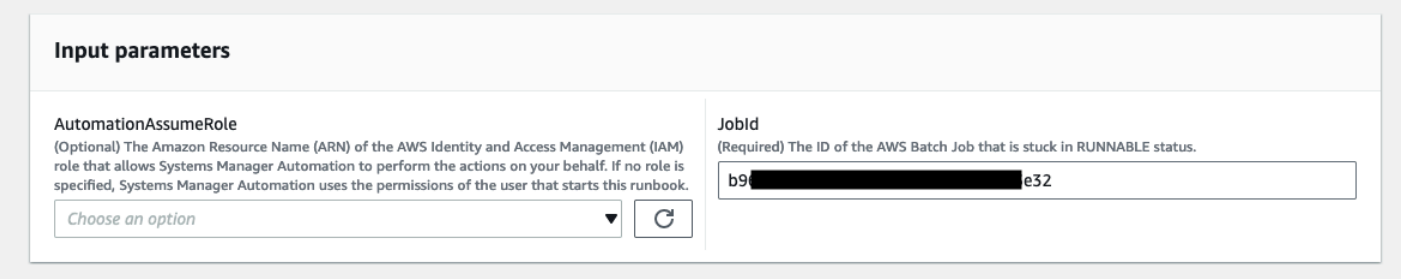
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sts:GetCallerIdentity

Istruzioni

1. Vai al AWSSupport-T roubleshootAWSBatch Job nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole(Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - JobId(Obbligatorio):

     L'ID del AWS Batch Job bloccato nello RUNNABLE stato.



4. Seleziona Esegui.
5. Notate che l'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:
   - PreflightPermissionChecks:

Esegue controlli preliminari delle IAM autorizzazioni rispetto all'utente/ruolo iniziante. Se mancano delle autorizzazioni, questo passaggio fornisce le API Azioni mancanti nella sezione Global Output.

- ProceedOnlyIfUserHasPermission:

  I rami dipendono dal fatto che si disponga delle autorizzazioni necessarie per eseguire tutte le azioni richieste per il runbook.

- AWSBatchJobEvaluation:

  Esegue controlli sul AWS Batch Job verificandone l'esistenza e lo `RUNNABLE` stato.

- ProceedOnlyIfBatchJobExistsAndIsinRunnableStato:

  Succursali in base al fatto che il lavoro esista o `RUNNABLE` meno.

- BatchComputeEnvironmentEvaluation:

  Esegue controlli rispetto all'ambiente di AWS Batch calcolo.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

  Filiali in base all'esito dei controlli dell'ambiente di calcolo.

- UnderlyingInfraEvaluation:

  Esegue controlli rispetto all'Auto Scaling Group o Spot Fleet Request sottostante.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Filiali in base alla presenza di istanze che non si uniscono al ECS cluster Amazon.

- EcsAutomationRunner:

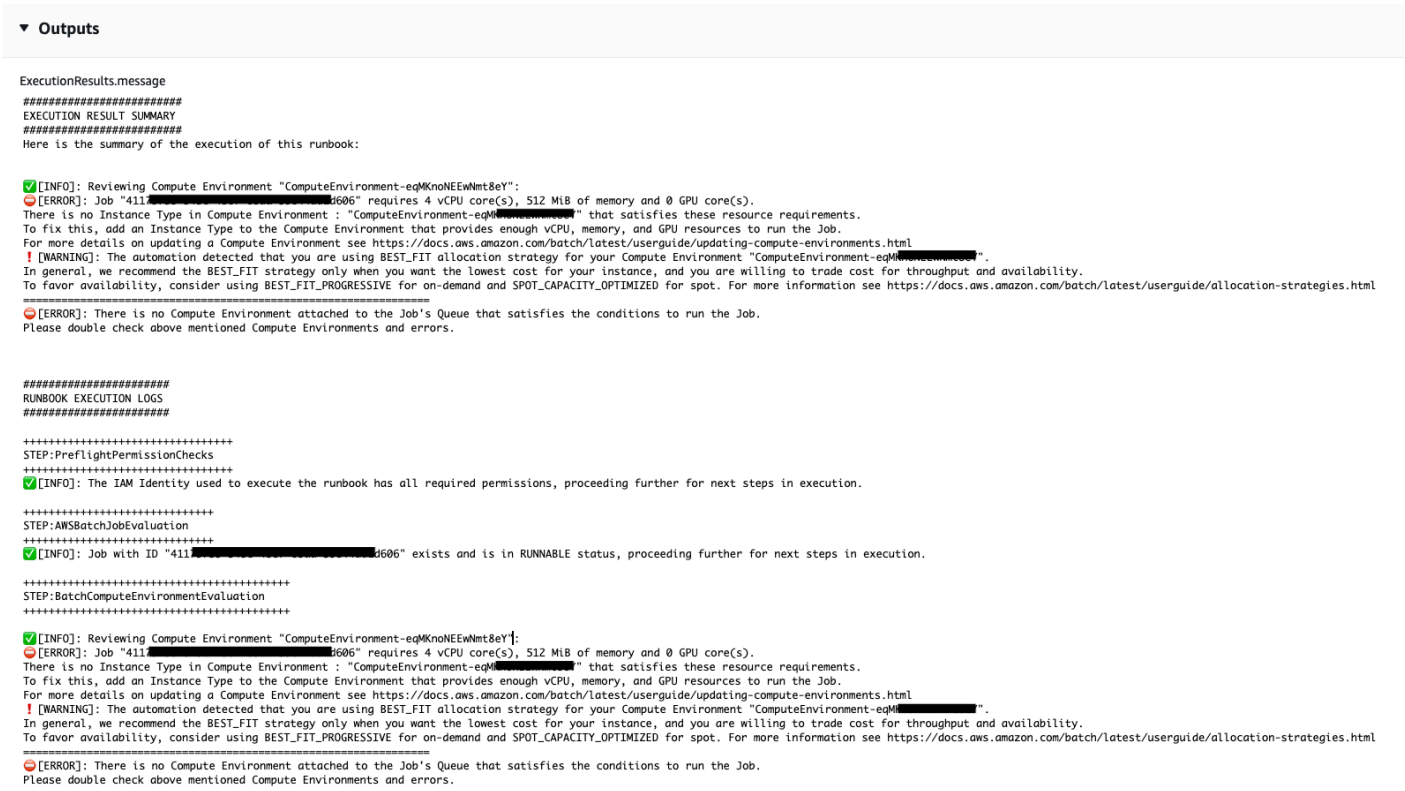
  Esegue l'ECSautomazione Amazon per le istanze che non entrano a far parte del cluster.

- ExecutionResults:

  Genera l'output in base ai passaggi precedenti.

7. Dopo il completamento, viene fornito URI il HTML file del rapporto di valutazione:

   S3 Console link e Amazon URI S3 per il report sull'esecuzione riuscita del runbook



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS CloudFormation

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CloudFormation Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification

- AWS-RunCfnLint
- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

AWS-DeleteCloudFormationStack

Descrizione

Eliminazione di uno stack di AWS CloudFormation.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- StackNameOrId

  Tipo: String

  Descrizione: (obbligatorio) Nome o ID univoco dello CloudFormation stack da eliminare

AWS-EnableCloudFormationSNSNotification

Descrizione

Il `AWS-EnableCloudFormationSNSNotification` runbook abilita le notifiche di Amazon Simple Notification Service (AmazonSNS) per lo stack AWS CloudFormation (AWS CloudFormation) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- StackArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN o il nome dello AWS CloudFormation stack per cui desideri abilitare SNS le notifiche Amazon.
- NotificationArn

  Tipo: stringa

Descrizione: (Obbligatorio) L'ARNSNSargomento Amazon che desideri associare allo AWS CloudFormation stack.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- formazione di nuvole: DescribeStacks
- formazione di nuvole: UpdateStack
- kms:Decrypt
- km: GenerateDataKey
- sns:Publish
- seggioloni: GetQueueAttributes

Fasi del documento

- CheckCfnSnsLimits (`aws:executeScript`) - Verifica che il numero massimo di SNS argomenti Amazon non sia già stato associato allo AWS CloudFormation stack specificato.
- EnableCfnSnsNotification (`aws:executeAwsApi`) - Abilita SNS le notifiche Amazon per lo AWS CloudFormation stack.
- VerificationCfnSnsNotification (`aws:executeScript`) - Verifica che SNS le notifiche Amazon siano state abilitate per lo AWS CloudFormation stack.

Output

CheckCfnSnsLimits. NotificationArnList - Un elenco di quelli ARNs che ricevono SNS notifiche Amazon per lo AWS CloudFormation stack.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Risposta dell'APIoperazione di conferma che SNS le notifiche di Amazon sono state abilitate per lo AWS CloudFormation stack.

AWS-RunCfnLint

Descrizione

Questo runbook utilizza un AWS CloudFormationLinter (`cfn-python-lint`) per convalidare i modelli YAML e JSON rispetto alle specifiche della risorsa. AWS CloudFormation Il `AWS-RunCfnLint` runbook esegue controlli aggiuntivi, ad esempio assicurando che siano stati inseriti valori validi per le proprietà delle risorse. Se la convalida non ha esito positivo, il passaggio `RunCfnLintAgainstTemplate` non riesce e l'output dello strumento linter viene fornito in un messaggio di errore. Questo runbook utilizza cfn-lint v0.24.4.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ConfigureRuleFlag

  Tipo: String

  Descrizione: (Facoltativo) Opzioni di configurazione per passare una regola al parametro `--configure-rule`.

Esempio: E2001:strict=false, E3012:strict=false.

- FormatFlag

  Tipo: String

  Descrizione: (Facoltativo) Valore da passare al parametro `--format` per specificare il formato di output.

  Valori validi: Predefinito | quiet | parseable | json

  Impostazione predefinita: Default

- IgnoreChecksFlag

  Tipo: String

  Descrizione: ID (facoltativo) delle regole da passare al parametro ignore-checks. Queste regole non sono controllate.

  Esempio: E1001, E1003, W7001

- IncludeChecksFlag

  Tipo: String

  Descrizione: (Facoltativo) ID delle regole da passare al parametro `--include-checks`. Queste regole sono controllate.

  Esempio: E1001, E1003, W7001

- InfoFlag

  Tipo: String

  Descrizione: (Facoltativo) Opzione per il parametro `--info`. Includere l'opzione per abilitare ulteriori informazioni di registrazione sull'elaborazione del modello.

  Di default: false

- TemplateFileName

  Tipo: String

  Descrizione: il nome o la chiave del file modello nel bucket S3.

- Modelli 3 BucketName

  Tipo: String

  Descrizione: il nome del bucket S3 contenente il modello di packer.
- RegionsFlag

  Tipo: String

  Descrizione: (Facoltativo) Valori da passare al `--regions` parametro for per testare il modello rispetto a quanto specificatoRegioni AWS.

  Esempio: us-east-1, us-west-1

Fasi del documento

RunCfnLintAgainstTemplate— Esegue lo `cfn-python-lint` strumento sul AWS CloudFormation modello specificato.

Output

RunCfnLintAgainstTemplate.output — Lo stdout dello strumento. `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

Descrizione

Il `AWSSupport-TroubleshootCFNCustomResource` runbook aiuta a diagnosticare il motivo per cui uno AWS CloudFormation stack non è riuscito a creare, aggiornare o eliminare una risorsa personalizzata. Il runbook controlla il token di servizio utilizzato per la risorsa personalizzata e il messaggio di errore restituito. Dopo aver esaminato i dettagli della risorsa personalizzata, l'output del runbook fornisce una spiegazione del comportamento dello stack e dei passaggi per la risoluzione dei problemi della risorsa personalizzata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- StackName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome dello AWS CloudFormation stack in cui la risorsa personalizzata ha avuto esito negativo.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation:ListStackResources`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeSubnets`

- `logs:FilterLogEvents`

Fasi del documento

- `validateCloudFormationStack`- Verifica che lo AWS CloudFormation stack esista nello stesso Account AWS e. Regione AWS
- `checkCustomResource`- Analizza lo AWS CloudFormation stack, controlla la risorsa personalizzata non riuscita e fornisce informazioni su come risolvere i problemi relativi alla risorsa personalizzata non riuscita.

AWS-UpdateCloudFormationStack

Descrizione

Aggiorna uno AWS CloudFormation stack utilizzando un AWS CloudFormation modello archiviato in un bucket Amazon S3.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN ruolo assunto da Lambda
- StackNameOrId

  Tipo: stringa

  Descrizione: (Obbligatorio) Nome o ID univoco dello AWS CloudFormation stack da aggiornare
- TemplateUrl

  Tipo: stringa

  Descrizione: (Obbligatoria) posizione del bucket S3 che contiene il modello aggiornato CloudFormation (ad es. `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. CloudFront Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject`

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` runbook configura l'oggetto root predefinito per la distribuzione Amazon CloudFront (CloudFront) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- CloudFrontDistributionId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione per cui si desidera configurare l'oggetto root predefinito.
- DefaultRootObject

  Tipo: String

  Descrizione: (Obbligatorio) L'oggetto che desideri CloudFront restituire quando una richiesta del visualizzatore punta al tuo URL principale.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

Fasi del documento

- `aws:executeScript`- Configura l'oggetto root predefinito per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook consente la registrazione degli accessi per la distribuzione Amazon CloudFront (CloudFront) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui desideri archiviare i log di accesso. I bucket in af-south-1, ap-east-1, eu-south-1 e me-south-1 non sono supportati. Regione AWS

- CloudFrontId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della distribuzione a cui desideri abilitare la registrazione degli accessi. CloudFront

- IncludeCookies

  Tipo: Booleano

  Valori validi: true | false

  Descrizione: (Obbligatorio) Imposta questo parametro su`true`, se desideri che i cookie vengano inclusi nei log di accesso.

- Prefix

  Tipo: stringa

  Descrizione: (Facoltativo) Una stringa opzionale che desideri CloudFront aggiungere come prefisso al registro degli accessi `filenames` per la tua distribuzione, ad esempio,. `myprefix/`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `s3:GetBucketLocation`

- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

> **Note**
>
> L'`s3:GetBucketLocation`API può essere utilizzata solo per i bucket S3 nello stesso account. Non puoi utilizzarla per bucket S3 con più account.

Fasi del documento

- `aws:executeScript`- Abilita la registrazione degli accessi per la CloudFront distribuzione specificata nel parametro. `CloudFrontDistributionId`

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` runbook abilita l'identità di accesso all'origine per la distribuzione Amazon CloudFront (CloudFront) specificata. Questa automazione assegna la stessa identità di accesso di CloudFront origine a tutti i tipi di origine di Amazon Simple Storage Service (Amazon S3) senza identità di accesso all'origine per la CloudFront distribuzione specificata. Questa automazione non concede l'autorizzazione di lettura all'identità di accesso di origine per accedere CloudFront agli oggetti nel tuo bucket Amazon S3. Devi aggiornare le autorizzazioni del bucket Amazon S3 per consentire l'accesso.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- CloudFrontDistributionId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui si desidera abilitare il failover di origine.
- OriginAccessIdentityId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID dell'identità di accesso all'CloudFrontorigine da associare all'origine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

Fasi del documento

- `aws:executeScript`- Abilita l'identità di accesso all'origine per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che l'identità di accesso all'origine sia stata assegnata.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontOriginFailover` runbook abilita il failover di origine per la distribuzione Amazon CloudFront (CloudFront) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- CloudFrontDistributionId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui si desidera abilitare il failover di origine.
- OriginGroupId

  Tipo: String

  Descrizione: (obbligatorio) L'ID del gruppo di origine.

- PrimaryOriginId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'origine principale nel gruppo di origine.

- SecondaryOriginId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'origine secondaria nel gruppo di origine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

Fasi del documento

- `aws:executeScript`- Abilita il failover di origine per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che il failover sia stato abilitato.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` runbook abilita la policy del protocollo di visualizzazione per la distribuzione Amazon CloudFront (CloudFront) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- CloudFrontDistributionId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui si desidera abilitare la policy del protocollo del visualizzatore.
- ViewerProtocolPolicy

  Tipo: String

  Valori validi: https-only, redirect-to-https

  Descrizione: (Obbligatorio) Il protocollo che gli utenti possono utilizzare per accedere ai file nell'origine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`

- `cloudfront:UpdateDistribution`
- `cloudfront:GetDistribution`

Fasi del documento

- `aws:executeScript`- Abilita la politica del protocollo del visualizzatore per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che la politica sia stata assegnata.

CloudTrail

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CloudTrail Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-CreateCloudTrailMultiRegionTrail
- AWS-EnableCloudTrail
- AWS-EnableCloudTrailCloudWatchLogs
- AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS
- AWS-EnableCloudTrailKmsEncryption
- AWSConfigRemediation-EnableCloudTrailLogFileValidation
- AWS-EnableCloudTrailLogFileValidation
- AWS-QueryCloudTrailLogs

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`

Descrizione

Il `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` runbook crea un AWS CloudTrail (CloudTrail) trail che invia file di log da più utenti Regioni AWS al bucket Amazon Simple Storage Service (Amazon S3) di tua scelta.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BucketName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 in cui desideri caricare i log.
- KeyPrefix

  Tipo: String

  Descrizione: (Facoltativo) Il prefisso chiave Amazon S3 che segue il nome del bucket che hai designato per la consegna dei file di registro.
- TrailName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome del CloudTrail percorso da creare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`
- `cloudtrail:GetTrail`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:PutBucketLogging`
- `s3:ListBucket`

Fasi del documento

- `aws:executeAwsApi`- Accetta il nome del percorso e il nome del bucket Amazon S3 come input e crea un CloudTrail percorso.
- `aws:executeAwsApi`- Consente la registrazione sul percorso creato e avvia la consegna dei log nel bucket Amazon S3 specificato.
- `aws:assertAwsResourceProperty`- Verifica che il CloudTrail percorso sia stato creato.

AWS-EnableCloudTrail

Descrizione

Crea un trail AWS CloudTrail e configura l'accesso a un bucket S3.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- S3 BucketName

  Tipo: String

  Descrizione: (obbligatoria) nome del bucket S3 designato per la pubblicazione dei file di log.

  > **Note**
  >
  > Il bucket S3 deve esistere e la policy del bucket deve concedere a CloudTrail l'autorizzazione di scrittura nel bucket stesso. Per informazioni, consulta la politica dei bucket di Amazon S3 per. CloudTrail
- TrailName

  Tipo: String

  Descrizione: (obbligatorio) nome del nuovo trail.

AWS-EnableCloudTrailCloudWatchLogs

Descrizione

Questo runbook aggiorna la configurazione di uno o più AWS CloudTrail trail per inviare eventi a un gruppo di log di Amazon CloudWatch Logs.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- CloudWatchLogsLogGroupArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN del gruppo di log CloudWatch Logs in cui verranno CloudTrail consegnati i log.
- CloudWatchLogsRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN del ruolo IAM CloudWatch Logs Logs presuppone la scrittura nel gruppo di log specificato.
- TrailNames

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole dei nomi dei CloudTrail percorsi di cui si desidera inviare gli eventi ai CloudWatch registri.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudtrail:UpdateTrail`
- `iam:PassRole`

Fasi del documento

- `aws:executeScript`- Aggiorna i CloudTrail percorsi specificati per fornire eventi al gruppo di log CloudWatch Logs specificato.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Descrizione

Il `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` runbook crittografa un percorso AWS CloudTrail (CloudTrail) utilizzando la chiave AWS Key Management Service (AWS KMS) gestita dal cliente che hai specificato. Questo runbook deve essere utilizzato solo come base per garantire che i CloudTrail percorsi siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Ti consigliamo di crittografare più percorsi con chiavi KMS diverse. CloudTrailI file digest non sono crittografati. Se in precedenza hai impostato il `EnableLogFileValidation` parametro su `true` per il percorso, consulta la sezione «Utilizza la crittografia lato server con chiavi AWS KMS gestite» dell'argomento CloudTrailPreventative Security Best Practices nella Guida per l'AWS CloudTrailutente per ulteriori informazioni.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KM KeyId

  Tipo: String

  Descrizione: (Obbligatorio) L'ARN, l'ID chiave o l'alias chiave della chiave gestita dal cliente che desideri utilizzare per crittografare il percorso specificato nel parametro. `TrailName`

- TrailName

  Tipo: String

  Descrizione: (Obbligatorio) L'ARN o il nome del percorso che desideri aggiornare devono essere crittografati.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia sul percorso specificato nel `TrailName` parametro.
- `aws:executeAwsApi`- Raccoglie l'ARN per la chiave gestita dal cliente specificata nel `KMSKeyId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata sul CloudTrail percorso.

AWS-EnableCloudTrailKmsEncryption

Descrizione

Questo runbook aggiorna la configurazione di uno o più AWS CloudTrail percorsi per utilizzare la crittografia AWS Key Management Service (AWS KMS).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- KMS KeyId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente che desideri utilizzare per crittografare la traccia specificata nel `TrailName` parametro. Il valore può essere un nome alias preceduto da «alias/», un ARN completamente specificato in un alias o un ARN completamente specificato in una chiave.
- TrailNames

  Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole dei percorsi che desideri aggiornare per essere crittografati.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudtrail:UpdateTrail`
- `kms:DescribeKey`
- `kms:ListKeys`

Fasi del documento

- `aws:executeScript`- Abilita AWS KMS la crittografia sui percorsi specificati nel `TrailName` parametro.

`AWSConfigRemediation-EnableCloudTrailLogFileValidation`

Descrizione

Il `AWSConfigRemediation-EnableCloudTrailLogFileValidation` runbook consente la convalida dei file di registro per il percorso. AWS CloudTrail

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- TrailName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome o Amazon Resource Name (ARN) del percorso per il quale desideri abilitare la convalida dei log.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

Fasi del documento

- `aws:executeAwsApi`- Abilita la convalida del registro per il AWS CloudTrail percorso specificato nel `TrailName` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la convalida dei log sia abilitata per il percorso.

AWS-EnableCloudTrailLogFileValidation

Descrizione

Il `AWS-EnableCloudTrailLogFileValidation` runbook consente la convalida dei file di registro per i AWS CloudTrail percorsi specificati.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- TrailNames

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole dei nomi dei CloudTrail percorsi per i quali si desidera abilitare la convalida dei log.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

Fasi del documento

- `aws:executeScript`- Abilita la convalida dei log per i AWS CloudTrail percorsi specificati nel `TrailNames` parametro.

AWS-QueryCloudTrailLogs

Descrizione

Il `AWS-QueryCloudTrailLogs` runbook crea una tabella Amazon Athena dal bucket Amazon Simple Storage Service (Amazon S3) di tua scelta contenente AWS CloudTrail () log. CloudTrail Dopo aver creato la tabella, l'automazione esegue le query SQL specificate e quindi elimina la tabella.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Query

  Tipo: String

  Descrizione: (Obbligatoria) La query SQL che si desidera eseguire.

- SourceBucketPath

  Tipo: String

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 contenente i file di CloudTrail registro che desideri interrogare.

- TableName

  Tipo: String

  Descrizione: (Facoltativo) Il nome della tabella Athena creata dall'automazione.

  Impostazione predefinita: cloudtrail_logs

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `athena:GetQueryResults`
- `athena:GetQueryExecution`
- `athena:StartQueryExecution`
- `glue:CreateTable`
- `glue:DeleteTable`
- `glue:GetDatabase`
- `glue:GetPartitions`
- `glue:GetTable`
- `s3:AbortMultipartUpload`
- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`

Fasi del documento

- `aws:executeAwsApi`- Crea un tavolo Athena.
- `aws:executeAwsApi`- Esegue la stringa di query specificata nel `Query` parametro.
- `aws:executeScript`- Sondaggi e attende il completamento della richiesta.
- `aws:executeAwsApi`- Ottiene i risultati dell'interrogazione.
- `aws:executeAwsApi`- Elimina la tabella creata dall'automazione.

CloudWatch

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. CloudWatch Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

`AWS-ConfigureCloudWatchOnEC2Instance`

Descrizione

Abilita o disabilita il monitoraggio CloudWatch dettagliato di Amazon sulle istanze gestite.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 su cui desideri abilitare il CloudWatch monitoraggio.
- properties

  Tipo: String

  Descrizione: (Facoltativo) Questo parametro non è supportato. È elencato qui per la compatibilità con le versioni precedenti.
- status

  Valori validi: Abilitato | Disabilitato

  Descrizione: (facoltativo) specifica se abilitare o disabilitare CloudWatch.

  Impostazione predefinita: Enabled

Fasi del documento

configureCloudWatch- Si configura CloudWatch sull'istanza Amazon EC2 con lo stato specificato.

Output

Questa automazione non ha alcun output.

AWS-EnableCWAlarm

Descrizione

Il `AWS-EnableCWAlarm` runbook crea allarmi Amazon CloudWatch (CloudWatch) per le AWS risorse del tuo computer Account AWS che non ne hanno già uno. CloudWatch gli allarmi vengono creati per le seguenti risorse: AWS

- Istanze Amazon Elastic Compute Cloud (Amazon EC2)
- Volumi Amazon Elastic Block Store (Amazon EBS)
- Bucket Amazon Simple Storage Service (Amazon S3)
- Cluster Amazon Relational Database Service (Amazon RDS)

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ComparisonOperator

  Tipo: stringa

  Valori validi: GreaterThanOrEqualToThreshold | | GreaterThanThreshold | LessThanLowerOrGreaterThanUpper Threshol GreaterThanUpperThreshold | | | LessThanLowerThreshold LessThanOrEqualToThreshold LessThanThreshold

Descrizione: (Obbligatoria) L'operazione aritmetica da utilizzare per confrontare la statistica e la soglia specificate.

- MetricName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della metrica associata all'allarme.

- Periodo

  Tipo: integer

  Valori validi: 10 | 30 | 60 | Un multiplo di 60

  Descrizione: (Obbligatorio) Il periodo, in secondi, durante il quale viene applicata la statistica.

- Resource ARNS

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole degli ARN delle risorse per cui creare un CloudWatch allarme

- Statistic

  Tipo: stringa

  Valori validi: Media | Massimo | Minimo | SampleCount | Somma

  Descrizione: (Obbligatoria) La statistica per la metrica associata all'allarme.

- Threshold

  Tipo: integer

  Descrizione: (Obbligatorio) Il valore da confrontare con la statistica specificata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudwatch:PutMetricAlarm`

Fasi del documento

- `aws:executeScript`- Crea un CloudWatch allarme in base ai valori specificati nei parametri del runbook per le risorse specificate nel `ResourceARNs` parametro.

Output

Abilita CWALarm. FailedResources: Una mappatura degli ARN di risorse per i quali non è stato creato un CloudWatch allarme e il motivo dell'errore.

Abilita CW Alarm. SuccessfulResources: Un elenco di ARN di risorse per i quali è stato creato correttamente un CloudWatch allarme.

Amazon DocumentDB

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon DocumentDB (con compatibilità con MongoDB). Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableDocDbClusterBackupRetentionPeriod

`AWS-EnableDocDbClusterBackupRetentionPeriod`

Descrizione

Il `AWS-EnableDocDbClusterBackupRetentionPeriod` runbook consente un periodo di conservazione dei backup per il cluster Amazon DocumentDB specificato. Questa funzionalità imposta il numero totale di giorni per i quali viene conservato un backup automatico. Per modificare un cluster, il cluster deve essere nello stato disponibile con un tipo di motore di`docdb`.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DBClusterResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della risorsa per il cluster Amazon DocumentDB per cui desideri abilitare il periodo di conservazione del backup.
- BackupRetentionPeriod

  Tipo: integer

  Descrizione: (Obbligatorio) Il numero di giorni per i quali vengono conservati i backup automatici. Deve essere un valore compreso tra 7 e 35 giorni.
- PreferredBackupWindow

  Tipo: stringa

  Descrizione: (Facoltativo) Un intervallo di tempo giornaliero in Universal Time Coordinated (UTC) nel formato hh24:mm-hh24:mm, ad esempio 07:14-07:44. Il valore deve essere di almeno 30 minuti e non può essere in conflitto con la finestra di manutenzione preferita.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `docdb:DescribeDBClusters`

- `docdb:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- GetDocDbClusterIdentifier (`aws:executeAwsApi`) - Restituisce l'identificatore del cluster Amazon DocumentDB utilizzando l'ID di risorsa fornito.
- VerifyDocDbEngine (`aws:assertAwsResourceProperty`) - Verifica che il tipo `docdb` di motore Amazon DocumentDB serva a prevenire modifiche involontarie ad altri tipi di motore Amazon. RDS
- VerifyDocDbStatus (`aws:waitAwsResourceProperty`) - Verifica che lo stato del cluster Amazon DocumentDB sia. `available`
- ModifyDocDbRetentionPeriod (`aws:executeAwsApi`) - Imposta il periodo di conservazione utilizzando i valori forniti per il cluster Amazon DocumentDB specificato.
- VerifyDocDbBackupsEnabled (`aws:executeScript`) - Verifica che il periodo di conservazione per il cluster Amazon DocumentDB e la finestra di backup preferita, se specificata, siano state impostate correttamente.

Output

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - Risposta dell'`ModifyDBCluster`APIoperazione.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse - Output della `VerifyDocDbBackupsEnabled` fase di conferma dell'avvenuta modifica del cluster Amazon DocumentDB.

CodeBuild

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CodeBuild Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Descrizione

Il AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK runbook crittografa gli artefatti di compilazione di un progetto AWS CodeBuild (CodeBuild) utilizzando la chiave gestita dal cliente AWS Key Management Service (AWS KMS) specificata. AWS Config deve essere abilitato nel luogo in Regione AWS cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  -Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KMS KeyId

  -Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare il CodeBuild progetto specificato nel parametro. ProjectId

- ProjectId

- Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del CodeBuild progetto di cui desideri crittografare gli artefatti di build.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `codebuild:BatchGetProjects`
- `codebuild:UpdateProject`
- `config:GetResourceConfigHistory`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome del CodeBuild progetto dall'ID del progetto.
- `aws:executeAwsApi`- Abilita la crittografia sul CodeBuild progetto specificato nel `ProjectId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata nel CodeBuild progetto.

Output

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Risposta dalla chiamata `UpdateFunctionConfiguration` API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descrizione

Il `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` runbook elimina le variabili di `AWS_SECRET_ACCESS_KEY` ambiente `AWS_ACCESS_KEY_ID` e il progetto AWS

CodeBuild (CodeBuild) specificato. AWS Configdeve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ResourceId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID del CodeBuild progetto di cui si desidera eliminare le variabili di ambiente chiave di accesso.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`

- `codebuild:BatchGetProjects`
- `codebuild:UpdateProject`

Fasi del documento

- `aws:executeScript`- Elimina le variabili di ambiente della chiave di accesso per il CodeBuild progetto specificato nel `ResourceId` parametro.

AWS CodeDeploy

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CodeDeploy Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-TroubleshootCodeDeploy

`AWSSupport-TroubleshootCodeDeploy`

Descrizione

Il `AWSSupport-TroubleshootCodeDeploy` runbook aiuta a diagnosticare il motivo per cui un'AWS CodeDeployimplementazione non è riuscita su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Il runbook riporta i passaggi per aiutarti a risolvere il problema o a risolverlo ulteriormente. CodeDeployVengono inoltre fornite le migliori pratiche per aiutarti a evitare problemi simili in futuro.

Questo runbook può aiutarti a risolvere i seguenti problemi:

- L'CodeDeployagente non è installato o non è in esecuzione sull'istanza Amazon EC2
- L'istanza Amazon EC2 non dispone di un profilo di istanza AWS Identity and Access Management (IAM) collegato
- Il profilo dell'istanza IAM collegato all'istanza Amazon EC2 non dispone delle autorizzazioni Amazon Simple Storage Service (Amazon S3) richieste
- Manca una revisione archiviata in Amazon S3 oppure il bucket Amazon S3 utilizzato si trova in un'istanza diversa da Regione AWS quella di Amazon EC2

- Problemi relativi ai file delle specifiche dell'applicazione (AppSpec)
- Errori «Il file esiste già nella posizione»
- Hook degli eventi del ciclo di vita CodeDeploy gestito non riusciti
- Eventi relativi al ciclo di vita gestito dai clienti con errori
- Eventi di scalabilità durante l'implementazione

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DeploymentId

  Tipo: String

  Descrizione: (obbligatorio) L'ID della distribuzione non riuscita.
- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 in cui la distribuzione non è riuscita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `codedeploy:GetDeployment`
- `codedeploy:GetDeploymentTarget`
- `ec2:DescribeInstances`

Fasi del documento

- `aws:executeAwsApi`- Verifica i valori forniti per i `InstanceId` parametri `DeploymentId` and.
- `aws:executeScript`- Raccoglie informazioni dall'istanza Amazon EC2 come lo stato dell'istanza e i dettagli del profilo dell'istanza IAM.
- `aws:executeScript`- Esamina la distribuzione specificata e restituisce un'analisi del motivo per cui la distribuzione non è riuscita.

AWS Config

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Config Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-SetupConfig

`AWSSupport-SetupConfig`

Descrizione

Il `AWSSupport-SetupConfig` runbook crea un ruolo collegato ai servizi AWS Identity and Access Management (IAM), un registratore di configurazione basato su e un canale di AWS Config distribuzione con un bucket Amazon Simple Storage Service (Amazon S3) in cui AWS Config invia istantanee di configurazione e file di cronologia della configurazione. Se si specificano valori per i `AggregatorAccountRegion` parametri `AggregatorAccountId` and, il runbook crea anche autorizzazioni per l'aggregazione dei dati per raccogliere dati di AWS Config configurazione e

conformità da più e più Account AWS dati. Regioni AWS Per ulteriori informazioni sull'aggregazione di dati da più account e regioni, consulta Aggregazione di dati multiaccount in più regioni nella Guida per gli sviluppatori. AWS Config

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- AggregatorAccountId

  Tipo: String

  Descrizione: (Facoltativo) L'ID del Account AWS luogo in cui verrà aggiunto un aggregatore per aggregare i dati di AWS Config configurazione e conformità di più account e. Regioni AWS Questo account viene utilizzato anche dall'aggregatore per autorizzare gli account di origine.
- AggregatorAccountRegion

  Tipo: String

  Descrizione: (Facoltativo) La regione in cui verrà aggiunto un aggregatore per aggregare i dati di AWS Config configurazione e conformità di più account e regioni.
- IncludeGlobalResourcesRegion

Tipo: String

Predefinito: us-east-1

Descrizione: (Obbligatorio) Per evitare di registrare i dati globali delle risorse in ciascuna regione, specificare una regione da cui registrare i dati globali delle risorse.

- Partizione

  Tipo: String

  Impostazione predefinita: `aws`

  Descrizione: (Obbligatoria) La partizione da cui si desidera raccogliere i dati di AWS Config configurazione e conformità.

- S3 BucketName

  Tipo: String

  Impostazione predefinita: `aws-config-delivery-channel`

  Descrizione: (Facoltativo) Il nome che desideri applicare al bucket Amazon S3 creato per il canale di consegna. L'ID dell'account viene aggiunto alla fine del nome.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:DescribeConfigurationRecorders`
- `config:DescribeDeliveryChannels`
- `config:PutAggregationAuthorization`
- `config:PutConfigurationRecorder`
- `config:PutDeliveryChannel`
- `config:StartConfigurationRecorder`
- `iam:CreateServiceLinkedRole`

- `iam:PassRole`
- `s3:CreateBucket`
- `s3:ListAllMyBuckets`
- `s3:PutBucketPolicy`

Fasi del documento

- `aws:executeScript`- Crea un ruolo IAM collegato al servizio AWS Config se non ne esiste già uno.
- `aws:executeScript`- Crea un registratore di configurazione se non ne esiste già uno.
- `aws:executeScript`- Crea un bucket Amazon S3 da utilizzare dal canale di distribuzione, se non ne esiste già uno.
- `aws:executeScript`- Crea un canale di distribuzione utilizzando le risorse create dal runbook.
- `aws:executeAwsApi`- Avvia il registratore di configurazione.
- `aws:executeScript`- Se sono stati specificati valori per i `AggregatorAccountRegion` parametri `AggregatorAccountId` and, vengono configurate le autorizzazioni per l'aggregazione di dati tra più account e più regioni.

Amazon Connect

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Connect. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows
- AWSSupport-CollectAmazonConnectContactFlowLog

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`

Descrizione

Ti `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` aiuta ad associare i numeri di telefono ai flussi di contatti nella tua istanza Amazon Connect. Fornendo le mappature dei numeri di telefono e dei flussi di contatti in un file di input con valori separati da virgole (CSV),

il runbook associa il maggior numero possibile di numeri di telefono ai flussi di contatti entro 14,5 minuti. Il runbook produce un CSV file con tutte le coppie di numeri di telefono e flussi di contatti che non è riuscito ad associare entro il limite di tempo, in modo da poterle inserire nella prossima esecuzione.

Come funziona?

Il runbook ti `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` aiuta ad associare i numeri di telefono ai flussi di contatti nella tua istanza Amazon Connect utilizzando un CSV file di dati di mappatura archiviato in un bucket Amazon Simple Storage Service (Amazon S3). Il CSV file di input deve essere allineato al seguente formato, con `PhoneNumber` valori in formato E.164.

Esempio di file di input CSV

```
PhoneNumber,ContactFlowName
+1800555xxxx,ContactFlowA
+1800555yyyy,ContactFlowB
+1800555zzzz,ContactFlowC
```

Il runbook di automazione crea anche i seguenti file nella posizione di destinazione specificata in `DestinationFileBucket` and`DestinationFilePath`.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: Un file temporaneo che contiene le `ContactFlowId` coppie `PhoneNumberId` and necessarie per. `AssociatePhoneNumberContactFlow` API
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: Un file che contiene il numero di telefono e le coppie del flusso di contatti che non è stato possibile elaborare a causa di un errore, ad esempio `ResourceNotFoundException` nel formato di`PhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: Un file che contiene il numero di telefono e le coppie di flussi di contatti che non sono state elaborate. Il runbook tenta di elaborare il maggior numero possibile di numeri di telefono e flussi di contatti entro 14,5 minuti (15 minuti di timeout della AWS Lambda funzione - 30 secondi di buffer). Se alcuni numeri di telefono o flussi di contatti non possono essere elaborati a causa del vincolo di tempo, il runbook li include in un CSV file da utilizzare come input per la successiva esecuzione del runbook.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Statement": [
        {
            "Action": [
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketAcl",
                "s3:GetObject",
                "s3:GetObjectAttributes",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
            "arn:aws:s3:::YOUR-BUCKET/*",
            "arn:aws:s3:::YOUR-BUCKET"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DeleteStack",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
```

```
                    "iam:GetRole",
                    "iam:PutRolePolicy",
                    "lambda:CreateFunction",
                    "lambda:DeleteFunction",
                    "lambda:GetFunction",
                    "lambda:InvokeFunction",
                    "lambda:TagResource",
                    "connect:AssociatePhoneNumberContactFlow",
                    "logs:CreateLogGroup",
                    "logs:TagResource",
                    "logs:PutRetentionPolicy",
                    "logs:DeleteLogGroup",
                    "s3:GetAccountPublicAccessBlock"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "connect:DescribeInstance",
                    "connect:ListPhoneNumbers",
                    "connect:ListContactFlows",
                    "ds:DescribeDirectories"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Condition": {
                    "StringLikeIfExists": {
                        "iam:PassedToService": [
                            "ssm.amazonaws.com",
                            "lambda.amazonaws.com"
                        ]
                    }
                },
                "Action": [
                    "iam:PassRole"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere AWSSupport-AssociatePhoneNumbersToConnectContactFlowsa Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo)

     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - ConnectInstanceId (Obbligatorio)

     L'ID della tua istanza Amazon Connect.
   - SourceFileBucket (Obbligatorio)

     Il bucket Amazon S3 che archivia il CSV file che contiene il numero di telefono e le coppie di flussi di contatti.
   - SourceFilePath (Obbligatorio)

     La chiave oggetto Amazon S3 del CSV file che contiene il numero di telefono e le coppie di flussi di contatti. Ad esempio `path/to/input.csv`.
   - DestinationFileBucket (Obbligatorio)

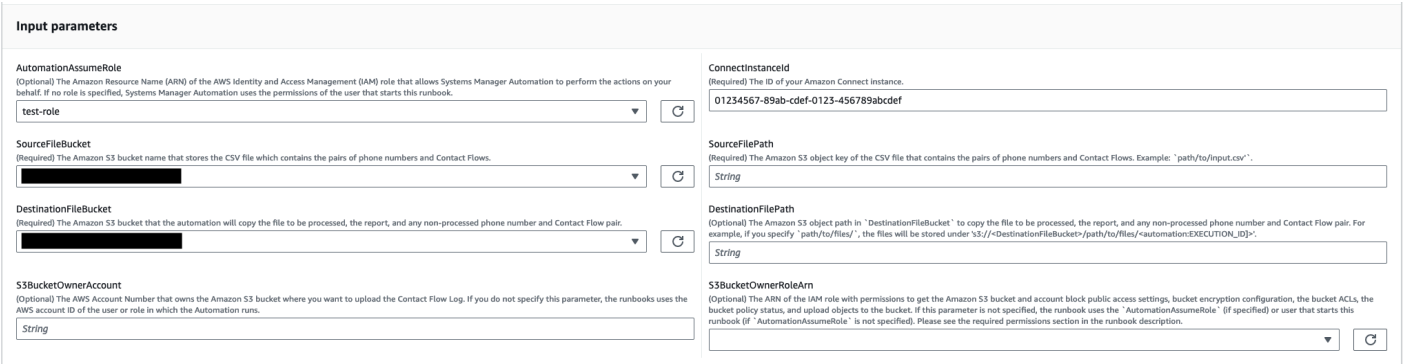
     Il bucket Amazon S3 in cui l'automazione inserirà un file intermedio e un rapporto sui risultati.
   - DestinationFilePath (Facoltativo)

     Il percorso dell'oggetto Amazon S3 `DestinationFileBucket` in cui archiviare un file intermedio e un report sui risultati. Ad esempio, se si specifica`path/to/files/`, i file vengono archiviati in. `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`
   - S3 BucketOwnerAccount (opzionale)

Il numero di AWS account proprietario del bucket Amazon S3 in cui desideri caricare il registro del flusso di contatti. Se non specifichi questo parametro, i runbook utilizzano l'ID AWS account dell'utente o del ruolo in cui viene eseguita l'automazione.

- S3 BucketOwnerRoleArn (opzionale)

  Il IAM ruolo con le autorizzazioni per ottenere le impostazioni ARN di accesso pubblico del bucket Amazon S3 e dell'account, la configurazione della crittografia dei bucket, il bucket, lo stato della policy del ACLs bucket e il caricamento di oggetti nel bucket. Se questo parametro non è specificato, il runbook utilizza l'utente `AutomationAssumeRole` (se specificato) o che avvia questo runbook (se non è specificato). `AutomationAssumeRole` Consulta la sezione sulle autorizzazioni richieste nella descrizione del runbook.



4. Seleziona Esegui.
5. L'automazione si avvia.
6. Il documento esegue le seguenti operazioni:
   - CheckConnectInstanceExistance

     Verifica se l'istanza Amazon Connect fornita `ConnectInstanceId` esiste.
   - Controlla S3 BucketPublicStatus

     Verifica se i bucket Amazon S3 specificati in `SourceFileBucket` e `DestinationFileBucket` consentono autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.
   - CheckSourceFileExistenceAndSize

     Verifica se il CSV file sorgente specificato in `SourceFilePath` esiste e se la dimensione del file supera il limite di 25 MiB.
   - GenerateResourceIdMap

Scarica il CSV file sorgente specificato in `SourceFilePath` and identify `PhoneNumberId` e `ContactFlowId` per ogni risorsa. Al termine, carica un CSV file che contiene`PhoneNumber`, `PhoneNumberId``ContactFlowName`, e `ContactFlowId` nel bucket Amazon S3 di destinazione specificato in. `DestinationFileBucket` Se `PhoneNumberId` non può essere identificato per un determinato numero, il file sarà vuoto nel file. CSV

- AssociatePhoneNumbersToContactFlows

  Crea una AWS Lambda funzione nel tuo account utilizzando uno AWS CloudFormation stack. La AWS Lambda funzione associa ogni numero a un flusso di contatti elencato nel CSV file sorgente specificato in `SourceFileBucket` e `SourceFilePath` e lo AWS CloudFormation stack richiama la funzione. La AWS Lambda funzione associa il maggior numero possibile di numeri di telefono ai flussi di contatto prima del timeout (15 minuti). L'elenco dei numeri di telefono e dei flussi di contatti che non è stato possibile elaborare a causa di un errore viene caricato in`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Vengono caricati quelli che non è stato possibile elaborare a causa di un eccesso del numero massimo di numeri di telefono che possono essere elaborati in un'unica esecuzione`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Se questo passaggio fallisce, passa alla `DescribeCloudFormationErrorFromStackEvents` fase che mostra il motivo dell'errore in base agli eventi AWS CloudFormation dello stack.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Attende che venga creata la AWS Lambda funzione che mappa i numeri di telefono ai flussi di contatti e che lo AWS CloudFormation stack completi la sua chiamata.

- GenerateReport

  Genera il rapporto che contiene il numero di numeri di telefono mappati ai flussi di contatti, quelli che non è stato possibile elaborare a causa di un errore e quelli che non hanno potuto essere elaborati a causa di un eccesso del numero massimo di numeri di telefono che possono essere elaborati in un'unica esecuzione. Il rapporto mostra anche la posizione (Amazon S3 URI e URL console Amazon S3) di `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` o, se `[automation:EXECUTION_ID]/ErrorResourceList.csv` applicabile.

- **`DeleteCloudFormationStack`**

  Elimina lo AWS CloudFormation stack, inclusa la funzione Lambda per la mappatura.

- **`DescribeCloudFormationErrorFromStackEvent`**

Descrive gli errori della pila del AWS CloudFormation passo. `AssociatePhoneNumbersToContactFlows`

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

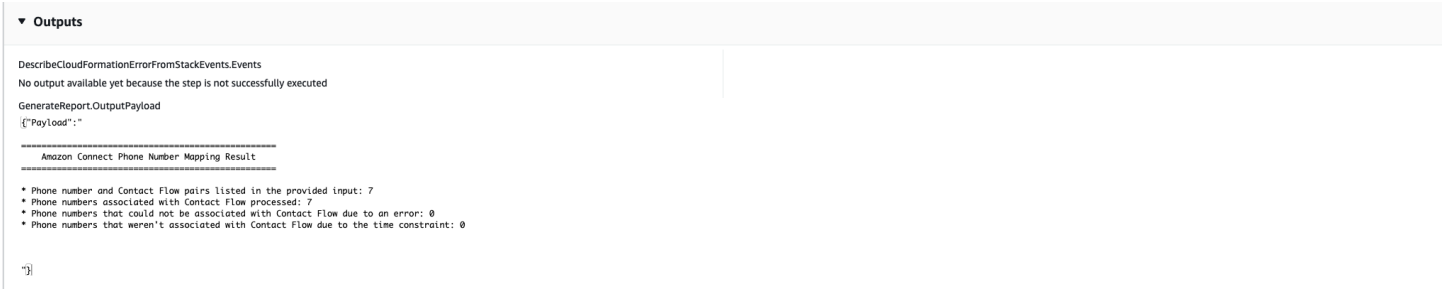
   - GenerateReport.OutputPayload

     Emissione delle associazioni tra numeri di telefono e flussi di contatti. Questo rapporto contiene le seguenti informazioni:

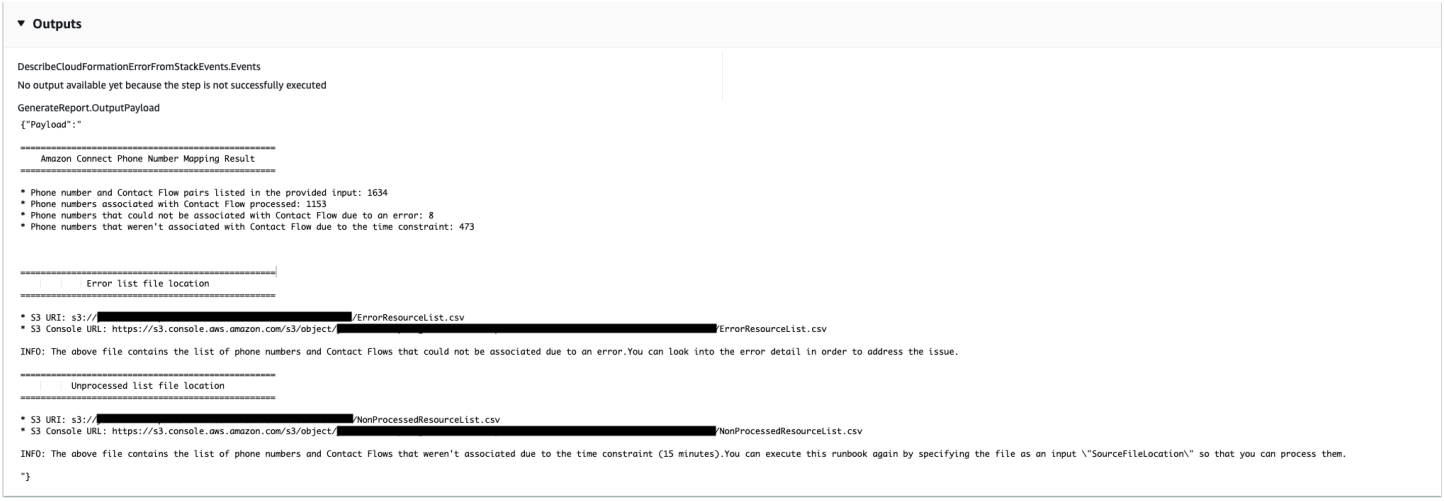
     - Il numero di coppie di numeri di telefono e flussi di contatti elencate nel CSV file di input
     - Il numero di numeri di telefono associati ai flussi di contatti come specificato nel CSV file di input
     - Il numero di numeri di telefono che non è stato possibile associare ai flussi di contatti a causa di un errore
     - Il numero di numeri di telefono che non sono stati associati ai flussi di contatti a causa di vincoli di tempo
     - La posizione (Amazon S3 URI e URL console Amazon S3) del file che contiene CSV il numero di telefono e le coppie di flussi di contatti che non è stato possibile associare a causa di un errore
     - La posizione (Amazon S3 URI e Amazon S3 URL Console) del file che contiene CSV il numero di telefono e le coppie di flussi di contatti che non erano associate a causa di vincoli di tempo
   - DescribeCloudFormationErrorFromStackEvents.Eventi

     Output che mostra gli eventi AWS CloudFormation dello stack se il `AssociatePhoneNumbersToContactFlows` passaggio fallisce.

Output di esecuzione con un numero limitato di numeri di telefono e flussi di contatti



Output di esecuzione con un gran numero di numeri di telefono e flussi di contatti e numeri di telefono che non sono stati associati a causa di errori o vincoli di tempo



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWSSupport-CollectAmazonConnectContactFlowLog

Descrizione

Il runbook di `AWSSupport-CollectAmazonConnectContactFlowLog` automazione viene utilizzato per raccogliere i log del flusso di contatti di Amazon Connect per un ID di contatto specifico. Fornendo l'ID dell'istanza e l'ID del contatto di Amazon Connect, il runbook cerca il contatto nei log del flusso di contatti dal gruppo di CloudWatch log di Amazon e li carica nel bucket Amazon Simple Storage Service (Amazon S3) specificato nel parametro di richiesta. Il runbook genera un output che fornisce la URL console Amazon S3 AWS CLI e il comando per scaricare i log.

Come funziona?

Il runbook di `AWSSupport-CollectAmazonConnectContactFlowLog` automazione aiuta a raccogliere i log del flusso di contatti di Amazon Connect per un ID di contatto specifico archiviato nel gruppo di CloudWatch log configurato e li carica in un bucket Amazon S3 specificato. Per

contribuire alla sicurezza dei log raccolti dal flusso di contatti di Amazon Connect, l'automazione valuta la configurazione del bucket Amazon S3 per determinare se il bucket concede autorizzazioni `read` pubbliche `write` o di accesso ed è di proprietà dell'account specificato nel parametro. AWS `S3BucketOwnerAccountId` Se il tuo bucket Amazon S3 utilizza la crittografia lato server con AWS Key Management Service chiavi (SSE-KMS), assicurati che l'utente o il ruolo AWS Identity and Access Management (IAM) che esegue questa automazione disponga delle autorizzazioni sulla `kms:GenerateDataKey` chiave. AWS KMS Per ulteriori informazioni sui log generati dalla tua istanza Amazon Connect, consulta Flow logs stored in an Amazon CloudWatch log group.

> **Important**
>
> Le query di CloudWatch Logs Insights comportano addebiti in base alla quantità di dati interrogati. Ai clienti del piano gratuito viene addebitato solo l'importo per l'utilizzo che supera le Service Quotas. Per ulteriori informazioni, consulta la pagina CloudWatchdei prezzi di Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Statement": [
        {
```

```
                "Action": [
                    "s3:GetBucketPublicAccessBlock",
                    "s3:GetBucketPolicyStatus",
                    "s3:GetBucketAcl",
                    "s3:GetObject",
                    "s3:GetObjectAttributes",
                    "s3:PutObject",
                    "s3:PutObjectAcl"
                ],
                "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-bucket"
                ],
                "Effect": "Allow"
            },
            {
                "Action": [
                    "connect:DescribeInstance",
                    "connect:DescribeContact",
                    "ds:DescribeDirectories"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "logs:StartQuery",
                    "logs:GetQueryResults"

                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-CollectAmazonConnectContactFlowLog](#)a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).

3. Per i parametri di input, immettete quanto segue:

   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

   - ConnectInstanceId (Obbligatorio):

     L'ID della tua istanza Amazon Connect.

   - ContactId (Obbligatorio):

     L'ID del contatto per cui desideri raccogliere il registro del flusso di contatti.

   - S3 BucketName (obbligatorio):

     Il nome del bucket Amazon S3 nel tuo account in cui desideri caricare il log del flusso di contatti. Assicurati che la bucket policy non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log raccolti.

   - S3 (opzionale): ObjectPrefix

     Il percorso dell'oggetto Amazon S3 nel bucket Amazon S3 per un log del flusso di contatti caricato. Ad esempio, se lo specifichi`CollectedLogs`, il log verrà caricato come. `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz` Se non si specifica questo parametro, viene utilizzato l'ID di esecuzione di Systems Manager Automation, ad esempio:`s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. Nota: se si specifica un valore per `S3ObjectPrefix` ed si esegue questa automazione utilizzando lo stesso [ContactId], il registro del flusso di contatti verrà sovrascritto.

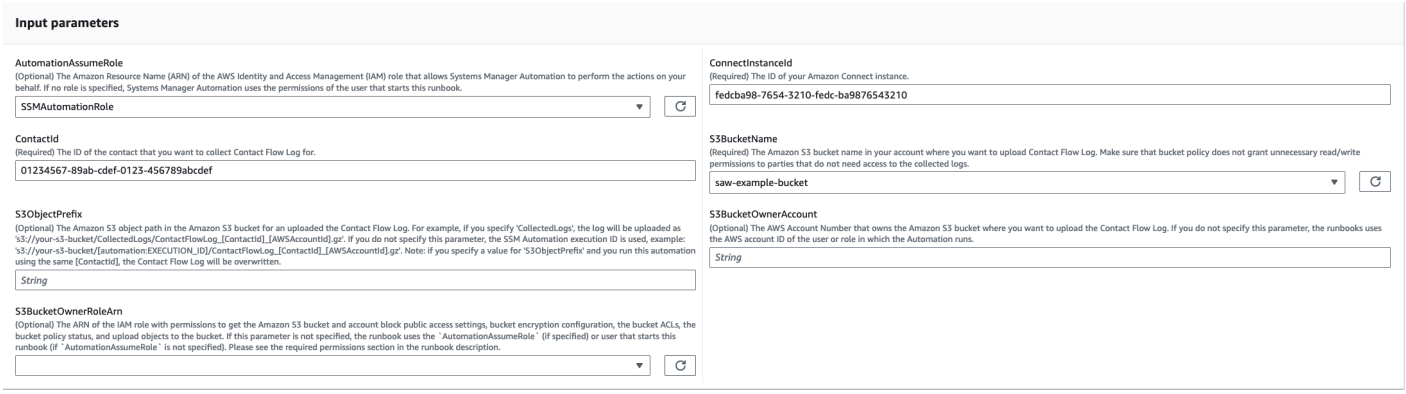
   - S3 BucketOwnerAccount (opzionale):

     Il numero di AWS account proprietario del bucket Amazon S3 in cui desideri caricare il log del flusso di contatti. Se non specifichi questo parametro, il runbook utilizza l'ID AWS account dell'utente o del ruolo in cui viene eseguita l'automazione.

   - S3 BucketOwnerRoleArn (opzionale):

     Il IAM ruolo con le autorizzazioni per ottenere le impostazioni ARN di accesso pubblico del bucket Amazon S3 e dell'account, la configurazione della crittografia dei bucket, lo stato

della policy del ACLs bucket e il caricamento di oggetti nel bucket. Se questo parametro non è specificato, il runbook utilizza l'utente `AutomationAssumeRole` (se specificato) o che avvia questo runbook (se non è specificato). `AutomationAssumeRole` Vedi la sezione sulle autorizzazioni richieste nella descrizione del runbook.



4. Seleziona Esegui.
5. L'automazione inizia.
6. Il documento esegue le seguenti operazioni:
   - CheckConnectInstanceExistance

     Verifica se l'istanza Amazon Connect fornita in `ConnectInstanceId` è`ACTIVE`.
   - Controlla S3 BucketPublicStatus

     Verifica se il bucket Amazon S3 specificato in `S3BucketName` consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.
   - GenerateLogSearchTimeRange

     Genera `StartTime` e `EndTime` per il `StartQuery` passaggio in base a `InitiationTimestamp` e `LastUpdateTimestamp` restituito da. `DescribeContact` API `StartTime`sarà un'ora prima `InitiationTimestamp` e `EndTime` sarà un'ora dopo`LastUpdateTimestamp`.
   - StartQuery

     Avvia un log di query per il file fornito `ContactId` nel gruppo di log CloudWatch Logs associato all'istanza Amazon Connect fornita in`ConnectInstanceId`. Le query scadono dopo 60 minuti di esecuzione. Se la query scade, riduci l'intervallo di tempo in cui viene effettuata la ricerca. Puoi visualizzare le query attualmente in corso e la cronologia delle query recenti nella CloudWatch console. Per ulteriori informazioni, consulta Visualizzare le query in esecuzione o la cronologia delle query.

- WaitForQueryCompletion

  Attende il completamento del registro CloudWatch delle query di Logs fornito`ContactId`. Si noti che la query scade dopo 60 minuti di esecuzione. Se la query scade, riduci l'intervallo di tempo in cui viene eseguita la ricerca. Puoi visualizzare le query attualmente in corso e la cronologia delle query recenti nella console Amazon Connect. Per ulteriori informazioni, consulta Visualizza le query in esecuzione o la cronologia delle query.

- UploadContactFlowLog

  Ottiene il risultato della query e carica il log del flusso di contatti nel bucket Amazon S3 specificato in. `S3BucketName`

- GenerateReport

  Restituisce la console Amazon S3 URL in cui è stato caricato il log del flusso di contatti e un AWS CLI comando di esempio che puoi utilizzare per scaricare il file di registro.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

   - GenerateReport.OutputPayload

     Output che indica che il runbook ha recuperato correttamente i log del flusso di contatti per il contatto specificato. Questo report contiene anche la console Amazon S3 URL e un AWS CLI comando di esempio per scaricare il file di registro.

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione

- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS Directory Service

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Directory Service Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-CreateDSManagementInstance
- AWSSupport-TroubleshootADConnectorConnectivity
- AWSSupport-TroubleshootDirectoryTrust

`AWS-CreateDSManagementInstance`

Descrizione

Il `AWS-CreateDSManagementInstance` runbook crea un'istanza Windows di Amazon Elastic Compute Cloud (Amazon EC2) che puoi utilizzare per gestire la tua directory. AWS Directory Service L'istanza di gestione non può essere utilizzata per gestire le directory di AD Connector.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

Tipo: String

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Un ID

  Tipo: String

  Impostazione predefinita: `{{ ssm:/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-Base }}`

  Descrizione: (Obbligatorio) L'ID del Amazon Machine Image (AMI) che si desidera utilizzare per avviare l'istanza di gestione.

- DirectoryId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID della AWS Directory Service directory che desideri gestire. L'istanza viene aggiunta alla directory specificata.

- IamInstanceProfileName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome specificato viene applicato al profilo dell'istanza IAM creato dall'automazione e collegato all'istanza di gestione.

- InstanceType

  Tipo: String

  Impostazione predefinita: t3.medium

  Valori consentiti:

  - t2.nano
  - t2.micro
  - t2.small
  - t2.medium

- t2.large
- t2.xlarge
- t2.2xlarge
- t3.nano
- t3.micro
- t3.small
- t3.medium
- t3.large
- t3.xlarge
- t3.2xlarge

Descrizione: (Obbligatorio) Il tipo di istanza che desideri avviare.

- KeyPairName

  Tipo: String

  Descrizione: (Facoltativo) La coppia di chiavi da utilizzare durante la creazione dell'istanza. Se non specificate un valore, nessuna coppia di chiavi è associata all'istanza.

- RemoteAccessCidr

  Tipo: String

  Descrizione: (Obbligatorio) Il blocco CIDR da cui si desidera consentire il traffico RDP (porta 3389). Il blocco CIDR specificato viene applicato a una regola in entrata aggiunta al gruppo di sicurezza creato dall'automazione.

- SecurityGroupName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome specificato viene applicato al gruppo di sicurezza creato dall'automazione e associato all'istanza di gestione.

- Tag

  Tipo: MapList

  Descrizione: (Facoltativo) Una coppia chiave-valore che desideri applicare alle risorse create dall'automazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ds:DescribeDirectories`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:DeleteInstanceProfile`
- `iam:DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfiles`
- `iam:ListInstanceProfilesForRole`
- `iam:PassRole`

- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution

Fasi del documento

- aws:executeAwsApi- Raccoglie dettagli sulla directory specificata nel DirectoryId parametro.
- aws:executeAwsApi- Ottiene il blocco CIDR del cloud privato virtuale (VPC) in cui è stata lanciata la directory.
- aws:executeAwsApi- Crea un gruppo di sicurezza utilizzando il valore specificato nel SecurityGroupName parametro.
- aws:executeAwsApi- Crea una regola in entrata per il gruppo di sicurezza appena creato che consente il traffico RDP dal CIDR specificato nel parametro. RemoteAccessCidr
- aws:executeAwsApi- Crea un ruolo IAM e un profilo di istanza utilizzando il valore specificato nel IamInstanceProfileName parametro.
- aws:executeAwsApi- Avvia un'istanza Amazon EC2 in base ai valori specificati nei parametri del runbook.
- aws:executeAwsApi- Crea un AWS Systems Manager documento per aggiungere l'istanza appena lanciata alla tua directory.
- aws:runCommand- Aggiunge la nuova istanza alla tua directory.
- aws:runCommand- Installa strumenti di amministrazione remota del server sulla nuova istanza.

AWSSupport-TroubleshootADConnectorConnectivity

Descrizione

Il AWSSupport-TroubleshootADConnectorConnectivity runbook verifica i seguenti prerequisiti per un AD Connector:

- Verifica se il traffico richiesto è consentito dalle regole del gruppo di sicurezza e della lista di controllo dell'accesso alla rete (ACL) associate ad AD Connector.
- Verifica se gli VPC endpoint dell' CloudWatch interfaccia AWS Systems Manager AWS Security Token Service, e Amazon esistono nello stesso cloud privato virtuale (VPC) di AD Connector.

Quando i controlli dei prerequisiti vengono completati correttamente, il runbook avvia due istanze Amazon Elastic Compute Cloud (AmazonEC2) Linux t2.micro nelle stesse sottoreti del tuo AD Connector. I test di connettività di rete vengono quindi eseguiti utilizzando le utilità and. netcat nslookup

Esegui questa automazione (console)

> **Important**
>
> L'utilizzo di questo runbook potrebbe comportare costi aggiuntivi per le Account AWS EC2 istanze Amazon, i volumi Amazon Elastic Block Store Amazon Machine Image e AMI () creati durante l'automazione. Per ulteriori informazioni, consulta i prezzi di Amazon Elastic Compute Cloud e i prezzi di Amazon Elastic Block Store.
> Se il aws:deletestack passaggio non riesce, vai alla AWS CloudFormation console per eliminare manualmente lo stack. Il nome dello stack creato da questo runbook inizia con. AWSSupport-TroubleshootADConnectorConnectivity Per informazioni sull'eliminazione degli AWS CloudFormation stack, vedere Eliminazione di uno stack nella Guida per l'utente.AWS CloudFormation

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DirectoryId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della directory AD Connector a cui desideri risolvere i problemi di connettività.
- Ec2 InstanceProfile

  Tipo: stringa

  Numero massimo di caratteri: 128

  Descrizione: (Obbligatorio) Il nome del profilo di istanza che si desidera assegnare alle istanze avviate per eseguire i test di connettività. Il profilo di istanza specificato deve avere la `AmazonSSMManagedInstanceCore` policy o autorizzazioni equivalenti allegate.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`

- ec2:DescribeNetworkAcls
- ec2:DescribeVpcEndpoints
- ec2:CreateTags
- ec2:RunInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:ListStackResources
- cloudformation:DeleteStack
- ds:DescribeDirectories
- ssm:SendCommand
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:DescribeInstanceInformation
- iam:PassRole

Fasi del documento

- aws:assertAwsResourceProperty- Conferma che la directory specificata nel DirectoryId parametro è un AD Connector.
- aws:executeAwsApi- Raccoglie informazioni su AD Connector.
- aws:executeAwsApi- Raccoglie informazioni sui gruppi di sicurezza associati ad AD Connector.
- aws:executeAwsApi- Raccoglie informazioni sulle ACL regole di rete associate alle sottoreti per AD Connector.
- aws:executeScript- Valuta le regole del gruppo di sicurezza AD Connector per verificare che il traffico in uscita richiesto sia consentito.
- aws:executeScript- Valuta le ACL regole di rete AD Connector per verificare che il traffico di rete in uscita e in entrata richiesto sia consentito.
- aws:executeScript- Verifica se AWS Systems Manager gli endpoint CloudWatch dell'interfaccia AWS Security Token Service e Amazon esistono nello stesso VPC di AD Connector.

- `aws:executeScript`- Compila gli output dei controlli eseguiti nei passaggi precedenti.
- `aws:branch`- Suddivide l'automazione in base all'output dei passaggi precedenti. L'automazione si interrompe qui se mancano le regole in uscita e in entrata richieste per i gruppi di sicurezza e la rete. ACLs
- `aws:createStack`- Crea uno AWS CloudFormation stack per avviare EC2 istanze Amazon per eseguire test di connettività.
- `aws:executeAwsApi`- Raccoglie le IDs EC2 istanze Amazon appena lanciate.
- `aws:waitForAwsResourceProperty`- Attende che la prima EC2 istanza Amazon appena lanciata venga segnalata come gestita da AWS Systems Manager.
- `aws:waitForAwsResourceProperty`- Attende che la seconda EC2 istanza Amazon appena lanciata venga segnalata come gestita da AWS Systems Manager.
- `aws:runCommand`- Esegue test di connettività di rete sugli indirizzi IP dei DNS server locali dalla prima EC2 istanza Amazon.
- `aws:runCommand`- Esegue test di connettività di rete sugli indirizzi IP dei DNS server locali dalla seconda EC2 istanza Amazon.
- `aws:changeInstanceState`- Arresta le EC2 istanze Amazon utilizzate per i test di connettività.
- `aws:deleteStack`- Elimina lo stack. AWS CloudFormation
- `aws:executeScript`- Fornisce istruzioni su come eliminare manualmente lo AWS CloudFormation stack se l'automazione non riesce a eliminare lo stack.

`AWSSupport-TroubleshootDirectoryTrust`

Descrizione

Il `AWSSupport-TroubleshootDirectoryTrust` runbook diagnostica i problemi di creazione di trust tra un Microsoft Active Directory AWS Managed Microsoft AD e un Microsoft Active Directory. L'automazione garantisce che il tipo di directory supporti i trust e quindi controlla le regole dei gruppi di protezione associati, gli elenchi di controllo di accesso alla rete (ACL di rete) e le tabelle di routing per potenziali problemi di connettività.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DirectoryId

  Tipo: String

  Modello consentito: ^d- [a-z0-9] {10} $

  Descrizione: (Obbligatorio) L'ID di AWS Managed Microsoft AD da risolvere.
- RemoteDomainCidrs

  Tipo: StringList

  Schema consentito: ^ ([0-9] | [1-9] [0-9] |1 [0-9] {2} |2 [0-4] [0-9] |25 [0-5])\.) {3} ([0-9] | [1-9] [0-9] {2} |2 [0-4] [0-9] [0-4] [0-9] [0-9] |25 [0-5]) (\/3 [0-2] | [1-2] [0-9] | [1-9])) $

  Descrizione: (Obbligatorio) I CIDR del dominio remoto con cui si sta tentando di stabilire una relazione di trust. È possibile aggiungere più CIDR utilizzando valori separati da virgole. Ad esempio: 172.31.48.0/20, 192.168.1.10/32.
- RemoteDomainName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome di dominio completo del dominio remoto con cui si sta stabilendo una relazione di trust.

- RequiredTrafficACL

  Tipo: String

  Descrizione: (Obbligatorio) I requisiti di porta predefiniti per AWS Managed Microsoft AD. Nella maggior parte dei casi, non è necessario modificare il valore predefinito.

  Default: {"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}
- RequiredTrafficSG

  Tipo: String

  Descrizione: (Obbligatorio) I requisiti di porta predefiniti per AWS Managed Microsoft AD. Nella maggior parte dei casi, non è necessario modificare il valore predefinito.

  Default: {"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}
- TrustId

  Tipo: String

  Descrizione: (facoltativo) L'ID della relazione di trust da risolvere.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ds:DescribeConditionalForwarders`
- `ds:DescribeDirectories`
- `ds:DescribeTrusts`
- `ds:ListIpRoutes`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il tipo di directory èAWS Managed Microsoft AD.
- `aws:executeAwsApi`- Ottiene informazioni suAWS Managed Microsoft AD.
- `aws:branch`- Automazione delle filiali se viene fornito un valore per il parametro `TrustId` di input.
- `aws:executeAwsApi`- Ottiene informazioni sulla relazione di fiducia.
- `aws:executeAwsApi`- Ottiene gli indirizzi IP DNS del trasmettitore condizionale per. `RemoteDomainName`
- `aws:executeAwsApi`- Ottiene informazioni sulle rotte IP che sono state aggiunte aAWS Managed Microsoft AD.
- `aws:executeAwsApi`- Ottiene i CIDR delle sottoreti. AWS Managed Microsoft AD
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati aAWS Managed Microsoft AD.
- `aws:executeAwsApi`- Ottiene informazioni sugli ACL di rete associati a. AWS Managed Microsoft AD
- `aws:executeScript`- Conferma che `RemoteDomainCidrs` sono valori validi. Conferma che AWS Managed Microsoft AD dispone di inoltratori condizionali per e che le rotte IP richieste `RemoteDomainCidrs` sono state aggiunte agli indirizzi IP 1918 AWS Managed Microsoft AD non RFC. `RemoteDomainCidrs`
- `aws:executeScript`- Valuta le regole dei gruppi di sicurezza.
- `aws:executeScript`- Valuta gli ACL di rete.

Output

evalDirectorySecurityGroup.output: risulta dalla valutazione se le regole del gruppo di sicurezza associate AWS Managed Microsoft AD consentono il traffico necessario per la creazione di trust.

evalAclEntries.output: risultato della valutazione se gli ACL di rete associati AWS Managed Microsoft AD consentono il traffico necessario per la creazione di fiducia.

evaluateRemoteDomaincidr.Output: risultati della valutazione della validità dei `RemoteDomainCidrs` valori. Conferma che AWS Managed Microsoft AD dispone di inoltratori condizionali per e che le rotte

IP richieste `RemoteDomainCidrs` sono state aggiunte agli indirizzi IP 1918 AWS Managed Microsoft AD non RFC. `RemoteDomainCidrs`

AWS AppSync

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS AppSync Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

Descrizione

Il `AWS-EnableAppSyncGraphQLApiLogging` runbook consente la registrazione a livello di campo e la registrazione a livello di richiesta per l'API GraphQL specificata. AWS AppSync Il runbook applicherà le modifiche all'API GraphQL specificata anche se la registrazione è già stata abilitata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ApiId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'API per cui si desidera abilitare la registrazione.

- FieldLogLevel

  Tipo: stringa

  Valori validi: ERROR | ALL

  Descrizione: (Obbligatorio) Il livello di registrazione del campo.

- CloudWatchLogsRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN del ruolo di servizio che AWS AppSync si presuppone di pubblicare su Amazon Logs. CloudWatch

- ExcludeVerboseContent

  Tipo: Booleano

  Impostazione predefinita: False

  Descrizione: (Facoltativo) Imposta su `True` per escludere informazioni come intestazioni, contesto e modelli di mappatura valutati, indipendentemente dal livello di registrazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `appsync:GetGraphqlApi`
- `appsync:UpdateGraphqlApi`
- `iam:PassRole`

Fasi del documento

- aws: executeAwsApi - Raccoglie il tipo di autenticazione e le informazioni di configurazione rilevanti per il tipo di autenticazione principale.
- aws:branch - Filiali basate sul tipo di autenticazione.
- aws: executeAwsApi - Aggiorna la configurazione di registrazione per l'API AWS AppSync GraphQL in base ai valori specificati per i parametri di input del runbook.

Output

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Risposta dalla chiamata. `UpdateGraphqlApi`
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphqlApi` chiamata.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphqlApi` chiamata.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphqlApi` chiamata.

Amazon Athena

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Athena. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableAthenaWorkGroupEncryptionAtRest

`AWS-EnableAthenaWorkGroupEncryptionAtRest`

Descrizione

Il `AWS-EnableAthenaWorkGroupEncryptionAtRest` runbook abilita la crittografia a riposo per il gruppo di lavoro Amazon Athena specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- WorkGroup

  Tipo: stringa

  Descrizione: (Obbligatorio) Il gruppo di lavoro per cui si desidera abilitare la crittografia a riposo.
- EncryptionOption

  Tipo: stringa

  Valori validi: SSE_S3 | SSE_KMS | CSE_KMS

  Descrizione: (Obbligatorio) Specificate l'opzione di crittografia utilizzata. Puoi scegliere la crittografia lato server con chiavi gestite Amazon S3 (SSE_S3), la crittografia lato server con chiavi gestite (SSE_KMS) o la crittografia lato client AWS KMS con chiavi gestite (CSE_KMS). AWS KMS
- KmsKeyId

  Tipo: stringa

  Descrizione: (Facoltativo) Se utilizzi un'opzione di AWS KMS crittografia, specifica l'ARN della chiave, l'ID della chiave o l'alias della chiave che desideri utilizzare.

- EnableMinimumEncryptionConfiguration

  Tipo: Booleano

  Impostazione predefinita: True

  Descrizione: (Facoltativo) Applica un livello minimo di crittografia per il gruppo di lavoro per i risultati di query e calcoli scritti su Amazon S3. Se abilitata, gli utenti del gruppo di lavoro possono impostare la crittografia solo al livello minimo impostato dall'amministratore o superiore quando inviano le query. Questa impostazione non si applica ai gruppi di lavoro abilitati per Spark.

- EnforceWorkGroupConfiguration

  Tipo: Booleano

  Impostazione predefinita: True

  Descrizione: (Facoltativo) Se impostata su`True`, le impostazioni per il gruppo di lavoro hanno la precedenza sulle impostazioni lato client. Se impostato su, vengono utilizzate le `False` impostazioni lato client.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `athena:GetWorkGroup`
- `athena:UpdateWorkGroup`

Fasi del documento

- aws:branch - Rami basati sull'opzione di crittografia specificata nel parametro. `EncryptionOption`
- aws: executeAwsApi - Questo passaggio aggiorna il gruppo di lavoro Athena con l'impostazione di crittografia specificata.
- aws: executeAwsApi - Aggiorna l'Athena Work Group con l'impostazione di crittografia specificata.

- aws: assertAwsResource Property - Verifica che la crittografia per il gruppo di lavoro sia stata abilitata.

DynamoDB

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon DynamoDB. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-ChangeDDBRWCapacityMode
- AWS-CreateDynamoDBBackup
- AWS-DeleteDynamoDbBackup
- AWSConfigRemediation-DeleteDynamoDbTable
- AWS-DeleteDynamoDbTableBackups
- AWSConfigRemediation-EnableEncryptionOnDynamoDbTable
- AWSConfigRemediation-EnablePITRForDynamoDbTable
- AWS-EnableDynamoDbAutoscaling
- AWS-RestoreDynamoDBTable

AWS-ChangeDDBRWCapacityMode

Descrizione

Il `AWS-ChangeDDBRWCapacityMode` runbook modifica la modalità di capacità di lettura/scrittura per una o più tabelle Amazon DynamoDB (DynamoDB) in modalità on demand o in modalità provisioning.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CapacityMode

  Tipo: stringa

  Valori validi: PROVISIONED | PAY_PER_REQUEST

  Descrizione: (Obbligatoria) La modalità di capacità di lettura/scrittura desiderata. Quando si passa dalla capacità su richiesta (pay-per-request) alla capacità fornita, è necessario impostare i valori della capacità fornita iniziale. I valori della capacità iniziale assegnata sono stimati in base alla capacità di lettura e scrittura consumata dalla tabella e dagli indici secondari globali negli ultimi 30 minuti.

- ReadCapacityUnits

  Tipo: integer

  Impostazione Predefinita: 0

  Descrizione: (Facoltativo) Il numero massimo di letture fortemente coerenti consumate al secondo prima che DynamoDB restituisca un'eccezione di limitazione.

- TableNames

  Tipo: stringa

  Descrizione: (Obbligatorio) Elenco separato da virgole di nomi di tabelle DynamoDB per modificare la modalità di capacità di lettura/scrittura per..

- WriteCapacityUnits

  Tipo: integer

Impostazione Predefinita: 0

Descrizione: (Facoltativo) Il numero massimo di scritture consumate al secondo prima che DynamoDB restituisca un'eccezione di limitazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `dynamodb:DescribeTable`
- `dynamodb:UpdateTable`

Fasi del documento

- `aws:executeScript`- Modifica la modalità di capacità di lettura/scrittura per le tabelle DynamoDB specificate nel parametro. `TableNames`

Output

DBRW CapacityMode modificato. SuccessesTables - Elenco di nomi di tabelle DynamoDB in cui la modalità di capacità è stata modificata con successo

DBRW modificato. CapacityMode FailedTables - Elenco di mappe dei nomi delle tabelle DynamoDB in cui la modifica della modalità di capacità non è riuscita e il motivo dell'errore.

AWS-CreateDynamoDBBackup

Descrizione

Crea un backup di una tabella Amazon DynamoDB.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BackupName

  Tipo: String

  Descrizione: (obbligatorio) nome del backup da creare.
- LambdaAssumeRole

  Tipo: String

  Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.
- TableName

  Tipo: String

  Descrizione: (obbligatorio) nome della tabella DynamoDB.

AWS-DeleteDynamoDbBackup

Descrizione

Elimina il backup di una tabella Amazon DynamoDB.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BackupArn

  Tipo: String

  Descrizione: (obbligatorio) ARN del backup della tabella DynamoDB da eliminare.

AWSConfigRemediation-DeleteDynamoDbTable

Descrizione

Il `AWSConfigRemediation-DeleteDynamoDbTable` runbook elimina la tabella Amazon DynamoDB (DynamoDB) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- TableName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome della tabella DynamoDB che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `dynamodb:DeleteTable`
- `dynamodb:DescribeTable`

Fasi del documento

- `aws:executeScript`- Elimina la tabella DynamoDB specificata nel parametro. `TableName`
- `aws:executeScript`- Verifica che la tabella DynamoDB sia stata eliminata.

AWS-DeleteDynamoDbTableBackups

Descrizione

Elimina i backup delle tabelle DynamoDB in base ai giorni o al numero di giorni di conservazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LambdaAssumeRole

  Tipo: String

  Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.
- RetentionCount

  Tipo: String

  Impostazione predefinita: 10

  Descrizione: (facoltativo) numero di backup da conservare per la tabella. Se esiste un numero di backup maggiore del numero specificato, verranno eliminati i backup meno recenti che superano tale numero. Uno RetentionCount o RetentionDays possono essere usati, non entrambi.

- RetentionDays

  Tipo: String

  Descrizione: (facoltativo) numero di giorni durante i quali conservare i backup della tabella. I backup precedenti al numero di giorni specificato vengono eliminati. Uno RetentionCount o RetentionDays possono essere usati, non entrambi.

- TableName

  Tipo: String

  Descrizione: (obbligatorio) nome della tabella DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descrizione

Il `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` runbook crittografa una tabella Amazon DynamoDB (DynamoDB) utilizzando la chiave gestita dal cliente AWS KMS() specificata per AWS Key Management Service il parametro. `KMSKeyId`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parameters (Parametri)

- AutomationAssumeRole

  -Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KMS KeyId

  -Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN della chiave gestita dal cliente che desideri utilizzare per crittografare la tabella DynamoDB specificata nel parametro. `TableName`

- TableName

  -Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della tabella DynamoDB che desideri crittografare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `dynamodb:DescribeTable`
- `dynamodb:UpdateTable`

Fasi del documento

- `aws:executeAwsApi`- Crittografa la tabella DynamoDB specificata nel parametro. `TableName`
- `aws:waitForAwsResourceProperty`- Verifica che la `Enabled` proprietà della tabella `SSESpecification` DynamoDB sia impostata su. `true`
- `aws:assertAwsResourceProperty`- Verifica che la tabella DynamoDB sia crittografata con la chiave gestita dal cliente specificata nel parametro. `KMSKeyId`

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descrizione

Il `AWSConfigRemediation-EnablePITRForDynamoDbTable` runbook abilita il point-in-time ripristino (PITR) sulla tabella Amazon DynamoDB specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- TableName

  Tipo: String

  Descrizione: (Obbligatorio) Il nome della tabella DynamoDB su cui abilitare point-in-time il ripristino.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `dynamodb:DescribeContinuousBackups`

- `dynamodb:UpdateContinuousBackups`

Fasi del documento

- `aws:executeAwsApi`- Abilita point-in-time il ripristino sulla tabella DynamoDB specificata nel `TableName` parametro.
- `aws:assertAwsResourceProperty`- Conferma che point-in-time il ripristino è abilitato nella tabella DynamoDB.

`AWS-EnableDynamoDbAutoscaling`

Descrizione

Il `AWS-EnableDynamoDbAutoscaling` runbook abilita l'Application Auto Scaling per la tabella Amazon DynamoDB con capacità fornita specificata. Application Auto Scaling regola dinamicamente la capacità di throughput assegnata in risposta ai modelli di traffico. Per ulteriori informazioni, consulta Gestire automaticamente la capacità di throughput con la scalabilità automatica di DynamoDB nella Amazon DynamoDB Developer Guide.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- TableName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della tabella DynamoDB su cui si desidera abilitare l'Application Auto Scaling.
- MinReadCapacity

  Tipo: integer

  Descrizione: (Obbligatorio) Il numero minimo di unità di capacità di lettura del throughput assegnate per la tabella DynamoDB.
- MaxReadCapacity

  Tipo: integer

  Descrizione: (Obbligatorio) Il numero massimo di unità di capacità di lettura del throughput assegnate per la tabella DynamoDB.
- TargetReadCapacityUtilization

  Tipo: integer

  Descrizione: (Obbligatorio) L'utilizzo della capacità di lettura desiderata. L'utilizzo previsto è la percentuale del throughput assegnato consumato in un determinato momento. È possibile impostare i valori di utilizzo target con scalabilità automatica tra il 20 e il 90 percento.
- ReadScaleOutCooldown

  Tipo: integer

  Descrizione: (Obbligatorio) La quantità di tempo, espressa in secondi, di attesa per l'entrata in vigore di una precedente attività di scalabilità orizzontale della capacità di lettura.
- ReadScaleInCooldown

  Tipo: integer

  Descrizione: (Obbligatorio) La quantità di tempo, in secondi, dopo il completamento di un'attività di scalabilità in base alla capacità di lettura prima che possa iniziare un'altra attività scalabile.
- MinWriteCapacity

  Tipo: integer

Descrizione: (Obbligatorio) Il numero minimo di unità di scrittura di throughput assegnate per la tabella DynamoDB.

- MaxWriteCapacity

  Tipo: integer

  Descrizione: (Obbligatorio) Il numero massimo di unità di scrittura di throughput assegnate per la tabella DynamoDB.

- TargetWriteCapacityUtilization

  Tipo: integer

  Descrizione: (Obbligatorio) L'utilizzo della capacità di scrittura desiderata. L'utilizzo previsto è la percentuale del throughput assegnato consumato in un determinato momento. È possibile impostare i valori di utilizzo target con scalabilità automatica tra il 20 e il 90 percento.

- WriteScaleOutCooldown

  Tipo: integer

  Descrizione: (Obbligatorio) La quantità di tempo, in secondi, di attesa per l'entrata in vigore di una precedente attività di scalabilità orizzontale della capacità di scrittura.

- WriteScaleInCooldown

  Tipo: integer

  Descrizione: (Obbligatorio) La quantità di tempo in secondi dopo il completamento di un'attività di scalabilità in base alla capacità di scrittura prima che possa iniziare un'altra attività scalabile.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `application-autoscaling:DescribeScalableTargets`
- `application-autoscaling:DescribeScalingPolicies`

- `application-autoscaling:PutScalingPolicy`
- `application-autoscaling:RegisterScalableTarget`

- RegisterAppAutoscalingTargetWrite (`aws:executeAwsApi`) - Configura Application Auto Scaling nella tabella DynamoDB specificata.
- RegisterAppAutoscalingTargetWriteDelay (`aws:sleep`) - Dorme per evitare rallentamenti. API
- PutScalingPolicyWrite (`aws:executeAwsApi`) - Configura l'utilizzo della capacità di scrittura di destinazione per la tabella DynamoDB.
- PutScalingPolicyWriteDelay (`aws:sleep`) - Dorme per evitare rallentamenti. API
- RegisterAppAutoscalingTargetRead (`aws:executeAwsApi`) - Configura le unità di capacità di lettura minima e massima per la tabella DynamoDB.
- RegisterAppAutoscalingTargetReadDelay (`aws:sleep`) - Dorme per evitare rallentamenti. API
- PutScalingPolicyRead (`aws:executeAwsApi`) - Configura l'utilizzo della capacità di lettura prevista per la tabella DynamoDB.
- VerifyDynamoDbAutoscalingEnabled (`aws:executeScript`) - Verifica che l'Application Auto Scaling sia abilitato per la tabella DynamoDB in base ai valori specificati.

Output

- RegisterAppAutoscalingTargetWrite.Risposta
- PutScalingPolicyWrite.Risposta
- RegisterAppAutoscalingTargetRead.Risposta
- PutScalingPolicyRead.Risposta
- VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse

AWS-RestoreDynamoDBTable

Descrizione

Il `AWS-RestoreDynamoDBTable` runbook ripristina la tabella Amazon DynamoDB specificata tramite point-in-time recovery (PITR).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EnablePointInTimeRecoverAsNeeded

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Determina se l'automazione attiva il point-in-time ripristino in base alle necessità per ripristinare la tabella.
- GlobalSecondaryIndexOverride

  Tipo: String

  Descrizione: (Facoltativo) I nuovi indici secondari globali per sostituire gli indici secondari esistenti per la nuova tabella.
- LocalSecondaryIndexOverride

  Tipo: String

  Descrizione: (Facoltativo) I nuovi indici secondari locali per sostituire gli indici secondari esistenti per la nuova tabella.

- RestoreDateTime

  Tipo: String

  Descrizione: (Obbligatorio) Il point-in-time ripristino a cui desideri ripristinare la tabella negli ultimi 35 giorni. Specifica la data e l'ora utilizzando il seguente formato: `DD/MM/YYYY HH:MM:SS`
- SourceTableArn

  Tipo: String

  Descrizione: (Obbligatorio) L'ARN della tabella che si desidera ripristinare.
- SseSpecificationOverride

  Tipo: String

  Descrizione: (Facoltativo) Le impostazioni di crittografia lato server da utilizzare per la nuova tabella.
- TargetTableName

  Tipo: String

  Descrizione: (obbligatorio) Il nome della tabella da ripristinare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `dynamodb:BatchWriteItem`
- `dynamodb:DeleteItem`
- `dynamodb:DescribeTable`
- `dynamodb:GetItem`
- `dynamodb:PutItem`
- `dynamodb:Query`
- `dynamodb:RestoreTableToPointInTime`
- `dynamodb:Scan`
- `dynamodb:UpdateItem`

Fasi del documento

- `aws:executeScript`- Ripristina la tabella DynamoDB specificata nel `TargetTableName` parametro utilizzando il ripristino. point-in-time

Amazon EBS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Block Store. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWSSupport-AnalyzeEBSResourceUsage`

Descrizione

Il runbook di `AWSSupport-AnalyzeEBSResourceUsage` automazione viene utilizzato per analizzare l'utilizzo delle risorse su Amazon Elastic Block Store (AmazonEBS). Analizza l'utilizzo dei volumi e identifica i volumi, le immagini e le istantanee abbandonati in una determinata regione. AWS

Come funziona?

Il runbook svolge le seguenti quattro attività:

1. Verifica l'esistenza di un bucket Amazon Simple Storage Service (Amazon S3) o crea un nuovo bucket Amazon S3.
2. Raccoglie tutti i EBS volumi Amazon nello stato disponibile.
3. Raccoglie tutte le EBS istantanee Amazon per cui il volume di origine è stato eliminato.
4. Raccoglie tutte le Amazon Machine Images (AMIs) che non sono utilizzate da istanze Amazon Elastic Compute Cloud (AmazonEC2) non terminate.

Il runbook genera CSV report e li archivia in un bucket Amazon S3 fornito dall'utente. Il bucket fornito deve essere protetto seguendo le migliori pratiche AWS di sicurezza descritte alla fine. Se il bucket Amazon S3 fornito dall'utente non esiste nell'account, il runbook crea un nuovo bucket Amazon S3 con il formato del nome`<User-provided-name>-awssupport-YYYY-MM-DD`, crittografato con una chiave personalizzata AWS Key Management Service (AWS KMS), con il controllo delle versioni degli oggetti abilitato, l'accesso pubblico bloccato e richiede l'utilizzo di/. SSL TLS

Se desideri specificare il tuo bucket Amazon S3, assicurati che sia configurato seguendo queste best practice:

- Blocca l'accesso pubblico al bucket (impostato su`IsPublic`). `False`
- Attiva la registrazione degli accessi di Amazon S3.
- Consenti solo SSL le richieste al tuo bucket.
- Attiva il controllo delle versioni degli oggetti.
- Usa una chiave AWS Key Management Service (AWS KMS) per crittografare il tuo bucket.

> **Important**
>
> L'utilizzo di questo runbook potrebbe comportare costi aggiuntivi sul tuo account per la creazione di bucket e oggetti Amazon S3. Consulta i prezzi di Amazon S3 per ulteriori dettagli sugli addebiti che potrebbero comportare.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- S3 BucketName

  Tipo: `AWS::S3::Bucket::Name`

  Descrizione: (Obbligatorio) Il bucket Amazon S3 nel tuo account in cui caricare il report. Assicurati che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log raccolti. Se il bucket specificato non esiste nell'account, l'automazione crea un nuovo bucket nella regione in cui l'automazione viene avviata con il formato del nome, crittografato con una chiave personalizzata. `<User-provided-name>-awssupport-YYYY-MM-DD` AWS KMS

  Modello consentito: `$|^(?!(^(([0-9]{1,3}[.]){3}[0-9]{1,3}$)))^((?!xn—)(?!.*-s3alias))[a-z0-9][-.a-z0-9]{1,61}[a-z0-9]$`
- CustomerManagedKmsKeyArn

  Tipo: stringa

  Descrizione: (Facoltativo) La AWS KMS chiave personalizzata Amazon Resource Name (ARN) per crittografare il nuovo bucket Amazon S3 che verrà creato se il bucket specificato non esiste nell'account. L'automazione fallisce se si tenta di creare il bucket senza specificare una chiave personalizzata. AWS KMS ARN

  Modello consentito: `(^$|^arn:aws:kms:[-a-z0-9]:[0-9]:key/[-a-z0-9]*$)`

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVolumes`
- `kms:Decrypt`
- `kms:GenerateDataKey`
- `s3:CreateBucket`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `s3:ListAllMyBuckets`
- `s3:PutObject`
- `s3:PutBucketLogging`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutBucketTagging`
- `s3:PutBucketVersioning`
- `s3:PutEncryptionConfiguration`
- `ssm:DescribeAutomationExecutions`

Esempio di policy con IAM autorizzazioni minime richieste per eseguire questo runbook:

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

```
                "Action": [
                    "ec2:DescribeImages",
                    "ec2:DescribeInstances",
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeVolumes",
                    "ssm:DescribeAutomationExecutions"
                ],
                "Resource": ""
            }, {
                "Sid": "KMS_Generate_Permissions",
                "Effect": "Allow",
                "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
                "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }, {
                "Sid": "S3_Read_Only_Permissions",
                "Effect": "Allow",
                "Action": [
                    "s3:GetBucketAcl",
                    "s3:GetBucketPolicyStatus",
                    "s3:GetBucketPublicAccessBlock",
                    "s3:ListBucket"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket1",
                    "arn:aws:s3:::amzn-s3-demo-bucket2/"
                ]
            }, {
                "Sid": "S3_Create_Permissions",
                "Effect": "Allow",
                "Action": [
                    "s3:CreateBucket",
                    "s3:PutObject",
                    "s3:PutBucketLogging",
                    "s3:PutBucketPolicy",
                    "s3:PutBucketPublicAccessBlock",
                    "s3:PutBucketTagging",
                    "s3:PutBucketVersioning",
                    "s3:PutEncryptionConfiguration"
                ],
                "Resource": "*"
            }]
        }
```

Istruzioni

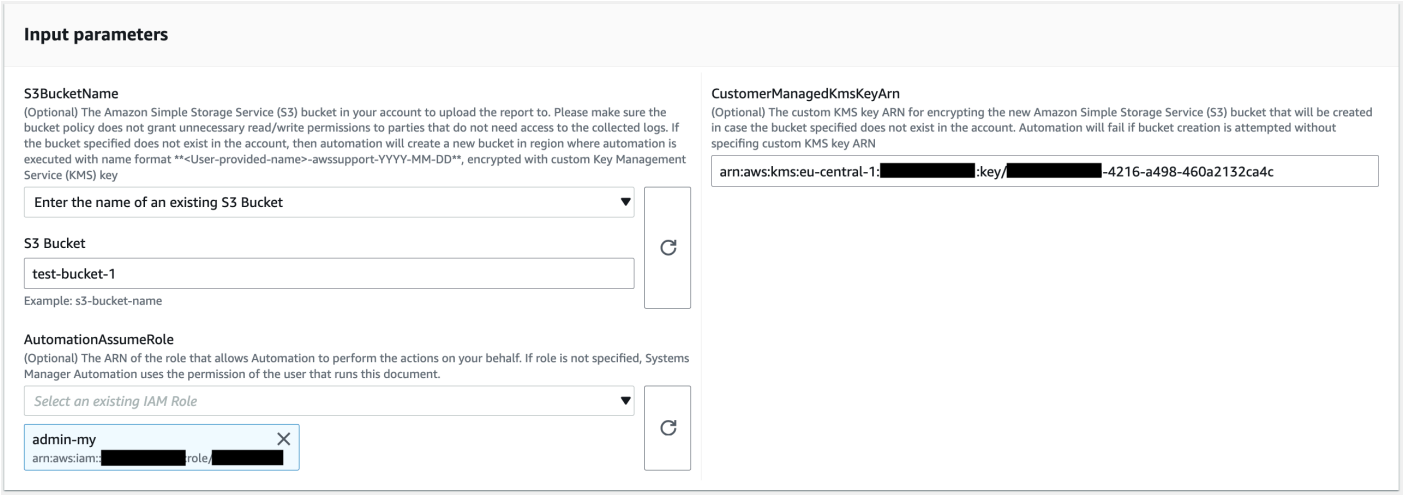
Segui questi passaggi per configurare l'automazione:

1. Vai a AWSSupport-A nalyzeEBSResource Usage nella AWS Systems Manager console.
2. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - S3 BucketName (richiesto):

     Il bucket Amazon S3 nel tuo account in cui caricare il report.
   - CustomerManagedKmsKeyArn(Facoltativo):

     La AWS KMS chiave personalizzata Amazon Resource Name (ARN) per crittografare il nuovo bucket Amazon S3 che verrà creato se il bucket specificato non esiste nell'account.



3. Seleziona Esegui.
4. L'automazione inizia.
5. Il runbook di automazione esegue i seguenti passaggi:
   - checkConcurrency:

Assicura che vi sia un solo avvio di questo runbook nella regione. Se il runbook rileva un'altra esecuzione in corso, restituisce un errore e termina.

- verifyOrCreateBucket S3:

  Verifica se il bucket Amazon S3 esiste. In caso contrario, crea un nuovo bucket Amazon S3 nella regione in cui l'automazione viene avviata con il formato del nome`<User-provided-name>-awssupport-YYYY-MM-DD`, crittografato con una chiave personalizzata. AWS KMS

- gatherAmiDetails:

  Le ricerche diAMIs, che non sono utilizzate da nessuna EC2 istanza Amazon, generano il report con il formato `<region>-images.csv` del nome e lo caricano nel bucket Amazon S3.

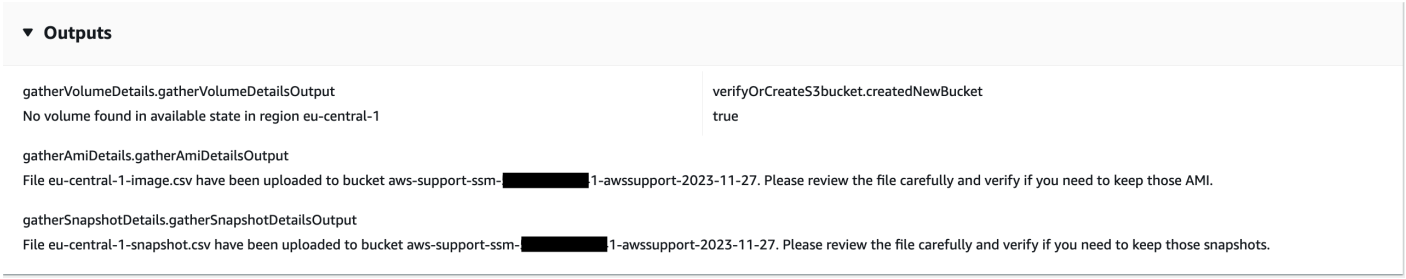
- gatherVolumeDetails:

  Verifica EBS i volumi Amazon nello stato disponibile, genera il report con il formato `<region>-volume.csv` del nome e lo carica in un bucket Amazon S3.

- gatherSnapshotDetails:

  Cerca le EBS istantanee Amazon dei EBS volumi Amazon che sono già stati eliminati, genera il report con il formato `<region>-snapshot.csv` del nome e lo carica nel bucket Amazon S3.

6. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS-ArchiveEBSSnapshots

Descrizione

Il `AWS-ArchiveEBSSnapshots` runbook ti aiuta ad archiviare gli snapshot per i volumi Amazon Elastic Block Store EBS (Amazon) specificando il tag che hai applicato agli snapshot. In alternativa, puoi fornire l'ID di un volume se gli snapshot non sono etichettati.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Descrizione

  Tipo: stringa

  Descrizione: (Facoltativa) Una descrizione dello EBS snapshot Amazon.
- DryRun

  Tipo: stringa

  Valori validi: Sì | No

Descrizione: (Obbligatorio) Verifica se l'utente dispone delle autorizzazioni necessarie per l'azione, senza effettuare effettivamente la richiesta, e fornisce una risposta di errore.

- RetentionCount

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero di istantanee che desideri archiviare. Non specificate un valore per questo parametro se specificate un valore per`RetentionDays`.

- RetentionDays

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero di giorni precedenti di istantanee che desideri archiviare. Non specificate un valore per questo parametro se specificate un valore per`RetentionCount`.

- SnapshotWithTag

  Tipo: stringa

  Valori validi: Sì | No

  Descrizione: (Obbligatorio) Specificate se le istantanee che si desidera archiviare sono contrassegnate.

- TagKey

  Tipo: stringa

  Descrizione: (Facoltativo) La chiave del tag assegnato alle istantanee che desideri archiviare.

- TagValue

  Tipo: stringa

  Descrizione: (Facoltativo) Il valore del tag assegnato alle istantanee che desideri archiviare.

- VolumeId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID del volume di cui desideri archiviare le istantanee. Utilizzate questo parametro se le istantanee non sono contrassegnate.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:ArchiveSnapshots`
- `ec2:DescribeSnapshots`

Fasi del documento

`aws:executeScript`- Archivia le istantanee utilizzando il tag specificato utilizzando i `TagValue` parametri `TagKey` and o il `VolumeId` parametro.

AWS-AttachEBSVolume

Descrizione

Collega un volume Amazon Elastic Block Store (AmazonEBS) a un'istanza Amazon Elastic Compute Cloud (AmazonEC2).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Dispositivo

  Tipo: stringa

  Descrizione: (obbligatorio) nome del dispositivo (ad esempio, /dev/sdh o xvdh).

- InstanceId

  Tipo: stringa

  Descrizione: (obbligatorio) ID dell'istanza in cui si desidera collegare il volume.

- VolumeId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del EBS volume Amazon. Il volume e l'istanza devono essere nella stessa zona di disponibilità.

AWSSupport-CalculateEBSPerformanceMetrics

Descrizione

Il `AWSSupport-CalculateEBSPerformanceMetrics` runbook aiuta a diagnosticare i problemi di EBS prestazioni di Amazon calcolando e pubblicando i parametri delle prestazioni in un pannello di controllo. CloudWatch La dashboard mostra la media IOPS e il throughput stimati per un EBS volume Amazon di destinazione o tutti i volumi collegati all'istanza Amazon Elastic Compute Cloud EC2 (Amazon) di destinazione. Per EC2 le istanze Amazon, mostra anche la media IOPS e il throughput dell'istanza. Il runbook mostra il link alla CloudWatch dashboard appena creata che mostra le metriche calcolate pertinenti. CloudWatch La CloudWatch dashboard viene creata nel tuo account con il nome:. `AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`

Come funziona?

Il runbook esegue i seguenti passaggi:

- Assicura che i timestamp specificati siano validi.
- Verifica se l'ID risorsa (Amazon EBS Volume o Amazon EC2 Instance) è valido.

- Quando fornisci un Amazon EC2 come ResourceID, viene creato CloudWatch un pannello di controllo con il IOPS totale/throughput effettivo per quell'istanza Amazon e il grafico Averimated IOPS Aver/Throughput per tutti i volumi EC2 Amazon collegati a un'istanza Amazon. EBS EC2
- Quando fornisci un EBS volume Amazon come ResourceID, viene creata CloudWatch una dashboard con il grafico Aver/Throughput IOPS stimato per quel volume.
- Dopo la generazione del CloudWatch dashboard, se il throughput medio stimato IOPS o il throughput medio stimato è rispettivamente superiore al throughput massimo IOPS o massimo, è possibile il microbursting per il volume o i volumi collegati a un'istanza Amazon. EC2

> **Note**
>
> Per i volumi espandibili (gp2, sc2 e st1), è necessario considerare il valore massimo di IOPS /throughput, fino a raggiungere il burst balance. Una volta che il burst balance è stato completamente utilizzato, vale a dire che diventa zero, prendete in considerazione le metriche di base/throughput. IOPS

> **Important**
>
> La creazione della CloudWatch dashboard potrebbe comportare costi aggiuntivi sul tuo account. Per ulteriori informazioni, consulta la guida ai CloudWatch prezzi di Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeVolumes`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypes`
- `cloudwatch:PutDashboard`

Politica di esempio

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "VisualEditor0",
                    "Effect": "Allow",
                    "Action": "cloudwatch:PutDashboard",
                    "Resource": "arn:aws:cloudwatch::Account-id:dashboard/*-EBS-
Performance-*"
                },
                {
                    "Sid": "VisualEditor1",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:DescribeInstances",
                        "ec2:DescribeVolumes",
                        "ec2:DescribeInstanceTypes"
                    ],
                    "Resource": "*"
                }
            ]
        }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

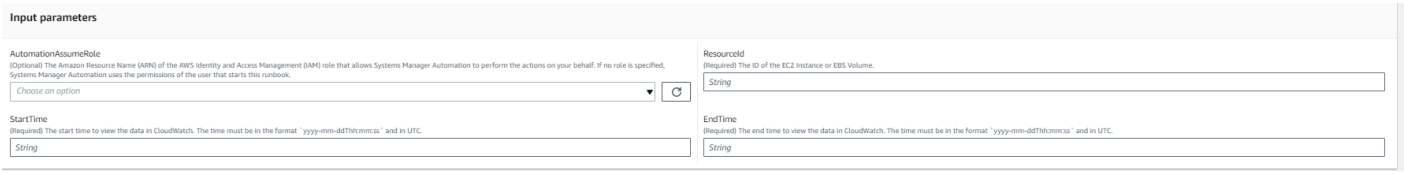
1. Accedere AWSSupport-CalculateEBSPerformanceMetricsa Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - ResourceID (obbligatorio):

     L'ID dell'EC2istanza Amazon o EBS del volume Amazon.
   - Ora di inizio (obbligatorio):

     L'ora di inizio in cui visualizzare i dati CloudWatch. L'ora deve essere nel formato `yyyy-mm-ddThh:mm:ss` e inUTC.
   - Ora di fine (obbligatorio):

     L'ora di fine della visualizzazione dei dati CloudWatch. L'ora deve essere nel formato `yyyy-mm-ddThh:mm:ss` e inUTC.



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:
   - CheckResourceIdAndTimeStamps:

     Verifica se l'ora di fine è superiore all'ora di inizio di almeno un minuto e se la risorsa fornita esiste.
   - CreateCloudWatchDashboard:

     Calcola EBS le prestazioni di Amazon e visualizza un grafico basato sul tuo Resource ID. Se fornisci un Amazon EBS Volume ID per il parametro Resource ID, questo runbook crea

una CloudWatch dashboard con il throughput medio IOPS e medio stimato per il volume AmazonEBS. Se fornisci un ID di EC2 istanza Amazon per il parametro Resource ID, questo runbook crea una CloudWatch dashboard con throughput totale medio IOPS e throughput totale medio per l'EC2istanza Amazon e con throughput medio IOPS e medio stimato per tutti i EBS volumi Amazon collegati all'istanza Amazon. EC2

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

CloudWatch Dashboard di esempio per Resource ID come EC2 istanza Amazon

CloudWatch > Dashboards >
AWSSupport-i-0[redacted]-EBS-Performance-40121150-f1be-4418-a[redacted]

Autosave: Off

AWSSupport-i-0[redacted]-EBS-Performance-... 2024-01-10T17:44:00 > 2024-01-10T18:07:00 UTC timezone Actions Save

Aggregated Metrics for EC2 Instance i-[redacted]

- Instance Type: t3.large
- EBS Optimized: True

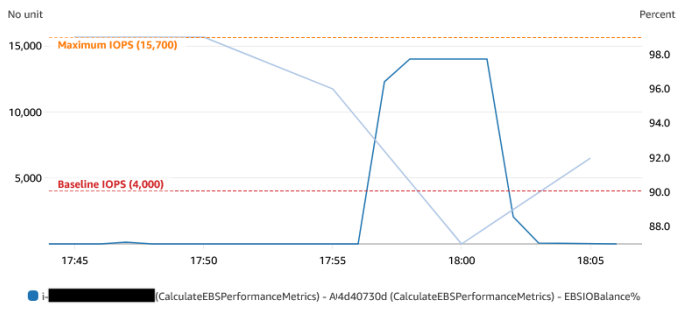
More details on EBS Optimized instances | More details on EBS Volume Types

How do I use CloudWatch to view the aggregate Amazon EBS performance metrics for an EC2 instance?

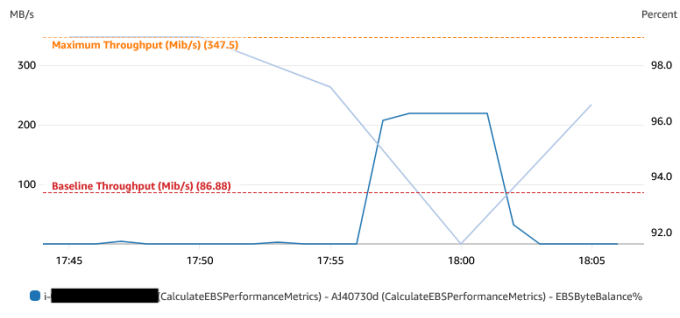
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

Note: The maximum performance can only be achieved if `BurstBalance%` for EBS volume or `EBSIOBalance%`, `EBSByteBalance%` for instance is greater than zero.

Average Total IOPS
2024-01-10 - 2024-01-10



Average Total Throughput
2024-01-10 - 2024-01-10



EBS Volume(s) Metrics

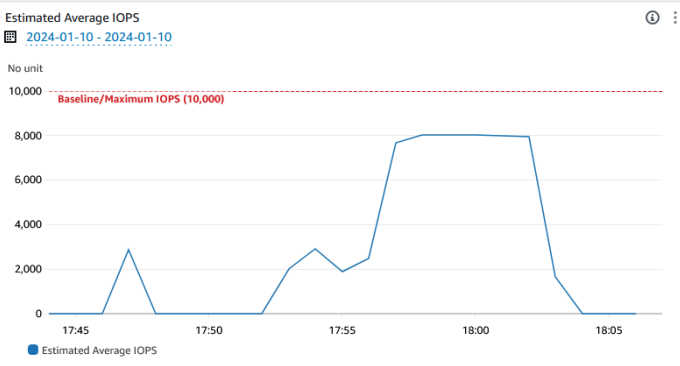
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

Note: If `Estimated Average IOPS` / `Estimated Average Throughput` is more than `Maximum IOPS` / `Maximum Throughput`, then microbusting is happening for that particular volume. **Realtime analysis for Microbusting may vary, to confirm further you can use OS-level tool that has a finer granularity than CloudWatch.** Also, the maximum performance for certain volume types can only be achieved if `BurstBalance%` is greater than zero.

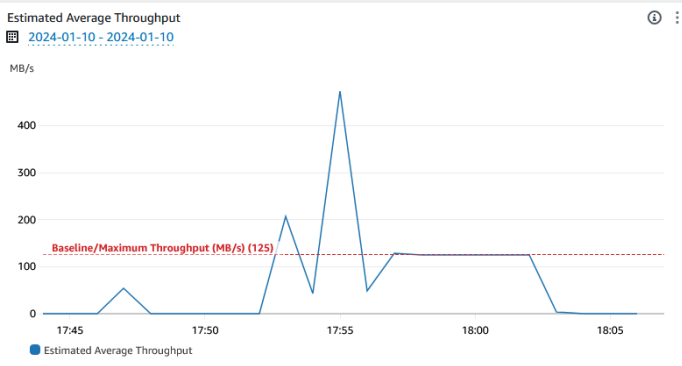
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

Estimated Average IOPS
2024-01-10 - 2024-01-10

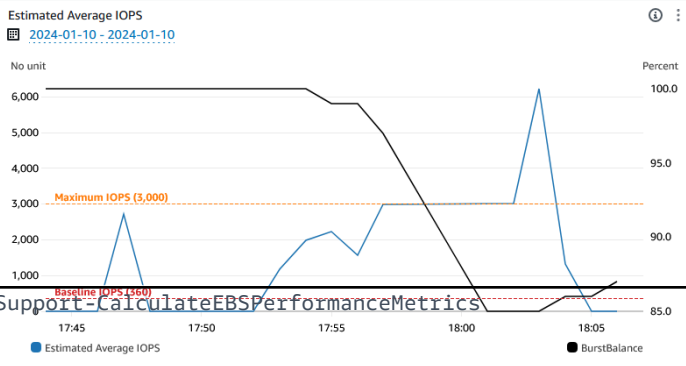


Estimated Average Throughput
2024-01-10 - 2024-01-10

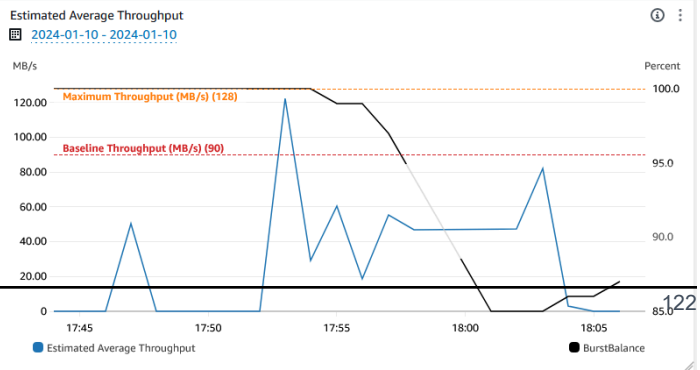


Volume: vol[redacted] | Type: gp2

Estimated Average IOPS
2024-01-10 - 2024-01-10



Estimated Average Throughput
2024-01-10 - 2024-01-10

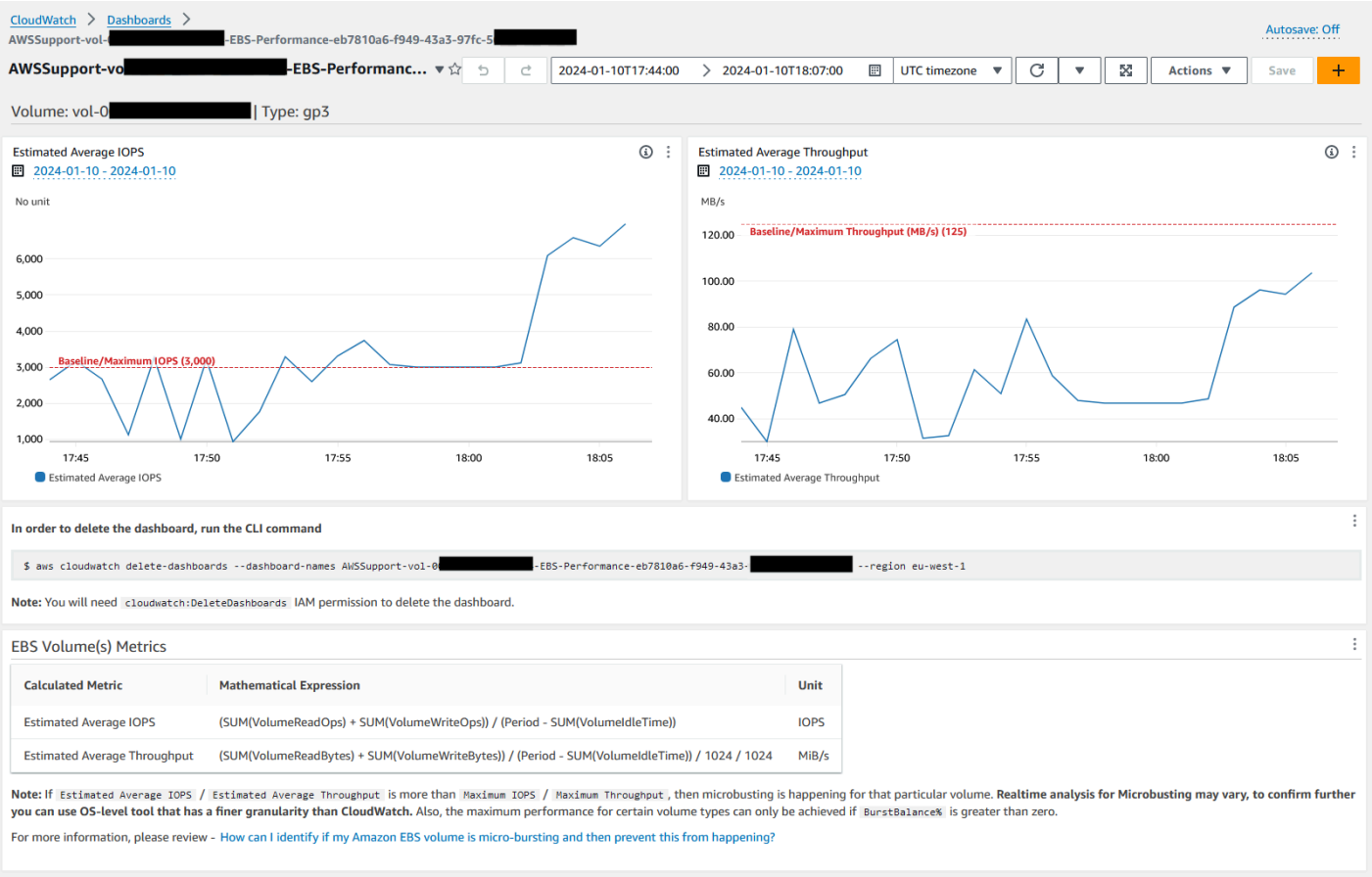


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

CloudWatch Dashboard di esempio per Resource ID come ID EBS volume Amazon



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Come posso verificare se il mio EBS volume Amazon è in fase di microscoppio e quindi evitare che ciò accada?
- Come posso utilizzare CloudWatch per visualizzare le metriche aggregate EBS delle prestazioni di Amazon per un'EC2istanza?

AWS-CopySnapshot

Descrizione

Copia uno point-in-time snapshot di un volume Amazon Elastic Block Store (AmazonEBS). Puoi copiare lo snapshot all'interno della stessa regione Regione AWS o da una regione all'altra. Le copie degli EBS snapshot Amazon crittografati rimangono crittografate. Le copie degli snapshot non crittografati rimangono non crittografate. Per copiare uno snapshot crittografato condiviso da un altro account, devi disporre delle autorizzazioni per la KMS chiave utilizzata per crittografare lo snapshot. Gli snapshot creati copiando un altro snapshot sono associati a un ID volume arbitrario che non deve essere utilizzato per nessun motivo.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Descrizione

  Tipo: stringa

  Descrizione: (Facoltativa) Una descrizione per lo EBS snapshot di Amazon.
- SnapshotId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dello EBS snapshot Amazon da copiare.

- SourceRegion

  Tipo: stringa

  Descrizione: (obbligatorio) Regione in cui lo snapshot di origine attualmente esiste.

Fasi del documento

copySnapshot - Copia un'istantanea di un EBS volume Amazon.

Output

copySnapshot. SnapshotId - L'ID della nuova istantanea.

AWS-CreateSnapshot

Descrizione

Crea un'istantanea di un EBS volume Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Descrizione

  Tipo: stringa

  Descrizione: (facoltativo) descrizione dello snapshot.

- VolumeId

  Tipo: stringa

  Descrizione: (obbligatorio) ID del volume.

AWS-DeleteSnapshot

Descrizione

Elimina un'istantanea di un EBS volume Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SnapshotId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'EBSistantanea.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descrizione

Il `AWSConfigRemediation-DeleteUnusedEBSVolume` runbook elimina un volume Amazon Elastic Block Store (EBSAmazon) inutilizzato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CreateSnapshot

Tipo: Booleano

Descrizione: (Facoltativo) Se impostata su`true`, l'automazione crea un'istantanea del EBS volume Amazon prima che venga eliminato.

- VolumeId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del EBS volume Amazon che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateSnapshot`
- `ec2:DeleteVolume`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVolumes`

Fasi del documento

- `aws:executeScript`- Verifica che il EBS volume Amazon specificato nel `VolumeId` parametro non sia in uso e crea un'istantanea in base al valore scelto per il `CreateSnapshot` parametro.
- `aws:branch`- Filiali in base al valore scelto per il `CreateSnapshot` parametro.
- `aws:waitForAwsResourceProperty`- Attende il completamento dell'istantanea.
- `aws:executeAwsApi`- Elimina l'istantanea se la creazione dell'istantanea non è riuscita.
- `aws:executeAwsApi`- Elimina il EBS volume Amazon specificato nel `VolumeId` parametro.
- `aws:executeScript`- Verifica che il EBS volume Amazon sia stato eliminato.

AWS-DeregisterAMIs

Descrizione

Il `AWS-DeregisterAMIs` runbook ti aiuta a cancellare la registrazione Amazon Machine Images (AMIs) specificando il tag che hai applicato al tuo. AMIs

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DryRun

  Tipo: stringa

  Valori validi: Sì | No

  Descrizione: (Obbligatorio) Verifica se l'utente dispone delle autorizzazioni necessarie per l'azione, senza effettuare effettivamente la richiesta, e fornisce una risposta di errore.
- RetainNumber

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero AMIs che desideri conservare. Non specificate un valore per questo parametro se specificate un valore per`Age`.
- Età

Tipo: stringa

Descrizione: (Facoltativo) Il numero di giorni precedenti AMIs che desideri conservare. Non specificate un valore per questo parametro se specificate un valore per`RetainNumber`.

- TagKey

  Tipo: stringa

  Descrizione: (Obbligatorio) La chiave del tag assegnato a AMIs cui si desidera annullare la registrazione.

- TagValue

  Tipo: stringa

  Descrizione: (Obbligatorio) Il valore del tag assegnato a chi desideri AMIs annullare la registrazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DeregisterImage`
- `ec2:DescribeImages`

Fasi del documento

- `aws:executeAwsApi`- Convalida i valori specificati per i parametri di input del runbook.
- `aws:executeAwsApi`- Annulla la registrazione AMIs utilizzando il tag specificato utilizzando i parametri and. `TagKey` `TagValue`

AWS-DetachEBSVolume

Descrizione

Scollega un EBS volume Amazon da un'istanza Amazon Elastic Compute Cloud EC2 (Amazon).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN ruolo assunto da Lambda
- VolumeId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del EBS volume. Il volume e l'istanza devono essere nella stessa zona di disponibilità.

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descrizione

Il `AWSConfigRemediation-EnableEbsEncryptionByDefault` runbook abilita la crittografia su tutti i nuovi volumi Amazon Elastic Block Store (AmazonEBS) nel Account AWS e nel

luogo in Regione AWS cui viene eseguita l'automazione. I volumi creati prima dell'esecuzione dell'automazione non sono crittografati.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:EnableEbsEncryptionByDefault`
- `ec2:GetEbsEncryptionByDefault`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Abilita l'impostazione di EBS crittografia Amazon predefinita nell'account e nella regione correnti.

- `aws:assertAwsResourceProperty`- Verifica che l'impostazione di EBS crittografia Amazon predefinita sia stata abilitata.

AWS-ExtendEbsVolume

Descrizione

Il `AWS-ExtendEbsVolume` runbook aumenta le dimensioni di un EBS volume Amazon ed estende il file system. Questa automazione supporta i `ext4` file system `xfs` e.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DriveLetter

  Tipo: stringa

  Descrizione: (Facoltativo) La lettera dell'unità di cui si desidera estendere il file system. Questo parametro è obbligatorio per le Windows istanze.

- InstanceId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID dell'EC2istanza Amazon a cui è allegato il EBS volume Amazon che desideri estendere.

- KeepSnapshot

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Determina se conservare lo snapshot creato prima di aumentare le dimensioni del EBS volume Amazon.

- MountPoint

  Tipo: stringa

  Descrizione: (Facoltativo) Il punto di montaggio dell'unità di cui si desidera estendere il file system. Questo parametro è obbligatorio per le istanze Linux.

- SizeGib

  Tipo: stringa

  Descrizione: (Obbligatorio) La dimensione in GiB in cui desideri modificare il EBS volume Amazon.

- VolumeId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del EBS volume che desideri estendere.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateSnapshot`
- `ec2:CreateTags`
- `ec2:DeleteSnapshot`

- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:SendCommand`

Fasi del documento

- `aws:executeScript`- Aumenta la dimensione del volume fino al valore specificato nel `VolumeId` parametro ed estende il file system.

AWSSupport-ModifyEBSSnapshotPermission

Descrizione

Il `AWSSupport-ModifyEBSSnapshotPermission` runbook ti aiuta a modificare le autorizzazioni per più snapshot di Amazon Elastic Block Store EBS (Amazon). Usando questo runbook, puoi creare istantanee `Public` o `Private` condividerle con altri. Account AWS Le istantanee crittografate con una KMS chiave predefinita non possono essere condivise con altri account utilizzando questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AccountIds

  Tipo: StringList

  Impostazione predefinita: none

  Descrizione: (Facoltativo) Gli IDs account con cui vuoi condividere le istantanee. Questo parametro è obbligatorio se si immette `No` il valore del `Private` parametro.

- AccountPermissionOperation

  Tipo: stringa

  Valori validi: aggiungi | rimuovi

  Impostazione predefinita: none

  Descrizione: (Facoltativo) Il tipo di operazione da eseguire.

- Privata

  Tipo: stringa

  Valori validi: Sì | No

  Descrizione: (Obbligatorio) Inserisci `No` il valore se desideri condividere istantanee con account specifici.

- SnapshotIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Le EBS istantanee IDs di Amazon di cui desideri modificare l'autorizzazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSnapshots`
- `ec2:ModifySnapshotAttribute`

Fasi del documento

1. `aws:executeScript`- Verifica le IDs istantanee fornite nel parametro. `SnapshotIds` Dopo aver verificato iIIDs, lo script verifica la presenza di istantanee crittografate e genera un elenco, se ne vengono trovate.
2. `aws:branch`- Suddivide l'automazione in base al valore immesso per il parametro. `Private`
3. `aws:executeScript`- Modifica le autorizzazioni delle istantanee specificate per condividerle con gli account specificati.
4. `aws:executeScript`- Modifica le autorizzazioni delle istantanee per cambiarle da a. `Public` `Private`

Output

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Risultato

MakePrivate.Risultato

MakePrivate.Comandi

`AWSConfigRemediation-ModifyEBSVolumeType`

Descrizione

Il `AWSConfigRemediation-ModifyEBSVolumeType` runbook modifica il tipo di volume di un volume Amazon Elastic Block Store EBS (Amazon). Dopo la modifica del tipo di volume, il volume entra in uno `optimizing` stato. Per informazioni sul monitoraggio dell'avanzamento delle modifiche del volume, consulta Monitorare l'avanzamento delle modifiche del volume nella Amazon EC2 User Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- EbsVolumeId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del EBS volume Amazon che desideri modificare.
- EbsVolumeType

  Tipo: stringa

  Valori validi: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

  Descrizione: il tipo di volume in cui desideri modificare il EBS volume Amazon. Per informazioni sui tipi di EBS volume Amazon, consulta i tipi di EBS volume Amazon nella Amazon EC2 User Guide.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Verifica che lo stato del volume sia `available` o. `in-use`
- `aws:executeAwsApi`- Modifica il EBS volume Amazon specificato nel `EbsVolumeId` parametro.
- `aws:waitForAwsResourceProperty`- Verifica che il tipo di volume sia stato modificato in base al valore specificato nel `EbsVolumeType` parametro.

Amazon EC2

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Compute Cloud. I runbook per Amazon Elastic Block Store si trovano nella Amazon EBS sezione di riferimento del runbook. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-ASGEnterStandby
- AWS-ASGExitStandby
- AWS-CreateImage
- AWS-DeleteImage
- AWS-PatchAsgInstance
- AWS-PatchInstanceWithRollback
- AWS-QuarantineEC2Instance
- AWS-ResizeInstance
- AWS-RestartEC2Instance
- AWS-SetupJupyter
- AWS-StartEC2Instance
- AWS-StopEC2Instance

- AWS-TerminateEC2Instance
- AWS-UpdateLinuxAmi
- AWS-UpdateWindowsAmi
- AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck
- AWSConfigRemediation-EnforceEC2InstanceIMDSv2
- AWSEC2-CloneInstanceAndUpgradeSQLServer
- AWSEC2-CloneInstanceAndUpgradeWindows
- AWSEC2-ConfigureSTIG
- AWSEC2-PatchLoadBalancerInstance
- AWSEC2-SQLServerDBRestore
- AWSSupport-ActivateWindowsWithAmazonLicense
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2
- AWSPremiumSupport-ChangeInstanceTypeIntelToAMD
- AWSSupport-CheckXenToNitroMigrationRequirements
- AWSSupport-ConfigureEC2Metadata
- AWSSupport-CopyEC2Instance
- AWSSupport-EnableWindowsEC2SerialConsole
- AWSSupport-ExecuteEC2Rescue
- AWSSupport-ListEC2Resources
- AWSSupport-ManageRDPSettings
- AWSSupport-ManageWindowsService
- AWSSupport-MigrateEC2ClassicToVPC
- AWSSupport-MigrateXenToNitroLinux
- AWSSupport-ResetAccess
- AWSSupport-ResetLinuxUserPassword
- AWSPremiumSupport-ResizeNitroInstance
- AWSSupport-RestoreEC2InstanceFromSnapshot
- AWSSupport-SendLogBundleToS3Bucket
- AWSSupport-StartEC2RescueWorkflow
- AWSPremiumSupport-TroubleshootEC2DiskUsage

- AWSSupport-TroubleshootEC2InstanceConnect
- AWSSupport-TroubleshootLinuxMGNDRSAgentLogs
- AWSSupport-TroubleshootRDP
- AWSSupport-TroubleshootSSH
- AWSSupport-TroubleshootSUSERegistration
- AWSSupport-TroubleshootWindowsPerformance
- AWSSupport-TroubleshootWindowsUpdate
- AWSSupport-UpgradeWindowsAWSDrivers

AWS-ASGEnterStandby

Descrizione

Modifica lo stato di standby di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) in un gruppo Auto Scaling.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID di un'istanza Amazon EC2 per la quale desideri modificare lo stato di standby all'interno di un gruppo Auto Scaling.
- LambdaRoleArn

  Tipo: String

  Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

AWS-ASGExitStandby

Descrizione

Modifica lo stato di standby di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) in un gruppo Auto Scaling.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID di un'istanza EC2 per la quale si desidera modificare lo stato di standby all'interno di un gruppo Auto Scaling.

- LambdaRoleArn

  Tipo: String

  Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

AWS-CreateImage

Descrizione

Crea un nuovo Amazon Machine Image (AMI) da un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatoria) ID dell'istanza EC2.

- NoReboot

  Tipo: Booleano

  Descrizione: (facoltativo) non riavviare l'istanza prima di creare l'immagine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage",
                "ec2:DescribeImages"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS-DeleteImage

Descrizione

Elimina una Amazon Machine Image (AMI) e tutte le istantanee associate.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ImageId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'AMI.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
```

```
            "Resource": "arn:aws:ec2:{region}::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeImages",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeregisterImage",
            "Resource": "*"
        }
    ]
}
```

AWS-PatchAsgInstance

Descrizione

Applica patch alle istanze di Amazon Elastic Compute Cloud (Amazon EC2) in un gruppo Auto Scaling.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza a cui applicare le patch. Non specificare un ID di istanza configurato per l'esecuzione durante una finestra di manutenzione.

- LambdaRoleArn

  Tipo: String

  Descrizione: (Facoltativo) L'ARN del ruolo che consente alla Lambda creata da Automation di eseguire le azioni per conto dell'utente. Se non specificato, verrà creato un ruolo transitorio per eseguire la funzione Lambda.

- WaitForInstance

  Tipo: String

  Valore predefinito: PT2M

  Descrizione: (Facoltativo) Durata della sospensione dell'automazione per consentire all'istanza di tornare in servizio.

- WaitForReboot

  Tipo: String

  Valore predefinito: PT5M

  Descrizione: (Facoltativo) Durata della sospensione dell'automazione per consentire il riavvio di un'istanza con patch.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- ssm:GetCommandInvocation
- ssm:GetParameter
- ssm:SendCommand
- cloudformation:CreateStack
- cloudformation:DeleteStack
- cloudformation:DescribeStacks
- ec2:CreateTags
- ec2:DescribeInstances
- ec2:RunInstances
- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:PassRole
- iam:PutRolePolicy
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction

AWS-PatchInstanceWithRollback

Descrizione

Conforma un'istanza EC2 alla baseline delle patch applicabili. Ripristina il volume principale in caso di errore.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (Obbligatorio) EC2 InstanceId a cui applichiamo la patch-baseline.
- LambdaAssumeRole

  Tipo: String

  Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.
- ReportS3Bucket

  Tipo: String

  Descrizione: (Facoltativo) Destinazione del bucket Amazon S3 per il rapporto di conformità generato durante il processo.

Fasi del documento

Numero fase	Nome fase	Operazione di automazione
1	createDocumentStack	`aws:createStack`
2	IdentifyRootVolume	`aws:invokeLambdaFunction`
3	PrePatchSnapshot	`aws:executeAutomation`
4	installMissingUpdates	`aws:runCommand`
5	SleepThruInstallation	`aws:invokeLambdaFunction`
6	CheckCompliance	`aws:invokeLambdaFunction`
7	SaveComplianceReportToS3	`aws:invokeLambdaFunction`
8	ReportSuccessOrFailure	`aws:invokeLambdaFunction`
9	RestoreFromSnapshot	`aws:invokeLambdaFunction`
10	DeleteSnapshot	`aws:invokeLambdaFunction`
11	deleteCloudFormationModello	`aws:deleteStack`

Output

IdentifyRootVolume.Carico utile

PrePatchSnapshot.Uscita

SaveComplianceReportToS3. Carico utile

RestoreFromSnapshot.Carico utile

CheckCompliance.Carico utile

AWS-QuarantineEC2Instance

Descrizione

Con il `AWS-QuarantineEC2Instance` runbook, puoi assegnare un gruppo di sicurezza a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che non consente alcun traffico in entrata o in uscita.

> **Important**
>
> Le modifiche alle impostazioni RDP devono essere esaminate attentamente prima di eseguire questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza gestita per la quale gestire le impostazioni RDP.

- IsolationSecurityGroup

  Tipo: String

  Descrizione: (Obbligatorio) Il nome del gruppo di sicurezza che desideri assegnare all'istanza per impedire il traffico in entrata o in uscita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:DescribeAutoScalingInstances`
- `autoscaling:DetachInstances`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSnapshot`
- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSnapshots`
- `ec2:ModifyInstanceAttribute`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza.
- `aws:executeScript`- Verifica che l'istanza non faccia parte di un gruppo Auto Scaling.
- `aws:executeAwsApi`- Crea un'istantanea del volume principale collegato all'istanza.

- `aws:waitForAwsResourceProperty`- Attende lo stato dell'istantanea. `completed`
- `aws:executeAwsApi`- Assegna il gruppo di sicurezza specificato nel `IsolationSecurityGroup` parametro all'istanza.

Output

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Descrizione

Cambia il tipo di istanza di un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza.
- InstanceType

  Tipo: String

  Descrizione: (obbligatorio) tipo di istanza.
- LambdaAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'ARN del ruolo assunto da Lambda.

AWS-RestartEC2Instance

Descrizione

Riavvia una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: StringList

  Descrizione: (Obbligatorio) Gli ID delle istanze Amazon EC2 da riavviare.

AWS-SetupJupyter

Descrizione

Il `AWS-SetupJupyter` runbook ti aiuta a configurare Jupyter Notebook su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Puoi specificare un'istanza esistente o fornire un Amazon Machine Image (AMI) ID per l'automazione per avviare e configurare una nuova istanza. Prima di iniziare, è necessario creare un `SecureString` parametro in Parameter Store da utilizzare come password per Jupyter Notebook. Parameter Store è una funzionalità di. AWS Systems Manager Per informazioni sulla creazione di parametri, vedere Creazione di parametri nella Guida per l'AWS Systems Managerutente.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: String

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AmiId

  Tipo: String

  Descrizione: (Facoltativo) L'ID AMI che desideri utilizzare per avviare una nuova istanza e configurare Jupyter Notebook.

- InstanceId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID dell'istanza su cui si desidera configurare Jupyter Notebook.

- InstanceType

  Tipo: String

  Predefinito: t3.medium

  Descrizione: (Facoltativo) Se stai lanciando una nuova istanza per configurare Jupyter Notebook, specifica il tipo di istanza che desideri utilizzare.

- JupyterPasswordChiave SSM

  Tipo: String

  Descrizione: (Obbligatorio) Il nome del `SecureString` parametro in Parameter Store che desideri utilizzare come password per Jupyter Notebook.

- KeyPairName

  Tipo: String

  Descrizione: (Facoltativo) La coppia di chiavi che desideri associare all'istanza appena avviata.

- RemoteAccessCidr

  Tipo: String

Impostazione predefinita: 0.0.0.0/0

Descrizione: (Facoltativo) L'intervallo CIDR da cui si desidera consentire il traffico SSH.

- RoleName

  Tipo: String

  Impostazione predefinita: SSM ManagedInstanceProfileRole

  Descrizione: (Facoltativo) Il nome del profilo dell'istanza per l'istanza appena avviata.

- StackName

  Tipo: String

  Predefinito: CreateManagedInstanceStack {{automation:Execution_ID}}

  Descrizione: (Facoltativo) Il nome AWS CloudFormation dello stack che desideri venga utilizzato dall'automazione.

- SubnetId

  Tipo: String

  Impostazione predefinita: Default

  Descrizione: (Facoltativo) La sottorete da utilizzare per avviare la nuova istanza.

- VpcId

  Tipo: String

  Impostazione predefinita: Default

  Descrizione: (Facoltativo) L'ID del cloud privato virtuale (VPC) in cui desideri avviare la nuova istanza.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`

- ssm:GetCommandInvocation
- ssm:GetParameter
- ssm:SendCommand
- ssm:StartAutomationExecution
- cloudformation:CreateStack
- cloudformation:DeleteStack
- cloudformation:DescribeStacks
- ec2:DescribeInstances
- ec2:DescribeKeyPairs
- ec2:RunInstances
- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:PassRole
- iam:PutRolePolicy
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction

Fasi del documento

- aws:executeScript- Configura Jupyter Notebook sull'istanza specificata o su un'istanza appena avviata, utilizzando i valori specificati per i parametri di input del runbook.

AWS-StartEC2Instance

Descrizione

Avvia una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: StringList

  Descrizione: (obbligatoria) istanze EC2 da avviare.

AWS-StopEC2Instance

Descrizione

Arresta una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: StringList

  Descrizione: (Obbligatorio) istanze EC2 da arrestare.

AWS-TerminateEC2Instance

Descrizione

Termina una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: StringList

  Descrizione: (obbligatoria) ID di una o più istanze EC2 da terminare.

AWS-UpdateLinuxAmi

Descrizione

Aggiorna un Amazon Machine Image (AMI) con pacchetti di distribuzione Linux e software Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  ▬Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ExcludePackages

  - Tipo: stringa

  Impostazione predefinita: none

  Descrizione: (facoltativo) nomi dei pacchetti da non aggiornare, in tutte le condizioni. Per impostazione predefinita ("none"), non viene escluso alcun pacchetto.

- IamInstanceProfileName

  - Tipo: stringa

  Impostazione predefinita: ManagedInstanceProfile

  Descrizione: (Obbligatorio) Il profilo dell'istanza che consente a Systems Manager di gestire l'istanza.

- IncludePackages

  - Tipo: stringa

  Impostazione predefinita: all

  Descrizione: (facoltativo) vengono aggiornati solo i pacchetti specificati. Per impostazione predefinita ("all"), vengono applicati tutti gli aggiornamenti disponibili.

- InstanceType

  - Tipo: stringa

  Impostazione predefinita: t2.micro

  Descrizione: (facoltativo) tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione.

- MetadataOptions

  Tipo: StringMap

Predefinito: {» HttpEndpoint «: «abilitato», "HttpTokens«: «opzionale"}

Descrizione: (Facoltativo) Le opzioni dei metadati per l'istanza. Per ulteriori informazioni, consulta InstanceMetadataOptionsRequest.

- PostUpdateScript

  -Tipo: stringa

  Impostazione predefinita: none

  Descrizione: (facoltativo) URL di uno script da eseguire dopo l'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.

- PreUpdateScript

  -Tipo: stringa

  Impostazione predefinita: none

  Descrizione: (facoltativo) URL di uno script da eseguire prima dell'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.

- SecurityGroupIds

  -Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole degli ID dei gruppi di sicurezza a cui si desidera applicareAMI.

- SourceAmiId

  -Tipo: stringa

  Descrizione: (obbligatorio) ID AMI (Amazon Machine Image) di origine.

- SubnetId

  -Tipo: stringa

  Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera avviare l'istanza. Se hai eliminato il tuo VPC predefinito, questo parametro è obbligatorio.

- TargetAmiName

- Tipo: stringa

  Predefinito: UpdateLinuxAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

  Descrizione: (facoltativo) nome della nuova AMI che verrà creata. L'impostazione predefinita è una stringa generata dall'ID AMI di origine e la data/ora di creazione.

AWS-UpdateWindowsAmi

Descrizione

Aggiorna un Microsoft Windows Amazon Machine Image (AMI). Per impostazione predefinita, questo runbook installa tutti gli aggiornamenti di Windows, il software Amazon e i driver Amazon. Esegue quindi Sysprep per creare una nuova AMI. Supporta Windows Server 2008 R2 o versione successiva.

> **Important**
>
> Se le istanze si connettono AWS Systems Manager tramite endpoint VPC, questo runbook fallirà a meno che non venga utilizzato nella regione us-east-1. Le istanze devono avere TLS 1.2 abilitato per utilizzare questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

  - Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Categories

  - Tipo: stringa

  Descrizione: (facoltativo) specifica una o più categorie di aggiornamento. È possibile filtrare le categorie utilizzando valori separati da virgole. Opzioni: Applicazione, Connettori CriticalUpdates DefinitionUpdates, DeveloperKits,, DriverFeaturePacks, Guida, Microsoft, SecurityUpdates ServicePacksUpdateRollups, Strumenti e Aggiornamenti. I formati validi includono una singola voce, per esempio:CriticalUpdates. Oppure puoi specificare un elenco separato da virgole:CriticalUpdates,SecurityUpdates. NOTA: non devono essere presenti spazi tra le virgole.

- ExcludeKbs

  - Tipo: stringa

  Descrizione: (facoltativo) specifica uno o più ID articolo Microsoft Knowledge Base (KB) da escludere. È possibile escludere più ID utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543.

- IamInstanceProfileName

  - Tipo: stringa

  Impostazione predefinita: ManagedInstanceProfile

  Descrizione: (Obbligatorio) Il nome del ruolo che consente a Systems Manager di gestire l'istanza.

- IncludeKbs

  - Tipo: stringa

  Descrizione: (facoltativo) specifica uno o più ID articolo Microsoft Knowledge Base (KB) da includere. È possibile installare più ID utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543.

- InstanceType

  - Tipo: stringa

Impostazione predefinita: t2.medium

Descrizione: (facoltativo) tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione. Impostazione predefinita: t2.medium

- MetadataOptions

  Tipo: StringMap

  Predefinito: {» HttpEndpoint «: «abilitato», "HttpTokens«: «opzionale"}

  Descrizione: (Facoltativo) Le opzioni dei metadati per l'istanza. Per ulteriori informazioni, consulta InstanceMetadataOptionsRequest.

- PostUpdateScript

  -Tipo: stringa

  Descrizione: (facoltativo) script specificato come stringa. Verrà eseguito dopo l'installazione degli aggiornamenti del sistema operativo.

- PreUpdateScript

  -Tipo: stringa

  Descrizione: (facoltativo) script specificato come stringa. Verrà eseguito prima dell'installazione degli aggiornamenti del sistema operativo.

- PublishedDateAfter

  -Tipo: stringa

  Descrizione: (facoltativo) specifica la data dopo la quale gli aggiornamenti devono essere pubblicati. Ad esempio, se viene specificato 01/01/2017, verranno restituiti tutti gli aggiornamenti rilevati durante la ricerca di Windows Update e la cui pubblicazione è successiva alla data 01/01/2017.

- PublishedDateBefore

  -Tipo: stringa

  Descrizione: (facoltativo) specifica la data prima della quale gli aggiornamenti devono essere pubblicati. Ad esempio, se viene specificato 01/01/2017, verranno restituiti tutti gli aggiornamenti

rilevati durante la ricerca di Windows Update e la cui pubblicazione è anteriore alla data 01/01/2017.

- PublishedDaysOld

  - Tipo: stringa

  Descrizione: (facoltativo) specifica il numero di giorni dalla data di pubblicazione degli aggiornamenti. Ad esempio, se si specifica 10, verranno restituiti tutti gli aggiornamenti rilevati durante la ricerca di Windows Update e la cui pubblicazione è avvenuta 10 o più giorni prima.

- SecurityGroupIds

  - Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole degli ID dei gruppi di sicurezza a cui si desidera applicareAMI.

- SeverityLevels

  - Tipo: stringa

  Descrizione: (facoltativo) specifica uno o più livelli di gravità MSRC associati a un aggiornamento. È possibile filtrare i livello di gravità utilizzando valori separati da virgole. Per impostazione predefinita, vengono selezionati tutti i livelli di sicurezza. Se il valore viene specificato, l'elenco di aggiornamenti viene filtrato in base a tali valori. Opzioni: Critical, Important, Low, Moderate o Unspecified. I formati validi includono una singola voce, ad esempio: Critical. In alternativa, è possibile specificare un elenco di valori separati da virgole: Critical,Important,Low.

- SourceAmiId

  - Tipo: stringa

  Descrizione: (Obbligatorio) L'AMIID di origine.

- SubnetId

  - Tipo: stringa

  Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera avviare l'istanza. Se hai eliminato il tuo VPC predefinito, questo parametro è obbligatorio.

- TargetAmiName

  - Tipo: stringa

Predefinito: UpdateWindowsAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

Descrizione: (facoltativo) nome della nuova AMI che verrà creata. L'impostazione predefinita è una stringa generata dall'ID AMI di origine e la data/ora di creazione.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Descrizione

Il `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` runbook consente i controlli di integrità per il gruppo Amazon EC2 Auto Scaling (Auto Scaling) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- AutoScalingGroupARN

  Tipo: String

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del gruppo di auto scaling su cui desideri abilitare i controlli di integrità.

- HealthCheckGracePeriod

  Tipo: integer

  Impostazione predefinita: 300

  Descrizione: (Facoltativo) La quantità di tempo, in secondi, che Auto Scaling attende prima di verificare lo stato di salute di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che è entrata in servizio.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeAutoScalingGroups`
- `ec2:UpdateAutoScalingGroup`

Fasi del documento

- `aws:executeScript`- Abilita i controlli di integrità sul gruppo Auto Scaling specificato nel `AutoScalingGroupARN` parametro.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descrizione

Il `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` runbook richiede l'istanza Amazon Elastic Compute Cloud (Amazon EC2) specificata per utilizzare Instance Metadata Service Version 2 (IMDSv2).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- InstanceId

  ▬Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 che desideri richiedere per utilizzare IMDSv2.
- AutomationAssumeRole

  ▬Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- HttpPutResponseHopLimit

  Tipo: integer

  Descrizione: (Facoltativo) Il limite di risposta Hop dal servizio IMDS ritorna al richiedente. Impostato su 2 o superiore per le istanze EC2 che ospitano contenitori. Imposta su 0 per non modificare (impostazione predefinita).

  Schema consentito: `^([1-5]?\d|6[0-4])$`

  Impostazione Predefinita: 0

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeInstances
- ec2:ModifyInstanceMetadataOptions

Fasi del documento

- aws:executeScript- Imposta l'HttpTokensopzione required su sull'istanza Amazon EC2 specificata nel InstanceId parametro.
- aws:assertAwsResourceProperty- Verifica che IMDSv2 sia richiesto sull'istanza Amazon EC2.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descrizione

Creane un'EC2istanza AMI da un'istanza per Windows Server eseguire SQL Server 2008 o versioni successive, quindi AMI aggiornala a una versione successiva di SQL Server. Sono supportate solo le versioni in lingua inglese di SQL Server.

Sono supportati i seguenti percorsi di aggiornamento:

- SQLDa Server 2008 a SQL Server 2017, 2016 o 2014
- SQLDa Server 2008 R2 a SQL Server 2017, 2016 o 2014
- SQLDa Server 2012 a SQL Server 2019, 2017, 2016 o 2014
- SQLDa Server 2014 a SQL Server 2019, 2017 o 2016
- SQLDa Server 2016 a SQL Server 2019 o 2017

Se si utilizza una versione precedente di Windows Server incompatibile con SQL Server 2019, il documento di automazione deve aggiornare la versione di Windows Server alla 2016.

L'aggiornamento è un processo in più fasi il cui completamento può richiedere 2 ore. L'automazione crea l'istanza AMI dall'istanza e quindi avvia un'istanza temporanea dalla nuova AMI nell'istanza specificata. SubnetID I gruppi di sicurezza associati all'istanza originale vengono applicati all'istanza temporanea. L'automazione esegue quindi un aggiornamento TargetSQLVersion sul posto

all'istanza temporanea. Dopo l'aggiornamento, l'automazione ne crea una nuova AMI dall'istanza temporanea e quindi termina l'istanza temporanea.

Puoi testare la funzionalità dell'applicazione lanciando la nuova AMI nel tuo. VPC Al termine del test e prima di eseguire un altro aggiornamento, pianificare il tempo di inattività dell'applicazione prima passare in modo definitivo all'istanza aggiornata.

> **Note**
>
> Se desideri modificare il nome del computer dell'EC2istanza avviata dalla nuovaAMI, consulta Rinominare un computer che ospita un'istanza autonoma del server. SQL

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Prerequisiti

- TLSversione 1.2.
- Sono supportate solo le versioni in inglese di SQL Server.
- L'EC2istanza deve utilizzare una versione Windows Server 2008 R2 (o successiva) e SQL Server 2008 (o successiva). Windows Server
- Verifica che SSM Agent sia installato sull'istanza. Per ulteriori informazioni, consulta Installazione e configurazione SSM dell'agente sulle EC2 istanze per Windows Server.
- Configurate l'istanza per utilizzare un ruolo di profilo di istanza AWS Identity and Access Management (IAM). Per ulteriori informazioni, vedere Creare un profilo di IAM istanza per Systems Manager.

- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio dell'istanza.
- Per le istanze che utilizzano una versione del SQL server Bring Your Own License (BYOL), si applicano i seguenti prerequisiti aggiuntivi:
  - Fornite un ID di EBS istantanea che includa il supporto di installazione del SQL server di destinazione. Per farlo:
    1. Verifica che sull'EC2istanza sia in esecuzione Windows Server 2008 R2 o versione successiva.
    2. Crea un EBS volume da 6 GB nella stessa zona di disponibilità in cui è in esecuzione l'istanza. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
    3. Fai clic con il pulsante destro del mouse sull'unità ISO e montalo su un'istanza come, ad esempio, l'unità E.
    4. Copiare il contenuto ISO dell'unità E:\ all'unità D:\
    5. Creare un'EBSistantanea del volume da 6 GB creato nel passaggio 2.

Limitazioni

- L'aggiornamento può essere eseguito solo su un SQL server utilizzando l'autenticazione Windows.
- Verificare che sulle istanze non siano presenti aggiornamenti delle patch di sicurezza in sospeso. Aprire Control Panel (Pannello di controllo), quindi scegliere Check for updates (Verifica disponibilità aggiornamenti).
- SQLLe distribuzioni di server in modalità HA e mirroring non sono supportate.

Parametri

- IamInstanceProfile

  Tipo: stringa

  Descrizione: (obbligatorio) profilo dell'istanza IAM.
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatoria) L'istanza che esegue Windows Server 2008 R2 (o versione successiva) e SQL Server 2008 (o versione successiva).

- KeepPreUpgradeImageBackUp

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, l'automazione non elimina il AMI creato dall'istanza prima dell'aggiornamento. Se è impostata su`true`, è necessario eliminare laAMI. Per impostazione predefinita, AMI viene eliminato.

- SubnetId

  Tipo: stringa

  Descrizione: (obbligatorio) specifica una sottorete per il processo di aggiornamento. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, Amazon S3 e Microsoft (per scaricare le patch).

- SQLServerSnapshotId

  Tipo: stringa

  Descrizione: ID snapshot (condizionale) per il supporto di installazione del server di destinazione. SQL Questo parametro è obbligatorio per le istanze che utilizzano una BYOL SQL versione del server. Questo parametro è facoltativo per le istanze incluse nella licenza SQL Server (istanze avviate utilizzando un' AWS Amazon Machine Image for Windows Server con Microsoft Server fornita). SQL

- RebootInstanceBeforeTakingImage

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, l'automazione riavvia l'istanza prima di creare un pre-aggiornamento. AMI Per impostazione predefinita, l'automazione non si riavvia prima dell'aggiornamento.

- T argetSQLVersion

  Tipo: stringa

  Descrizione: (Facoltativo) Seleziona la versione del SQL server di destinazione.

  Obiettivi possibili:

  - SQLServer 2019
  - SQLServer 2017

- SQLServer 2016
- SQLServer 2014

Obiettivo predefinito: SQL Server 2016

Output

AMIId: l'ID dell'istanza AMI creata dall'istanza che è stata aggiornata a una versione successiva di SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descrizione

Crea un'istanza Amazon Machine Image (AMI) da un'istanza Windows Server 2008 R2, 2012 R2, 2016 o 2019, quindi esegui l'aggiornamento AMI alla versione Windows Server 2016, 2019 o 2022. I percorsi di aggiornamento supportati sono i seguenti.

- Windows ServerDal 2008 R2 al 2016. Windows Server
- Da Windows Server 2012 R2 a Windows Server 2016.
- Windows Server 2012 R2 a Windows Server 2019.
- Windows ServerDal 2012 R2 al 2022. Windows Server
- Da Windows Server 2016 a Windows Server 2019.
- Windows ServerDal 2016 al Windows Server 2022.
- Windows ServerDal 2019 al Windows Server 2022.

L'operazione di aggiornamento è un processo in più fasi il cui completamento può richiedere 2 ore. Consigliamo di effettuare l'aggiornamento di un sistema operativo su istanze con almeno 2 vCPU e 4GB di RAM. L'automazione crea un'AMI dall'istanza e quindi avvia un'istanza temporanea dall'AMI appena creato nell'`SubnetId`ambito specificato. I gruppi di sicurezza associati all'istanza originale vengono applicati all'istanza temporanea. L'automazione esegue quindi un aggiornamento `TargetWindowsVersion` sul posto all'istanza temporanea. Per aggiornare l'istanza Windows Server 2008 R2 al Windows Server 2016, 2019 o 2022, un aggiornamento sul posto viene eseguito due volte perché l'aggiornamento diretto di Windows Server 2008 R2 al Windows Server 2016, 2019 o 2022 non è supportato. L'automazione aggiorna o installa anche i AWS driver richiesti dall'istanza

temporanea. Dopo l'aggiornamento, l'automazione crea una nuova AMI dall'istanza temporanea e quindi termina l'istanza temporanea.

Puoi testare la funzionalità dell'applicazione avviando un'istanza di test dall'AMI aggiornata nel tuo Amazon Virtual Private Cloud (Amazon VPC). Al termine del test e prima di eseguire un altro aggiornamento, pianificare il tempo di inattività dell'applicazione prima di passare in modo definitivo all'AMI aggiornata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows ServerEdizioni 2008 R2, 2012 R2, 2016 o 2019 Standard e Datacenter

Prerequisiti

- Versione TLS 1.2.
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta Installazione e configurazione dell'agente SSM su istanze EC2 per Windows Server.
- È necessario installare Windows PowerShell 3.0 o versione successiva sull'istanza.
- Per le istanze che vengono aggiunte a un dominio Microsoft Active Directory, si consiglia di specificare un `SubnetId` che non dispone di connettività ai controller di dominio per evitare conflitti di nomi host.
- La sottorete dell'istanza deve disporre di connettività in uscita a Internet, che consente l'accesso AWS servizi ad Amazon S3 e l'accesso al download di patch da Microsoft. Questo requisito è soddisfatto se la sottorete è una sottorete pubblica e l'istanza ha un indirizzo IP pubblico o se la sottorete è una sottorete privata con un percorso che invia il traffico Internet a un dispositivo NAT pubblico.
- Questa automazione funziona solo con le istanze Windows Server 2008 R2, 2012 R2, 2016 e 2019.

- Configura l'Windows Serveristanza con un profilo di istanza AWS Identity and Access Management (IAM) che fornisce le autorizzazioni necessarie per Systems Manager. Per ulteriori informazioni, consulta Creazione di un profilo dell'istanza IAM per Systems Manager.
- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio.
- Se l'istanza non utilizza una licenza Windows AWS fornita, specifica un ID snapshot Amazon EBS che includa i supporti di installazione Windows Server 2012 R2. Per farlo:
  - Verificare che l'istanza EC2 esegua Windows Server 2012 o versioni successive.
  - Creare un volume EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
  - Fare clic con il pulsante destro del mouse sull'oggetto ISO e montarlo su un'istanza, ad esempio, sull'unità E.
  - Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
  - Creare uno snapshot EBS del volume da 6 GB creato nella precedente fase 2.

Limitazioni

Questa automazione non supporta l'aggiornamento di controller di dominio Windows, cluster o sistemi operativi per desktop Windows. Questa automazione, inoltre, non supporta le istanze EC2 per Windows Server con i seguenti ruoli installati.

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Parameters (Parametri)

- AlternativeKeyPairName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome di una coppia di key pair alternativa da utilizzare durante il processo di aggiornamento. Ciò è utile in situazioni in cui la coppia di chiavi assegnata all'istanza originale non è disponibile. Se all'istanza originale non è stata assegnata una coppia di key pair, è necessario specificare un valore per questo parametro.

- BYOL WindowsMediaSnapshotId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID dello snapshot di Amazon EBS da copiare che include i supporti di installazione di Windows Server 2012R2. Obbligatorio solo se si sta eseguendo l'aggiornamento di un'istanza BYOL.

- IamInstanceProfile

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del profilo dell'istanza IAM che consente a Systems Manager di gestire l'istanza.

- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'istanza EC2 che esegue Windows Server 2008 R2, 2012 R2, 2016 o 2019.

- KeepPreUpgradeImageBackUp

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su True, l'automazione non elimina l'AMI creato dall'istanza EC2 prima dell'aggiornamento. Se impostato su True, è necessario eliminare l'AMI. Per impostazione predefinita, l'AMI viene eliminata.

- SubnetId

  Tipo: stringa

  Descrizione: (Obbligatoria) Questa è la sottorete per il processo di aggiornamento e dove risiede l'istanza EC2 di origine. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, Amazon S3 e Microsoft (per scaricare le patch).

- TargetWindowsVersion

  Tipo: stringa

  Descrizione: (obbligatorio) selezionare la versione di Windows di destinazione.

  Impostazione predefinita: 2022

- RebootInstanceBeforeTakingImage

  Tipo: stringa

  Descrizione: (facoltativo) se impostato su True, l'automazione riavvia l'istanza prima di creare un'AMI pre-aggiornamento. Per impostazione predefinita, l'automazione non viene riavviata prima dell'aggiornamento.

AWSEC2-ConfigureSTIG

Le guide tecniche di implementazione della sicurezza (STIGs) sono gli standard di rafforzamento della configurazione creati dalla Defense Information Systems Agency (DISA) per proteggere i sistemi informativi e il software. Per rendere i sistemi conformi STIG agli standard, è necessario installare, configurare e testare una serie di impostazioni di sicurezza.

Amazon EC2 fornisce un runbook Systems ManagerAWSEC2-ConfigureSTIG, che puoi usare per applicare STIG le impostazioni a un'istanza. Questo documento ti aiuta a creare rapidamente immagini conformi agli standard. STIG Il documento STIG Systems Manager analizza eventuali configurazioni errate ed esegue uno script di correzione. Viene inoltre installato InstallRoot dal Dipartimento della Difesa (DoD) su AMIs Windows per installare e aggiornare i certificati DoD e rimuovere i certificati non necessari per mantenere la conformità. STIG Non sono previsti costi aggiuntivi per l'utilizzo del documento STIG Systems Manager.

> **Important**
>
> Con poche eccezioni, i componenti di STIG protezione avanzata scaricati dal documento Systems Manager non installano pacchetti di terze parti. Se sull'istanza sono già installati pacchetti di terze parti e se ci sono pacchetti correlati STIGs EC2 supportati da Amazon per quel pacchetto, questi STIGs vengono applicati.

Questa pagina elenca tutto ciò STIGs che Amazon EC2 supporta e che i componenti di STIG protezione avanzata si applicano alla tua EC2 istanza.

Puoi scegliere quale categoria di STIG conformità applicare.

Livelli di conformità

- Alta (Categoria I)

Il rischio più grave. Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità.

- Medio (categoria II)

  Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità, ma il rischio può essere mitigato.

- Basso (categoria) III

  Include qualsiasi vulnerabilità che degrada le misure di protezione contro la perdita di riservatezza, disponibilità o integrità.

Argomenti

STIGrafforzamento dei download dei componenti

Amazon raggruppa i STIG componenti di protezione avanzata in pacchetti relativi al sistema operativo per ogni versione. I bundle sono file di archivio appropriati per il sistema operativo di destinazione da cui vengono scaricati ed eseguiti. I pacchetti di componenti Linux vengono archiviati come TAR file (estensione.tgz). I pacchetti di componenti Windows vengono archiviati come ZIP file (estensione.zip).

Amazon archivia i pacchetti di componenti nel bucket Image Builder `STIG` S3 di ciascuno. Regione AWS UsaSSL/per comunicare con TLS le risorse. AWS Richiediamo TLS 1.2 e consigliamo TLS 1.3.

I modelli e gli esempi per i percorsi di archiviazione dei componenti e i nomi dei file dei pacchetti sono i seguenti:

Percorso di archiviazione dei componenti

`s3://aws-windows-downloads-<region>/STIG/<bundle file name>`

Variabili del percorso dei componenti

region

Regione AWS (Ogni regione ha il proprio bucket di componenti.)

bundle file name

Il formato è *<os bundle name>*_*<YYYY>*_Q*<quarter>*[_*<release>*].*<file extension>*. Nota che il nome ha caratteri di sottolineatura tra i nodi, non punti.

os bundle name

Il prefisso standard del nome per il pacchetto del sistema operativo è o. `LinuxAWSConfigureSTIG` `AWSConfigureSTIG` Per mantenere la compatibilità con le versioni precedenti, il download per Windows non include un prefisso di piattaforma.

YYYY

L'anno a quattro cifre del rilascio.

quarter

Identifica il trimestre dell'anno: 1, 2, 3 o 4.

release

Numero incrementale che inizia da uno e aumenta di uno per ogni nuova versione. La versione non è inclusa nella prima versione in un trimestre e viene aggiunta solo per le versioni successive.

file extension

Formato di file compresso `tgz` (Linux) o `zip` (Windows).

Esempi di nomi di file di bundle

- `LinuxAWSConfigureSTIG_2023_Q1_2.tgz`
- `AWSConfigureSTIG_2022_Q4.zip`

Impostazioni Windows STIG

Amazon EC2 Windows STIG AMIs e i componenti di protezione avanzata sono progettati per server autonomi e applicano criteri di gruppo locali. STIG-i componenti conformi vengono installati

InstallRoot dal Dipartimento della Difesa (DoD) su Windows AMIs per scaricare, installare e aggiornare i certificati DoD. Inoltre rimuovono i certificati non necessari per mantenere la conformità. STIG Attualmente, Amazon EC2 supporta le STIG linee di base per le seguenti versioni di Windows Server: 2012 R2, 2016, 2019 e 2022.

Questa sezione elenca STIG le impostazioni correnti EC2 supportate da Amazon per la tua infrastruttura Windows, seguite da un registro della cronologia delle versioni.

Puoi applicare STIG impostazioni basse, medie o alte.

Windows STIG Low (categoriaIII)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di WindowsSTIGs, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

- Windows Server 2022 STIG versione 1 versione 1

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- Windows Server STIG 2019 versione 2 versione 5

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- Windows Server 2016 STIG versione 2 versione 5

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060
- Windows Server 2012 R2 MS STIG versione 3 versione 5

  V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 e V-225250

- Microsoft. NETFramework 4.0 STIG Versione 2 Release 2

  Nessuna STIG impostazione si applica a Microsoft. NETFramework per le III vulnerabilità delle categorie.

- Windows Firewall STIG versione 2 versione 1

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008

- Internet STIG Explorer 11 versione 2 versione 3

  V-46477, V-46629 e V-97527

- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)

  V-235727, V-235731, V-235751, V-235752 e V-235765

Windows STIG Medium (categoria II)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di WindowsSTIGs, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

> **Note**
>
> La categoria Windows STIG Medium include tutte le impostazioni di protezione STIG avanzata elencate che si applicano a Windows STIG low (CategoriaIII), oltre alle impostazioni di protezione avanzate EC2 supportate da Amazon per le STIG vulnerabilità di categoria II.

- Windows Server 2022 STIG versione 1 versione 1

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254341, V-254342, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254358, V-254359, V-254367, V-254361, V-254362, V-254364, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-25254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-25254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511 e V-254512

- Windows Server 2019 STIG versione 2 versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-2056651, V-2056652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205684, V-205685, V-205686, V-205686, V-205686 V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-792058 V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828 V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838,

V-205839, V-205840, V-205841, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925 e V-236001

- Windows Server 2016 STIG versione 2 versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 e V-236000

- Windows Server 2012 R2 MS STIG versione 3 versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555 V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532 V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500,

V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461 V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407 V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225348, V-225348, V-225352 V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259 e V-225239

- Microsoft. NETFramework STIG 4.0 Versione 2 Release 2

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-225238

- Windows Firewall STIG versione 2 versione 1

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-241989, V-241990, V-241991, V-241993, V-241998 e V-242003

- Internet STIG Explorer 11 versione 2 versione 3

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

  V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593, V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46615, V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46685, V-46689, V-46691, V-46693,

V-46695, V-46701, V-46705, V-46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46781, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46869, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005, V-47009, V-64711, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169 e V-75171

- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 e V-246736

- Defender STIG versione 2 Release 4 (solo Windows Server 2022)

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 e V-213466

Windows STIG High (Categoria I)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di WindowsSTIGs, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

> **Note**
>
> La categoria Windows STIG High include tutte le impostazioni di protezione STIG avanzata elencate che si applicano alle categorie Windows STIG Medium e Low, oltre alle impostazioni di protezione avanzate EC2 supportate STIG da Amazon per le vulnerabilità di categoria I.

- Windows Server 2022 STIG versione 1 versione 1

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 e V-254500

- Windows Server 2019 versione 2 STIG versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 e V-205919

- Windows Server 2016 STIG versione 2 versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 e V-225079

- Windows Server 2012 R2 MS STIG versione 3 versione 5

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 e V-225274

- Microsoft. NETFramework STIG 4.0 Versione 2 Release 2

  Include tutte le STIG impostazioni di protezione avanzata EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa) per Microsoft. NETStruttura. Non si applicano STIG impostazioni aggiuntive per le vulnerabilità di categoria I.

- Windows Firewall STIG versione 2 versione 1

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-241992, V-241997 e V-242002

- Internet Explorer 11 versione 2 versione 3 STIG

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa) per Internet Explorer 11. Non si applicano STIG impostazioni aggiuntive per le vulnerabilità di categoria I.

- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-235758 e V-235759

- Defender STIG versione 2 Release 4 (solo Windows Server 2022)

  Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

  V-213426, V-213452 e V-213453

Cronologia delle STIG versioni di Windows

Questa sezione registra la cronologia delle versioni dei componenti di Windows per gli aggiornamenti trimestraliSTIG. Per visualizzare le modifiche e le versioni pubblicate per un trimestre, scegli il titolo per espandere le informazioni.

Modifiche al secondo trimestre 2024 - 05/10/2024 (nessuna modifica):

Non sono state apportate modifiche al componente Windows per la versione del secondo STIGS trimestre 2024.

Modifiche al 1° trimestre 2024 - 23/02/2024 (nessuna modifica):

Non sono state apportate modifiche al componente STIGS Windows per la versione del primo trimestre 2024.

Modifiche al quarto trimestre 2023 - 12/07/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIGS Windows per la versione del quarto trimestre 2023.

Modifiche al terzo trimestre 2023 - 10/04/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIGS Windows per la versione del terzo trimestre 2023.

Modifiche al secondo trimestre 2023 - 05/03/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows per la versione del STIGS secondo trimestre 2023.

Modifiche al primo trimestre 2023 - 27/03/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows per la versione del STIGS primo trimestre 2023.

Modifiche al quarto trimestre 2022 - 01/02/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del quarto trimestre 2022 come segue:

STIG-Build-Windows-Low versione 2022.4.0

- Windows Server 2022 versione 1 versione 1 STIG
- Windows Server 2019 STIG versione 2 versione 5
- Windows Server 2016 STIG versione 2 versione 5
- Windows Server 2012 R2 MS STIG versione 3 versione 5
- Microsoft. NETFramework 4.0 STIG Versione 2 Release 2
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 2 versione 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)

STIG-Build-Windows-Medium versione 2022.4.0

- Windows Server 2022 versione 1 versione 1 STIG
- Windows Server 2019 STIG versione 2 versione 5

- Windows Server 2016 STIG versione 2 versione 5
- Windows Server 2012 R2 MS STIG versione 3 versione 5
- Microsoft. NETFramework 4.0 STIG Versione 2 Release 2
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 2 versione 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)
- Defender STIG versione 2 Release 4 (solo Windows Server 2022)

STIG-Build-Windows-High versione 2022.4.0

- Windows Server 2022 versione 1 versione 1 STIG
- Windows Server 2019 STIG versione 2 versione 5
- Windows Server 2016 STIG versione 2 versione 5
- Windows Server 2012 R2 MS STIG versione 3 versione 5
- Microsoft. NETFramework 4.0 STIG Versione 2 Release 2
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 2 versione 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)
- Defender STIG versione 2 Release 4 (solo Windows Server 2022)

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non sono state apportate modifiche al componente STIGS Windows per la versione del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 08/02/2022:

STIGVersioni aggiornate e applicate STIGS per la versione del secondo trimestre 2022.

STIG-Build-Windows-Low versione 1.5.0

- Windows Server 2019 versione 2 versione 4 STIG
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3

- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.5.0

- Windows Server 2019 versione 2 versione 4 STIG
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.5.0

- Windows Server 2019 versione 2 versione 4 STIG
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al 1° trimestre 2022 - 08/02/2022 (nessuna modifica):

Non sono state apportate modifiche al componente Windows per la versione del STIGS primo trimestre 2022.

Modifiche al quarto trimestre 2021 - 20/12/2021:

STIGVersioni aggiornate e applicate STIGS per la versione del quarto trimestre 2021.

STIG-Build-Windows-Low versione 1.5.0

- Windows Server 2019 versione 2 versione 3 STIG
- Windows Server 2016 STIG versione 2 versione 3

- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.5.0

- Windows Server 2019 versione 2 versione 3 STIG
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.5.0

- Windows Server 2019 versione 2 versione 3 STIG
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 2 versione 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al terzo trimestre 2021 - 30/09/2021:

STIGVersioni aggiornate e applicate STIGS per la versione del terzo trimestre 2021.

STIG-Build-Windows-Low versione 1.4.0

- Windows Server 2019 versione 2 versione 2 STIG
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 1 versione 7

- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.4.0

- Windows Server 2019 versione 2 versione 2 STIG
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 1 versione 7
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.4.0

- Windows Server 2019 versione 2 versione 2 STIG
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft. NETFramework 4.0 STIG versione 2 versione 1
- Windows Firewall STIG versione 1 versione 7
- Internet Explorer 11 STIG versione 1 versione 19

STIGImpostazioni Linux

Questa sezione contiene informazioni sulle impostazioni di protezione STIG avanzata di Linux EC2 supportate da Amazon, seguite da un registro della cronologia delle versioni. Se la distribuzione Linux non dispone di impostazioni di STIG protezione avanzate proprie, Amazon EC2 utilizza RHEL le impostazioni. Le impostazioni di STIG protezione avanzata supportate si applicano ad Amazon EC2 Linux AMIs e ai componenti basati sulla distribuzione Linux, come segue:

- Impostazioni di Red Hat Enterprise Linux (RHEL) 7 STIG
  - RHEL7
  - CentOS 7
  - Amazon Linux (2AL2)
- RHEL8 STIG impostazioni
  - RHEL8

  - CentOS 8
  - Amazon Linux 2023 (AL2023)
- RHEL9 STIG impostazioni
  - RHEL9
  - CentOS Stream 9

Linux STIG Low (CategoriaIII)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

RHEL7 STIG Versione 3 Release 14

- RHEL7/CentOS 7/ AL2

  V-204452, V-204576 e V-204605

RHEL8 Versione STIG 1 Release 14

- RHEL8/CentOS 8/AL 2023

  V-230241, V-244527, V-230269, V-230270, V-230285, V-230253, V-230346, V-230381, V-230395, V-230468, V-230469, V-230491, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 e V-230281

RHEL9 STIG Versione 1 Release 3

- RHEL9/CentOS Stream 9

  V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947, V-258037, V-258067, V-258069, V-258076 e V-258173

STIGUbuntu 18.04 versione 2 versione 14

V-219172, V-219173, V-219174, V-219175, V-219210, V-219164, V-219165, V-219178, V-219180, V-219301, V-219163, V-219332, V-219327 e V-219333

Ubuntu STIG 20.04 versione 1 versione 12

V-238202, V-238234, V-238235, V-238237, V-238323, V-238373, V-238221, V-238222, V-238223, V-238224, V-238226, V-238362, V-238357 e V-238308

STIGUbuntu 22.04 versione 1 versione 1

V-260472, V-260476, V-260479, V-260480, V-260481, V-260520, V-260521, V-260549, V-260550, V-260551, V-260552, V-260581 e V-260596

STIGLinux Medium (categoria II)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

> **Note**
>
> La categoria Linux STIG Medium include tutte le impostazioni di protezione STIG avanzata elencate che si applicano STIG a Linux Low (CategoryIII), oltre alle impostazioni di protezione avanzate EC2 supportate STIG da Amazon per le vulnerabilità di categoria II.

RHEL7 STIG Versione 3 Release 14

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL7/CentOS 7/ AL2

V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204516, V-204516, V-204511, V-204512, V-204514, V-204515, V-204516, V-204516, V-204511, V-204512, V-204514, V-204515, V-204516, V-204516, V-204516,, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204579, V-204631, V-204633 e V-256970

RHEL8 Versione 1 STIG Release 14

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL8/CentOS 8/AL 2023

V-230257, V-230258, V-230259, V-230550, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-230228, V-230298, V-230387, V-230231, V-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230548, V-230548 549, V-244550, V-244551, V-244552, V-244553, V-244554, V250317, V-2301718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230368, V-230369, V-230375, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-2307, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230334, V-230336, V-230338, V-230340, V-230342, V-230344, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230240, V-230282, V250315, V-230316,

V-230255, V-230277, V-230278, 230348, V-230353, V-230386, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, -230483, V-244542, V-230503, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-23043, V-251711, V-230238, V-230239, V-230273, V-230275, V-230478, V-230478, V-230238, V-230273, V-230275, V-230478, V-230238, V-230273, V-230275, V-230478, V-230238, V-230273, V-230275, V-230478, V-230238, V-230273, V-230275, V-230478, V-230238, V-230273 488, V-230489, V-230559, V-230560, V-230561, V-237640 e V-256974

RHEL9 STIG Versione 1 Release 3

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL9/CentOS Stream 9

V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257804, V-257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813, V-257814, V-257815, V-257816, V-257817, V-257818, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257885, V-257886, V-257887, V-257888, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257924, V-257925, V-257926, V-257927, V-257928, V-257929, V-257930, V-257931, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257949, V-257951, V-257952, V-257953, V-257954, V-257957, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257985, V-257987, V-257988, V-257989, V-257991, V-257992, V-257993, V-257994,

V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002 258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258036, V-258038, V-258040, V-258041, V-258043, V-258049, V-258052, V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258074, V-258075, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258120, V-258122, V-258123, V-258124, V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258134, V-258137, V-258140, V-258141, V-258142, V-258144, V-258145, V-258146, V-258147, V-258148, V-258150, V-258151, V-258152, V-258153, V-258154, V-258156, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258175, V-258175, V-258176, V-258177, V-258178, V-258179, V-258181, V-258182, V-258183, V-258183, V-258183, V-184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258208, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258215, V-258215, V-258215, V-258215, V-258214, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-2582258216, V-258217, V-258218, V-258219, V-258220, V-258221, V-258222, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258229, V-258232, V-258233, V-258234, V-258237, V-258239 e V-258240

Ubuntu 18.04 STIG Versione 2 Release 14

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219303, V-219326, V-219328, V-219328, V-219328, V-219209, V-219303, V-219326, V-219328, V-219328, V-219208, V-219209, V-219303, V-219326, V-219328, V-219328, V-219208, V-219209, V-219303, V-219326, V-219328 V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219221 V-19222, V-219223, V-219224, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243 19244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219277, V-219274 279, V-219281, V-219287,

V-219291, V-219297, V-219298, V-219299, V-219300, V-219309, V-219310, V-219311, V-219312, V-233779, V-233780, V-255906, V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219155, V-219156, V-219160, V-219306, V-219149, V-219166, V-219176, V-219339, V-219331, V-219337 e V-219335

Ubuntu 20.04 STIG Versione 1 Release 12

V-238205, V-238207, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-251505, V-238360, V-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238358, V-238356, V-238359, V-238370 e V-238334

Ubuntu 22.04 STIG Versione 1 Release 1

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-260471, V-260473, V-260474, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260491, V-260492, V-260493, V-260494, V-260495, V-260496, V-260497, V-260497, V-260497 498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260514, V-260516, V-260522, V-260527, V-260528, V-260530, V-260531, V-260531, V-260522 32, V-260533, V-260534, V-260542, V-260543, V-260545, V-260546, V-260547, V-260553, V-260554, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565 V-260566, V-260567, V-260568, V-260572, V-260573, V-260574, V-260576, V-260582, V-260584, V-260586, V-260588, V-260589, V-260590, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648 e V-260649

STIGLinux High (Categoria I)

L'elenco seguente contiene STIG le impostazioni EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di STIG protezione avanzata potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consultate la STIGsDocument Library. Per informazioni su come visualizzare l'elenco completo, vedere Strumenti STIG di visualizzazione.

> **Note**
>
> La categoria Linux STIG High include tutte le impostazioni di protezione avanzate STIG elencate che si applicano alle categorie Linux STIG Medium e Low, oltre alle impostazioni di protezione avanzate STIG EC2 supportate da Amazon per le vulnerabilità di categoria I.

RHEL7 STIG Versione 3 Release 14

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

- RHEL7/CentOS 7/ AL2

  V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620 e V-204621

RHELSTIG8 Versione 1 Release 14

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

- RHEL8/CentOS 8/AL 2023

  V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533 e V-230558

RHEL9 Versione 1 Release 3 STIG

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

- RHEL9/CentOS Stream 9

  V-257784, V-257785, V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-257984, V-257986, V-258059, V-258078, V-258094 e V-258235

Ubuntu STIG 18.04 versione 2 versione 14

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316 e V-251507

Ubuntu STIG 20.04 versione 1 versione 12

V-238218, V-238219, V-238201, V-238326, V-238327, V-238380 e V-251504

Ubuntu STIG 22.04 Versione 1 Release 1

Include tutte le impostazioni di STIG rafforzamento EC2 supportate da Amazon per le vulnerabilità di categoria II e III (media e bassa), oltre a:

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529, V-260570, V-260571 e V-260579

STIGCronologia delle versioni di Linux

Questa sezione registra la cronologia delle versioni dei componenti Linux per gli aggiornamenti trimestraliSTIG. Per visualizzare le modifiche e le versioni pubblicate per un trimestre, scegli il titolo per espandere le informazioni.

Modifiche al secondo trimestre 2024 - 05/10/2024:

STIGVersioni aggiornate e applicate STIGS per la versione del secondo trimestre 2024. È stato inoltre aggiunto il supporto per RHEL 9, CentOS Stream 9 e Ubuntu 22.04, come segue:

STIG-Build-Linux-Low versione 2024.2.x

- RHEL7 STIG Versione 3 Release 14
- RHEL8 STIG Versione 1 Release 14
- RHEL9 STIG Versione 1 Release 3
- Ubuntu 18.04 STIG Versione 2 Release 14

- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

STIG-Build-Linux-Medium versione 2024.2.x

- RHEL7 STIG Versione 3 Release 14
- RHEL8 STIG Versione 1 Release 14
- RHEL9 STIG Versione 1 Release 3
- Ubuntu 18.04 STIG Versione 2 Release 14
- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

STIG-Build-Linux-High versione 2024.2.x

- RHEL7 STIG Versione 3 Release 14
- RHEL8 STIG Versione 1 Release 14
- RHEL9 STIG Versione 1 Release 3
- Ubuntu 18.04 STIG Versione 2 Release 14
- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

Modifiche al primo trimestre 2024 - 02/06/2024:

STIGVersioni aggiornate e applicate STIGS per la versione del primo trimestre 2024 come segue:

STIG-Build-Linux-Low versione 2024.1.x

- RHEL7 STIG Versione 3 Release 14
- RHEL8 STIG Versione 1 Release 13
- Ubuntu 18.04 STIG Versione 2 Release 13
- Ubuntu 20.04 STIG versione 1 versione 11

STIG-Build-Linux-Medium versione 2024.1.x

- RHEL7 STIG Versione 3 Release 14

- RHEL8 STIG Versione 1 Release 13
- Ubuntu 18.04 STIG Versione 2 Release 13
- Ubuntu 20.04 STIG versione 1 versione 11

STIG-Build-Linux-High versione 2024.1.x

- RHEL7 STIG Versione 3 Release 14
- RHEL8 STIG Versione 1 Release 13
- Ubuntu 18.04 STIG Versione 2 Release 13
- Ubuntu 20.04 STIG versione 1 versione 11

Modifiche al quarto trimestre 2023 - 12/07/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del quarto trimestre 2023 come segue:

STIG-Build-Linux-Low versione 2023.4.x

- RHEL7 STIG Versione 3 Release 13
- RHEL8 STIG Versione 1 Release 12
- Ubuntu 18.04 STIG Versione 2 Release 12
- Ubuntu 20.04 STIG versione 1 versione 10

STIG-Build-Linux-Medium versione 2023.4.x

- RHEL7 STIG Versione 3 Release 13
- RHEL8 STIG Versione 1 Release 12
- Ubuntu 18.04 STIG Versione 2 Release 12
- Ubuntu 20.04 STIG versione 1 versione 10

STIG-Build-Linux-High versione 2023.4.x

- RHEL7 STIG Versione 3 Release 13
- RHEL8 STIG Versione 1 Release 12
- Ubuntu 18.04 STIG Versione 2 Release 12
- Ubuntu 20.04 STIG versione 1 versione 10

Modifiche al terzo trimestre 2023 - 10/04/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del terzo trimestre 2023 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 12
- RHEL8 STIG Versione 1 Release 11
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 9

Linux STIG Medium (categoria II)

- RHEL7 STIG Versione 3 Release 12
- RHEL8 STIG Versione 1 Release 11
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 9

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 12
- RHEL8 STIG Versione 1 Release 11
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 9

Modifiche al secondo trimestre 2023 - 05/03/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del secondo trimestre 2023 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 11
- RHEL8 STIG Versione 1 Release 10
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 8

Linux STIG Medium (categoria II)

- RHEL7 STIG Versione 3 Release 11
- RHEL8 STIG Versione 1 Release 10
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 8

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 11
- RHEL8 STIG Versione 1 Release 10
- Ubuntu 18.04 STIG Versione 2 Release 11
- Ubuntu 20.04 STIG versione 1 versione 8

Modifiche al primo trimestre 2023 - 27/03/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del primo trimestre 2023 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 10
- RHEL8 STIG Versione 1 Release 9
- Ubuntu 18.04 STIG Versione 2 Release 10
- Ubuntu 20.04 STIG versione 1 versione 7

Linux STIG Medium (categoria II)

- RHEL7 STIG Versione 3 Release 10
- RHEL8 STIG Versione 1 Release 9
- Ubuntu 18.04 STIG Versione 2 Release 10
- Ubuntu 20.04 STIG versione 1 versione 7

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 10

- RHEL8 STIG Versione 1 Release 9
- Ubuntu 18.04 STIG Versione 2 Release 10
- Ubuntu 20.04 STIG versione 1 versione 7

Modifiche al quarto trimestre 2022 - 02/01/2023:

STIGVersioni aggiornate e applicate STIGS per la versione del quarto trimestre 2022 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 9
- RHEL8 STIG Versione 1 Release 8
- Ubuntu 18.04 STIG Versione 2 Release 9
- Ubuntu 20.04 STIG versione 1 versione 6

Linux STIG Medium (categoria II)

- RHEL7 STIG Versione 3 Release 9
- RHEL8 STIG Versione 1 Release 8
- Ubuntu 18.04 STIG Versione 2 Release 9
- Ubuntu 20.04 STIG versione 1 versione 6

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 9
- RHEL8 STIG Versione 1 Release 8
- Ubuntu 18.04 STIG Versione 2 Release 9
- Ubuntu 20.04 STIG versione 1 versione 6

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non sono state apportate modifiche al componente STIGS Linux per la versione del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 08/02/2022:

È stato introdotto il supporto per Ubuntu, STIG versioni aggiornate e richiesto STIGS per la versione del secondo trimestre 2022 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 7
- RHEL8 STIG Versione 1 Release 6
- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Linux STIG Medium (categoria II)

- RHEL7 STIG Versione 3 Release 7
- RHEL8 STIG Versione 1 Release 6
- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 7
- RHEL8 STIG Versione 1 Release 6
- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Modifiche al 1° trimestre 2022 - 26/04/2022:

Rifattorizzato per includere un migliore supporto per i contenitori. Ha combinato lo AL2 script precedente con RHEL 7. STIGVersioni aggiornate e applicate STIGS per la versione del primo trimestre 2022 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 6
- RHEL8 STIG Versione 1 Release 5

Linux STIG Medium (Categoria II)

- RHEL7 STIG Versione 3 Release 6
- RHEL8 STIG Versione 1 Release 5

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 6
- RHEL8 STIG Versione 1 Release 5

Modifiche al quarto trimestre 2021 - 20/12/2021:

STIGVersioni aggiornate e applicate STIGS per la versione del quarto trimestre 2021 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 5
- RHEL8 STIG Versione 1 Release 4

Linux STIG Medium (Categoria II)

- RHEL7 STIG Versione 3 Release 5
- RHEL8 STIG Versione 1 Release 4

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 5
- RHEL8 STIG Versione 1 Release 4

Modifiche al terzo trimestre 2021 - 30/09/2021:

STIGVersioni aggiornate e applicate STIGS per la versione del terzo trimestre 2021 come segue:

Linux STIG Low (categoriaIII)

- RHEL7 STIG Versione 3 Release 4
- RHEL8 STIG Versione 1 Release 3

Linux STIG Medium (Categoria II)

- RHEL7 STIG Versione 3 Release 4
- RHEL8 STIG Versione 1 Release 3

Linux STIG High (Categoria I)

- RHEL7 STIG Versione 3 Release 4
- RHEL8 STIG Versione 1 Release 3

AWSEC2-PatchLoadBalancerInstance

Descrizione

Aggiorna e applica patch a una versione secondaria di un'istanza Amazon EC2 (Windows o Linux) collegata a qualsiasi sistema di bilanciamento del carico (classico, ALB o NLB). Il tempo di esaurimento della connessione predefinito viene applicato prima che l'istanza venga patchata. È possibile ignorare il tempo di attesa inserendo il tempo di scarico personalizzato in minuti (1-59) per il ConnectionDrainTimeparametro.

Il flusso di lavoro di automazione è il seguente:

1. Il sistema di bilanciamento del carico o il gruppo target a cui è collegata l'istanza viene determinata e l'istanza viene verificata come integra.
2. L'istanza viene rimossa dal sistema di bilanciamento del carico o dal gruppo di destinazione.
3. L'automazione attende il periodo di tempo specificato per il tempo di esaurimento della connessione.
4. L'RunPatchBaselineautomazione AWS viene chiamata per applicare una patch all'istanza.
5. L'istanza viene ricollegata al sistema di bilanciamento del carico o al gruppo di destinazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Prerequisiti

- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta Lavorare con SSM Agent su istanze EC2 per Windows Server.

Parametri

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza da applicare alla patch associata a un sistema di bilanciamento del carico (classico, ALB o NLB).
- ConnectionDrainTime

  Tipo: String

  Descrizione: (Facoltativo) Il tempo di esaurimento della connessione del load balancer, in minuti (1-). 59

AWSEC2-SQLServerDBRestore

Descrizione

Il `AWSEC2-SQLServerDBRestore` runbook ripristina i backup del database Microsoft SQL Server archiviati in Amazon S3 su SQL Server 2017 in esecuzione su un'istanza Linux di Amazon Elastic Compute Cloud (EC2). Puoi fornire un'istanza EC2 personale che esegue SQL Server 2017 Linux. Se non viene fornita un'istanza EC2, l'automazione avvia e configura una nuova istanza di Ubuntu 16.04 EC2 con SQL Server 2017. L'automazione supporta il ripristino dei backup dei log transazionali, differenziali e completi. Questa automazione accetta più file di backup del database e ripristina automaticamente il backup valido più recente di ogni database nei file forniti.

Per automatizzare sia il backup che il ripristino di un database SQL Server locale su un'istanza EC2 che esegue SQL Server 2017 Linux, puoi utilizzare lo script -signed. AWS PowerShell `MigrateSQLServerToEC2Linux`

> **Important**
>
> Questo runbook reimposta la password utente dell'amministratore del server SQL Server (SA) ogni volta che viene eseguita l'automazione. Una volta completata l'automazione, è necessario impostare nuovamente la propria password utente SA prima di connettersi all'istanza di SQL Server.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Prerequisiti

Per eseguire questa automazione, è necessario soddisfare i seguenti prerequisiti:

- L'utente o il ruolo IAM che esegue questa automazione deve avere una policy in linea allegata alle autorizzazioni descritte in. Autorizzazioni IAM richieste
- Se fornisci la tua istanza EC2:
  - L'istanza EC2 fornita deve essere un'istanza Linux su cui è in esecuzione Microsoft SQL Server 2017.
  - L'istanza EC2 fornita deve essere configurata con un profilo di istanza AWS Identity and Access Management (IAM) a cui sia allegata la policy `AmazonSSMManagedInstanceCore` gestita. Per ulteriori informazioni, consulta Creazione di un profilo dell'istanza IAM per Systems Manager.
  - L'agente SSM deve essere installato sull'istanza EC2. Per ulteriori informazioni, vedere Installazione e configurazione di SSM Agent su istanze EC2 per Linux.
  - L'istanza EC2 deve disporre di spazio libero su disco sufficiente per scaricare e ripristinare i backup di SQL Server.

Restrizioni

Questa automazione non supporta il ripristino in SQL Server in esecuzione in istanze EC2 per Windows Server. Questa automazione ripristina solo i backup del database compatibili con SQL Server Linux 2017. Per ulteriori informazioni, consulta Edizioni e funzionalità supportate di SQL Server 2017 in Linux.

Parametri

Questa automazione presenta i seguenti parametri:

- DatabaseNames

  Tipo: String

  Descrizione: (facoltativo) elenco separato da virgole con i nomi dei database da ripristinare.

- DataDirectorySize

  Tipo: String

  Descrizione: (facoltativo) le dimensioni del volume desiderate (GiB) della directory dei dati di SQL Server per la nuova istanza EC2.

  Valore predefinito: 100

- KeyPair

  Tipo: String

  Descrizione: (facoltativo) coppia di chiavi da utilizzare per creare la nuova istanza EC2.

- IamInstanceProfileName

  Tipo: String

  Descrizione: (Facoltativo) Il profilo dell'istanza IAM da collegare alla nuova istanza EC2. Al profilo dell'istanza IAM deve essere allegata la policy `AmazonSSMManagedInstanceCore` gestita.

- InstanceId

  Tipo: String

Descrizione: (facoltativo) l'istanza che esegue SQL Server 2017 in Linux. Se non InstanceId viene fornito alcun valore, l'automazione avvia una nuova istanza EC2 utilizzando il codice InstanceType SQL ServerEdition fornito.

- InstanceType

  Tipo: String

  Descrizione: (facoltativo) il tipo dell'istanza EC2 da avviare.

- iS3 PresignedUrl

  Tipo: String

  Descrizione: (Facoltativo) Se S3Input è un URL S3 prefirmato, indicare. `yes`

  Valore predefinito: no

  Valori validi: sì | no

- LogDirectorySize

  Tipo: String

  Descrizione: (facoltativo) le dimensioni del volume desiderate (GiB) della directory dei log di SQL Server per la nuova istanza EC2.

  Valore predefinito: 100

- Ingresso S3

  Tipo: String

  Descrizione: (obbligatorio) nome del bucket S3, elenco separato da virgole delle chiavi oggetto S3 o elenco separato da virgole degli URL S3 prefirmati contenenti i file di backup SQL da ripristinare.

- SQL ServerEdition

  Tipo: String

  Descrizione: (facoltativo) l'edizione di SQL Server 2017 da installare nell'istanza EC2 appena creata.

  Valori validi: Standard | Enterprise | Web | Express

- SubnetId

  Tipo: String

  Descrizione: (facoltativo) la sottorete in cui avviare la nuova istanza EC2. La sottorete deve avere una connettività in uscita ai servizi AWS. Se non SubnetId viene fornito un valore per, l'automazione utilizza la sottorete predefinita.

- TempDbDirectorySize

  Tipo: String

  Descrizione: (facoltativo) le dimensioni del volume desiderate (GiB) della directory TempDB di SQL Server per la nuova istanza EC2.

  Valore predefinito: 100

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands",
                "ssm:SendCommand",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::ACCOUNTID:role/ROLENAME"
        }
    ]
}
```

Fasi del documento

Per utilizzare questa automazione, segui i passaggi che si applicano al tuo tipo di istanza:

Per le nuove istanze EC2:

1. `aws:executeAwsApi`- Recupera l'ID AMI per SQL Server 2017 su Ubuntu 16.04.
2. `aws:runInstances`- Avvia una nuova istanza EC2 per Linux.
3. `aws:waitForAwsResourceProperty`- Attendi che l'istanza EC2 appena creata sia pronta.
4. `aws:executeAwsApi`- Riavviare l'istanza se l'istanza non è pronta.
5. `aws:assertAwsResourceProperty`- Verificare che SSM Agent sia installato.
6. `aws:runCommand`- Esegui lo script di ripristino di SQL Server inPowerShell.

Per le istanze EC2 esistenti:

1. `aws:waitForAwsResourceProperty`- Verificare che l'istanza EC2 sia pronta.
2. `aws:executeAwsApi`- Riavviare l'istanza se l'istanza non è pronta.
3. `aws:assertAwsResourceProperty`- Verificare che SSM Agent sia installato.
4. `aws:runCommand`- Esegui lo script di ripristino di SQL Server inPowerShell.

Output

getInstance. InstanceId

restoreToNewIstanza.Output

restoreToExistingIstanza.Output

AWSSupport-ActivateWindowsWithAmazonLicense

Descrizione

Il AWSSupport-ActivateWindowsWithAmazonLicense runbook attiva un'istanza Amazon Elastic Compute Cloud (Amazon EC2) Windows Server con una licenza fornita da Amazon. L'automazione verifica e configura le impostazioni del sistema operativo del servizio di gestione delle chiavi richieste e i tentativi di attivazione. Ciò include i percorsi del sistema operativo verso i server di gestione delle chiavi di Amazon e le impostazioni del sistema operativo del servizio di gestione delle chiavi. Impostando il parametro AllowOffline su true si consente all'automazione di indirizzare correttamente le istanze non gestite da AWS Systems Manager, ma richiede un arresto e l'avvio dell'istanza.

> **Note**
>
> Questo runbook non può essere utilizzato su istanze del modello Bring Your Own License (BYOL). Windows Server Per informazioni su come utilizzare la licenza, consulta la pagina sulle licenze Microsoft su AWS.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AllowOffline

  Tipo: String

  Valori validi: true | false

Di default: false

Descrizione: (Facoltativo) Impostalo su `true` se consenti una correzione dell'attivazione di Windows offline nel caso in cui la risoluzione dei problemi online fallisca o se l'istanza fornita non è un'istanza gestita.

> **Important**
>
> Nota: il metodo offline richiede l'arresto e il successivo avvio dell'istanza EC2 specificata. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ForceActivation

  Tipo: String

  Valori validi: true | false

  Di default: false

  Descrizione: (Facoltativo) Impostalo su `true` se desideri procedere anche se Windows è già attivato.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza EC2 gestita per Windows Server.

- SubnetId

  Tipo: String

Impostazione predefinita: CreateNew VPC

Descrizione: (facoltativo) solo offline - ID sottorete dell'istanza EC2Rescue utilizzata per eseguire la risoluzione dei problemi offline. `SelectedInstanceSubnet`Utilizzalo per utilizzare la stessa sottorete della tua istanza o `CreateNewVPC` per creare un nuovo VPC. IMPORTANTE: la sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Consigliamo che l'istanza EC2 che riceve il comando abbia un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. È necessario disporre almeno di ssm: StartAutomationExecution e ssm: SendCommand per eseguire l'automazione e inviare il comando all'istanza, oltre a ssm: GetAutomationExecution per poter leggere l'output dell'automazione. Per la correzione offline, consulta le autorizzazioni necessarie per. `AWSSupport-StartEC2RescueWorkflow`

Fasi del documento

1. `aws:assertAwsResourceProperty`- Verifica che la piattaforma dell'istanza fornita sia Windows.
2. `aws:assertAwsResourceProperty`- Conferma che l'istanza fornita sia un'istanza gestita:
   a. (Correzione di attivazione online) Se l'istanza di input è un'istanza gestita, `aws:runCommand` esegui per eseguire lo PowerShell script per tentare di correggere l'attivazione di Windows.
   b. (Correzione dell'attivazione offline) Se l'istanza di input non è un'istanza gestita:
      i. `aws:assertAwsResourceProperty`- Verifica che la `AllowOffline` bandiera sia impostata su. `true` In tal caso, viene avviata la correzione offline; in caso contrario, l'automazione termina.
      ii. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con lo script di correzione offline per l'attivazione di Windows. Lo script utilizza EC2Config o EC2Launch, a seconda della versione del sistema operativo.
      iii. `aws:executeAwsApi`- Leggi il risultato di`AWSSupport-StartEC2RescueWorkflow`.

Output

activateWindows.Output

getActivateWindowsOfflineResult.Uscita

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descrizione

Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook analizza la connettività da un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o da un'interfaccia di rete elastica a un endpoint. AWS servizio Il protocollo IPv6 non è supportato. Il runbook utilizza il valore specificato per il `ServiceEndpoint` parametro per analizzare la connettività a un endpoint. Se non riesci a trovare un AWS PrivateLink endpoint nel tuo VPC, il runbook utilizza un indirizzo IP pubblico per il servizio corrente. Regione AWS Questa automazione utilizza Reachability Analyzer di Amazon Virtual Private Cloud. Per ulteriori informazioni, consulta Cos'è Reachability Analyzer? , in Reachability Analyzer.

Questa automazione verifica quanto segue:

- Verifica se il tuo cloud privato virtuale (VPC) è configurato per utilizzare il server DNS fornito da Amazon.
- Verifica se esiste un AWS PrivateLink endpoint nel VPC per quello AWS servizio specificato. Se viene trovato un endpoint, l'automazione verifica che l'`privateDnsattributo` sia attivato.
- Verifica se l' AWS PrivateLink endpoint utilizza la policy predefinita per gli endpoint.

Considerazioni

- Ti viene addebitato un costo per ogni analisi eseguita tra un'origine e una destinazione. Per ulteriori informazioni, consulta la pagina dei Prezzi di Amazon VPC.
- Durante l'automazione, vengono creati un percorso di analisi della rete e un'analisi delle informazioni di rete. Se l'automazione viene completata correttamente, il runbook elimina queste risorse. Se la fase di pulizia fallisce, il percorso di network Insights non viene eliminato dal runbook e sarà necessario eliminarlo manualmente. Se non elimini manualmente il percorso di network Insights, esso continua a essere conteggiato ai fini della quota prevista per il tuo. Account AWSPer ulteriori informazioni sulle quote per Reachability Analyzer, vedere Quotas for Reachability Analyzer in Reachability Analyzer.

- Le configurazioni a livello di sistema operativo come l'uso di un proxy, un resolver DNS locale o un file hosts possono influire sulla connettività anche se il Reachability Analyzer ritorna. `PASS`
- Esamina la valutazione di tutti i controlli eseguiti dal Reachability Analyzer. Se uno qualsiasi dei controlli restituisce uno stato di`FAIL`, ciò potrebbe influire sulla connettività anche se il controllo di raggiungibilità complessivo restituisce uno stato di. `PASS`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  ▪Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Origine

  ▪Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 o dell'interfaccia di rete da cui desideri analizzare la raggiungibilità.
- ServiceEndpoint

  ▪Tipo: stringa

Descrizione: (Obbligatorio) Il nome host dell'endpoint del servizio su cui desideri analizzare la raggiungibilità.

- RetainVpcReachabilityAnalysis

  - Tipo: stringa

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Determina se il percorso di analisi della rete e la relativa analisi creata vengono conservati. Per impostazione predefinita, le risorse utilizzate per analizzare la raggiungibilità vengono eliminate dopo un'analisi riuscita. Se scegli di conservare l'analisi, il runbook non elimina l'analisi e puoi visualizzarla nella console Amazon VPC. Nell'output dell'automazione è disponibile un collegamento alla console.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateNetworkInsightsPath`
- `ec2:DeleteNetworkInsightsAnalysis`
- `ec2:DeleteNetworkInsightsPath`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeManagedPrefixLists`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:DescribeNetworkInterfaces`

- ec2:DescribePrefixLists
- ec2:DescribeRegions
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTransitGatewayAttachments
- ec2:DescribeTransitGatewayPeeringAttachments
- ec2:DescribeTransitGatewayConnects
- ec2:DescribeTransitGatewayRouteTables
- ec2:DescribeTransitGateways
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetManagedPrefixListEntries
- ec2:GetTransitGatewayRouteTablePropagations
- ec2:SearchTransitGatewayRoutes
- ec2:StartNetworkInsightsAnalysis
- elasticloadbalancing:DescribeListeners
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeRules
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:DescribeTargetGroups

- elasticloadbalancing:DescribeTargetHealth
- tiros:CreateQuery
- tiros:GetQueryAnswer
- tiros:GetQueryExplanation

Fasi del documento

1. aws:executeScript: convalida l'endpoint del servizio tentando di risolvere il nome host.
2. aws:executeScript: raccoglie dettagli sul VPC e sulla sottorete.
3. aws:executeScript: valuta la configurazione DNS del VPC.
4. aws:executeScript: valuta i controlli degli endpoint VPC.
5. aws:executeScript: individua un gateway Internet per la connessione all'endpoint del servizio pubblico.
6. aws:executeScript: determina la destinazione da utilizzare per l'analisi della raggiungibilità.
7. aws:executeScript: analizza la raggiungibilità dalla sorgente all'endpoint utilizzando Reachability Analyzer e pulisce le risorse se l'analisi ha esito positivo.
8. aws:executeScript: genera un rapporto di valutazione della raggiungibilità.
9. aws:executeScript: genera l'output in JSON.

Output

- generateReport.EvalReport- I risultati dei controlli eseguiti dall'automazione in formato testo.
- generateJsonOutput.Output- Una versione minimale dei risultati in formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descrizione

Il AWSPremiumSupport-ChangeInstanceTypeIntelToAMD runbook automatizza le migrazioni dalle istanze Amazon Elastic Compute Cloud (Amazon EC2) con tecnologia Intel ai tipi di istanze equivalenti basati su AMD. Questo runbook supporta istanze generiche (M), espandibili generiche (T), ottimizzate per l'elaborazione (C) e ottimizzate per la memoria (R) basate sul sistema Nitro. Questo runbook può essere utilizzato su istanze che non sono gestite da Systems Manager.

Per ridurre il rischio potenziale di perdita e downtime dei dati, il runbook verifica il comportamento di arresto dell'istanza, se l'istanza appartiene a un gruppo Amazon EC2 Auto Scaling, lo stato dell'istanza e se il tipo di istanza equivalente con tecnologia AMD è disponibile nella stessa zona di disponibilità. Per impostazione predefinita, questo runbook non modificherà il tipo di istanza se i volumi dell'archivio delle istanze sono collegati o se l'istanza fa parte di uno AWS CloudFormation stack. Se desideri modificare questo comportamento, specifica `yes` uno dei `AllowCloudFormationInstances` parametri `AllowInstanceStoreInstances` and.

> **Important**
>
> L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, consulta Confronta AWS Support i piani.

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook.
- La modifica del tipo di istanza richiede che il runbook interrompa l'istanza. Quando un'istanza viene interrotta, tutti i dati memorizzati nella RAM o nei volumi dell'archivio delle istanze vengono persi e l'indirizzo IPv4 pubblico automatico viene rilasciato. Per ulteriori informazioni, consulta Arrestare e avviare un'istanza.
- Se non specificate un valore per il `TargetInstanceType` parametro, il runbook tenta di identificare l'istanza AMD equivalente in termini di CPU virtuali e memoria all'interno della stessa famiglia di istanze. Il runbook termina se non è in grado di identificare un tipo di istanza AMD equivalente.
- Utilizzando l'`DryRun`opzione, è possibile acquisire il tipo di istanza AMD equivalente e convalidare i requisiti senza modificare effettivamente il tipo di istanza.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Accettare

  Tipo: String

  Descrizione: (Obbligatorio) Entra `yes` per confermare che l'istanza di destinazione verrà interrotta se è in esecuzione.
- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 di cui desideri modificare il tipo.
- TargetInstanceType

  Tipo: String

  Predefinito: automatico

  Descrizione: (Facoltativo) Il tipo di istanza AMD in cui desideri modificare l'istanza. Il `automatic` valore predefinito utilizza il tipo di istanza equivalente in termini di CPU e memoria virtuali. Ad esempio, un m5.large verrebbe modificato in m5a.large.
- AllowInstanceStoreInstances

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

Descrizione: (Facoltativo) Se si specifica`yes`, il runbook viene eseguito su istanze a cui sono collegati i volumi dell'archivio delle istanze.

- AllowCloudFormationInstances

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se impostato su`yes`, il runbook viene eseguito su istanze che fanno parte di uno AWS CloudFormation stack.

- AllowCrossGeneration

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se impostato su`yes`, il runbook tenta di trovare il tipo di istanza AMD equivalente più recente all'interno della stessa famiglia di istanze.

- DryRun

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se impostato su`yes`, il runbook restituisce il tipo di istanza AMD equivalente e convalida i requisiti di migrazione senza apportare modifiche al tipo di istanza.

- SleepWait

  Tipo: String

  Predefinito: PT3S

  Descrizione: (Facoltativo) Il tempo che il runbook deve attendere prima di avviare una nuova automazione. Il valore fornito per questo parametro deve corrispondere allo standard ISO 8601.

Per ulteriori informazioni sulla creazione di stringhe ISO 8601, vedere Formattazione delle stringhe di data e ora per Systems Manager.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:GetInstanceTypesFromInstanceRequirements`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeTags`
- `ec2:ModifyInstanceAttribute`
- `ec2:StartInstances`
- `ec2:StopInstances`

Fasi del documento

1. `aws:assertAwsResourceProperty`: conferma che lo stato dell'istanza Amazon EC2 di destinazione è`running`, `pending`o`stopped`, `stopping`. Altrimenti, l'automazione termina.
2. `aws:executeAwsApi`: raccoglie le proprietà dall'istanza Amazon EC2 di destinazione.
3. `aws:branch`: ramifica l'automazione in base allo stato dell'istanza Amazon EC2.
   a. In caso contrario `stopped`, `stopping`, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino all'arresto completo dell'istanza Amazon EC2.
   b. In caso `running` `pending` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino a quando l'istanza Amazon EC2 non supera i controlli di stato.

4. `aws:assertAwsResourceProperty`: conferma che l'istanza Amazon EC2 non fa parte di un gruppo Auto Scaling controllando se il `aws:autoscaling:groupName` tag è applicato.
5. `aws:executeAwsApi`: raccoglie le proprietà del tipo di istanza corrente per trovare il tipo di istanza AMD equivalente.
6. `aws:assertAwsResourceProperty`: conferma che un codice Marketplace AWS prodotto non è associato all'istanza Amazon EC2. Alcuni prodotti non sono disponibili per tutti i tipi di istanze.
7. `aws:branch`: ramifica l'automazione a seconda che tu voglia che l'automazione controlli se l'istanza Amazon EC2 fa parte di uno stack AWS CloudFormation
   a. Se il `aws:cloudformation:stack-name` tag viene applicato all'istanza, l'automazione viene eseguita `aws:assertAwsResourceProperty` per confermare che l'istanza non fa parte di uno AWS CloudFormation stack.
8. `aws:branch`: ramifica l'automazione in base al fatto che il tipo di volume principale dell'istanza sia Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: conferma che il comportamento di chiusura dell'istanza è `stop` e non lo è. `terminate`
10. `aws:executeScript`: conferma che esiste una sola automazione di questo runbook destinata all'istanza corrente. Se è già in corso un'altra automazione destinata alla stessa istanza, restituisce un errore e termina.
11. `aws:executeAwsApi`: restituisce un elenco dei tipi di istanze AMD con la stessa quantità di memoria e vCPU.
12. `aws:executeScript`: verifica se il tipo di istanza corrente è supportato e restituisce il tipo di istanza AMD equivalente. Se non c'è un equivalente, l'automazione termina.
13. `aws:executeScript`: conferma che il tipo di istanza AMD è disponibile nella stessa zona di disponibilità e verifica le autorizzazioni IAM fornite.
14. `aws:branch`: ramifica l'automazione in base al fatto che il valore del `DryRun` parametro sia`yes`.
15. `aws:branch`: verifica se il tipo di istanza originale e quello di destinazione sono gli stessi. Se sono uguali, l'automazione termina.
16. `aws:executeAwsApi`: ottiene lo stato corrente dell'istanza.
17. `aws:changeInstanceState`: arresta l'istanza Amazon EC2.
18. `aws:changeInstanceState`: forza l'arresto dell'istanza se è bloccata nello stato di arresto.
19. `aws:executeAwsApi`: modifica il tipo di istanza impostando il tipo di istanza AMD di destinazione.

20. `aws:sleep`: attende 3 secondi dopo aver modificato il tipo di istanza per una maggiore coerenza.
21. `aws:branch`: ramifica l'automazione in base allo stato dell'istanza precedente. In caso affermativo`running`, l'istanza viene avviata.
    a. `aws:changeInstanceState`: avvia l'istanza Amazon EC2 se era in esecuzione prima di cambiare il tipo di istanza.
    b. `aws:waitForAwsResourceProperty`: attende che l'istanza Amazon EC2 superi i controlli di stato. Se l'istanza non supera i controlli di stato, viene ripristinata al tipo di istanza originale.
        i. `aws:changeInstanceState`: arresta l'istanza Amazon EC2 prima di cambiarla nel tipo di istanza originale.
        ii. `aws:changeInstanceState`: forza l'arresto dell'istanza Amazon EC2 prima di cambiarla nel tipo di istanza originale nel caso in cui rimanga bloccata in uno stato di arresto.
        iii. `aws:executeAwsApi`: modifica il tipo originale dell'istanza Amazon EC2.
        iv. `aws:sleep`: attende 3 secondi dopo la modifica del tipo di istanza per una maggiore coerenza.
        v. `aws:changeInstanceState`: avvia l'istanza Amazon EC2 se era in esecuzione prima di cambiare il tipo di istanza.
        vi. `aws:waitForAwsResourceProperty`: attende che l'istanza Amazon EC2 superi i controlli di stato.
22. `aws:sleep`: Attende prima di terminare il runbook.

AWSSupport-CheckXenToNitroMigrationRequirements

Descrizione

Il `AWSSupport-CheckXenToNitroMigrationRequirements` runbook verifica che un'istanza Amazon Elastic Compute Cloud (Amazon EC2) soddisfi i prerequisiti per cambiare correttamente il tipo di istanza da un'istanza di tipo Xen a un tipo di istanza basata su Nitro. Questa automazione verifica quanto segue:

- Il dispositivo principale è un volume Amazon Elastic Block Store (Amazon EBS).
- L'`enaSupport`attributo è abilitato.
- Il modulo ENA è installato sull'istanza.
- Il modulo NVMe è installato sull'istanza. In caso affermativo, il modulo viene installato e uno script verifica che il modulo sia caricato nell'`initramfs`immagine.

- Analizza `/etc/fstab` e cerca i dispositivi a blocchi montati utilizzando i nomi dei dispositivi.
- Determina se il sistema operativo (OS) utilizza nomi di interfaccia di rete prevedibili per impostazione predefinita.

Questo runbook supporta i seguenti sistemi operativi:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server15 SP2
- SUSE Linux Enterprise Server12 SP5

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Di default: false

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 di cui desideri verificare i prerequisiti prima di migrare a un tipo di istanza basato su Nitro.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `ssm:SendCommand`
- `iam:ListRoles`
- `ec2:DescribeInstances`
- `ec2:DescribeInstancesTypes`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza.
- `aws:executeAwsApi`- Raccoglie informazioni sull'hypervisor dell'istanza.
- `aws:branch`- Diramazioni in base al fatto che l'istanza di destinazione stia già eseguendo un tipo di istanza basato su Nitro.
- `aws:branch`- Verifica se il sistema operativo dell'istanza è supportato da istanze basate su Nitro.
- `aws:assertAwsResourceProperty`- Verifica che l'istanza specificata sia gestita da Systems Manager e che lo stato sia`Online`.
- `aws:branch`- Diramazioni a seconda che il dispositivo principale dell'istanza sia un volume Amazon EBS.
- `aws:branch`- Diramazioni a seconda che l'attributo ENA sia abilitato per l'istanza.
- `aws:runCommand`- Verifica la presenza di driver ENA sull'istanza.
- `aws:runCommand`- Verifica la presenza di driver NVMe sull'istanza.
- `aws:runCommand`- Verifica la presenza di formati non riconosciuti nel `fstab` file.
- `aws:runCommand`- Verifica la configurazione prevedibile del nome dell'interfaccia sull'istanza.
- `aws:executeScript`- Genera output in base ai passaggi precedenti.

Output

finalOutput.output: i risultati dei controlli eseguiti dall'automazione.

`AWSSupport-ConfigureEC2Metadata`

Descrizione

Questo runbook ti aiuta a configurare le opzioni del servizio di metadata dell'istanza (IMDS) per le istanze Amazon Elastic Compute Cloud (Amazon EC2). Utilizzando questo runbook, puoi configurare quanto segue:

- Imponi l'uso di IMDSv2, ad esempio i metadati.
- `HttpPutResponseHopLimit`Configura il valore.
- Consenti o nega l'accesso ai metadati dell'istanza.

Per ulteriori informazioni sui metadati delle istanze, consulta Configuring the Instance Metadata Service nella Amazon EC2 User Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  -Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Applica IMDS V2

  -Tipo: stringa

  Valori validi: obbligatori | facoltativi

  Predefinito: opzionale

  Descrizione: (Facoltativo) Applica IMDSv2. Se lo desideri`required`, l'istanza Amazon EC2 utilizzerà solo IMDSv2. Se lo desiderio`optional`, puoi scegliere tra IMDSv1 e IMDSv2 per l'accesso ai metadati.

  > **Important**
  >
  > Se applichi IMDSv2, le applicazioni che utilizzano IMDSv1 potrebbero non funzionare correttamente. Prima di applicare IMDSv2, assicurati che le applicazioni che utilizzano IMDS siano aggiornate a una versione che supporti IMDSv2. Per informazioni su Instance

Metadata Service versione 2 (IMDSv2), consulta Configurazione del servizio di metadati dell'istanza nella Guida per l'utente di Amazon EC2.

- HttpPutResponseHopLimite

  Tipo: integer

  Valori validi: 0-64

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) Il valore limite dell'hop di risposta HTTP PUT desiderato (1-64), ad esempio le richieste di metadati. Questo valore controlla il numero di hop che la risposta PUT può attraversare. Per evitare che la risposta si sposti all'esterno dell'istanza, specificate il 1 valore del parametro.
- InstanceId

  -Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 di cui desideri configurare le impostazioni dei metadati.
- MetadataAccess

  -Tipo: stringa

  Valori validi: abilitato | disabilitato

  Impostazione predefinita: abilitato

  Descrizione: (Facoltativo) Consenti o nega l'accesso ai metadati dell'istanza nell'istanza Amazon EC2. Se lo specifichi`disabled`, tutti gli altri parametri verranno ignorati e l'accesso ai metadati verrà negato per l'istanza.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:ModifyInstanceMetadataOptions`

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

Fasi del documento

1. branch OnMetadataAccess - Automazione delle filiali in base al valore del `MetadataAccess` parametro.
2. disableMetadataAccess - Richiama l'azione ModifyInstanceMetadataOptions API per disabilitare l'accesso agli endpoint dei metadati.
3. branch OnHttpPutResponseHopLimit - Automazione delle filiali in base al valore del `HttpPutResponseHopLimit` parametro.
4. mantieni HopLimitAndConfigureImdsVersion - Se `HttpPutResponseHopLimit` è 0, mantiene il limite di hop corrente e modifica altre opzioni di metadati.
5. wait BeforeAsserting IMDSv2State - Attende 30 secondi prima di affermare lo stato di IMDSv2.
6. set HopLimitAndConfigureImdsVersion - Se `HttpPutResponseHopLimit` è maggiore di 0, configura le opzioni dei metadati utilizzando i parametri di input forniti.
7. wait BeforeAssertingHopLimit - Attende 30 secondi prima di affermare le opzioni dei metadati.
8. assertHopLimit - Asserisce che la `HttpPutResponseHopLimit` proprietà è impostata sul valore specificato.
9. branch VerificationOn IMDSv2Option - Verifica dei rami in base al valore del parametro. `EnforceIMDSv2`
10. assertImDSv2 - IsOptional Asserisce il valore impostato su. `HttpTokens optional`
11. assertimDSv2 - Asserisce IsEnforced il valore impostato su. `HttpTokens required`
12. wait BeforeAssertingMetadataState - Attende 30 secondi prima di affermare che lo stato dei metadati sia disabilitato.
13. assert MetadataIsDisabled - Asserisce che i metadati sono. `disabled`
14. describeMetadataOptions - Ottiene le opzioni relative ai metadati dopo l'applicazione delle modifiche specificate.

Output

descrivi .State MetadataOptions

descrivereMetadataOptions. MetadataAccess

descrivi MetadataOptions .IMDSv2

descrivereMetadataOptions. HttpPutResponseHopLimite

AWSSupport-CopyEC2Instance

Descrizione

Il `AWSSupport-CopyEC2Instance` runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo del Knowledge Center Come posso spostare la mia istanza EC2 in un'altra sottorete, zona di disponibilità o VPC? L'automazione si ramifica in base ai valori specificati per i `SubnetId` parametri `Region` and.

Se specifichi un valore per il `SubnetId` parametro ma non un valore per il `Region` parametro, l'automazione crea una Amazon Machine Image (AMI) dell'istanza di destinazione e avvia una nuova istanza dalla AMI sottorete specificata.

Se specifichi un valore per il `SubnetId` parametro e il `Region` parametro, l'automazione crea una AMI delle istanze di destinazione, AMI la Regione AWS copia AMI in quella specificata e avvia una nuova istanza dalla sottorete specificata.

Se specifichi un valore per il `Region` parametro ma non un valore per il `SubnetId` parametro, l'automazione crea un'istanza AMI di destinazione, la AMI copia nella regione specificata e avvia una nuova istanza dalla sottorete predefinita del cloud privato virtuale (VPC) nella regione di destinazione. AMI

Se non viene specificato alcun valore per nessuno dei `SubnetId` parametri `Region` o, l'automazione crea un'istanza AMI di destinazione e avvia una nuova istanza dalla AMI sottorete predefinita del VPC.

Per AMI copiare un file in una regione diversa, è necessario fornire un valore per il `AutomationAssumeRole` parametro. Se l'automazione si interrompe durante la `waitForAvailableDestinationAmi` fase, è AMI possibile che la copia sia ancora in corso. In tal caso, puoi attendere il completamento della copia e avviare l'istanza manualmente.

Prima di eseguire questa automazione, tieni presente quanto segue:

- AMIsi basano sugli snapshot di Amazon Elastic Block Store (Amazon EBS). Per i file system di grandi dimensioni senza un'istantanea precedente, AMI la creazione può richiedere diverse ore. Per ridurre i tempi AMI di creazione, crea uno snapshot Amazon EBS prima di creare il. AMI

- La creazione di un AMI non crea un'istantanea, ad esempio archivia i volumi sull'istanza. Per informazioni sul backup dei volumi di archiviazione delle istanze su Amazon EBS, vedi Come si esegue il backup di un volume di istanze di archiviazione sulla mia istanza Amazon EC2 su Amazon EBS?
- La nuova istanza Amazon EC2 ha un indirizzo IP IPv4 privato o IPv6 pubblico diverso. È necessario aggiornare tutti i riferimenti ai vecchi indirizzi IP (ad esempio, nelle voci DNS) con i nuovi indirizzi IP assegnati alla nuova istanza. Se utilizzi un indirizzo IP elastico sulla tua istanza di origine, assicurati di collegarlo alla nuova istanza.
- I problemi di conflitto con l'identificatore di sicurezza del dominio (SID) possono verificarsi quando la copia viene avviata e tenta di contattare il dominio. Prima di acquisire l'AMI, utilizzare Sysprep o rimuovere l'istanza aggiunta al dominio dal dominio per evitare problemi di conflitto. Per ulteriori informazioni, vedere Come posso usare Sysprep per creare e installare AMI Windows riutilizzabili personalizzate?

Esegui questa automazione (console)

> **Important**
>
> Non è consigliabile utilizzare questo runbook per copiare le istanze di Microsoft Active Directory Domain Controller.

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID dell'istanza che desideri copiare.

- KeyPair

  Tipo: String

  Descrizione: (Facoltativo) La coppia di chiavi da associare alla nuova istanza copiata. Se stai copiando l'istanza in una regione diversa, assicurati che la coppia di chiavi esista nella regione specificata.

- Regione

  Tipo: String

  Descrizione: (Facoltativo) La regione in cui si desidera copiare l'istanza. Se specifichi un valore per questo parametro, ma non specifichi i valori per i `SecurityGroupIds` parametri `SubnetId` and, l'automazione tenta di avviare l'istanza nel VPC predefinito con il gruppo di sicurezza predefinito. Se EC2-Classic è abilitato nella regione di destinazione, l'avvio avrà esito negativo.

- SubnetId

  Tipo: String

  Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera copiare l'istanza. Se EC2-Classic è abilitato nella regione di destinazione, è necessario fornire un valore per questo parametro.

- InstanceType

  Tipo: String

  Descrizione: (Facoltativo) Il tipo di istanza con cui deve essere avviata l'istanza copiata. Se non specificate un valore per questo parametro, viene utilizzato il tipo di istanza di origine. Se il tipo di istanza di origine non è supportato nella regione in cui viene copiata l'istanza, l'automazione fallisce.

- SecurityGroupIds

  Tipo: String

  Descrizione: (Facoltativo) Un elenco separato da virgole di ID dei gruppi di sicurezza che desideri associare all'istanza copiata. Se non specificate un valore per questo parametro e l'istanza non viene copiata in un'altra regione, vengono utilizzati i gruppi di sicurezza associati all'istanza di origine. Se stai copiando l'istanza in un'altra regione, viene utilizzato il gruppo di sicurezza predefinito per il VPC predefinito nella regione di destinazione.

- KeepImageSourceRegion

  Tipo: Booleano

  Valori validi: true | false

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'automazione non elimina l'istanza AMI di origine. Se si specifica `false` questo parametro, l'automazione annulla la registrazione AMI ed elimina le istantanee associate.

- KeepImageDestinationRegion

  Tipo: Booleano

  Valori validi: true | false

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'automazione non elimina AMI ciò che viene copiato nella regione specificata. Se si specifica `false` questo parametro, l'automazione annulla la registrazione AMI ed elimina le istantanee associate.

- NoRebootInstanceBeforeTakingImage

  Tipo: Booleano

  Valori validi: true | false

  Di default: false

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'istanza di origine non verrà riavviata prima di creare il. AMI Quando viene utilizzata questa opzione, non è garantita l'integrità del file system per l'immagine creata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Se stai copiando l'istanza in un'altra regione, avrai bisogno anche delle seguenti autorizzazioni.

- `ec2:CopyImage`

Fasi del documento

- describeOriginalInstanceDettagli: raccoglie i dettagli dell'istanza da copiare.
- assertRootVolumeIsEbs- Controlla se il tipo di dispositivo del volume principale è `eebs`, in caso contrario, termina l'automazione.
- evalInputParameters- Valuta i valori forniti per i parametri di input.
- createLocalAmi- Crea una AMI delle istanze di origine.
- tagLocalAmi- Contrassegna ciò che AMI è stato creato nel passaggio precedente.
- branchAssertRegionIsSame- Diramazioni in base al fatto che l'istanza venga copiata all'interno della stessa regione o in una regione diversa.
- branchAssertSameRegionWithKeyPair- Diramazioni in base al fatto che sia stato fornito un valore per il `KeyPair` parametro per un'istanza che viene copiata all'interno della stessa regione.
- sameRegionLaunchInstanceWithKeyPair- Avvia un'istanza Amazon EC2 dall'istanza AMI di origine nella stessa sottorete o nella sottorete specificata utilizzando la coppia di chiavi specificata.

- sameRegionLaunchInstanceWithoutKeyPair- Avvia un'istanza Amazon EC2 dall'istanza AMI di origine nella stessa sottorete o nella sottorete specificata senza una coppia di chiavi.
- copyAmiToRegione: copia il file AMI nella regione di destinazione.
- waitForAvailableDestinationAmi- Attende che AMI lo stato copiato diventi. `available`
- destinationRegionLaunchIstanza: avvia un'istanza Amazon EC2 utilizzando l'istanza copiata. AMI
- branchAssertDestinationAmiToDelete- Rami in base al valore fornito per il `KeepImageDestinationRegion` parametro.
- deregisterDestinationAmiAndDeleteSnapshots- Annulla la registrazione delle istantanee copiate AMI ed elimina le istantanee associate.
- branchAssertSourceAmiTodelete- Rami in base al valore fornito per il `KeepImageSourceRegion` parametro.
- deregisterSourceAmiAndDeleteSnapshots- Annulla la registrazione del file AMI creato dall'istanza di origine ed elimina le istantanee associate.
- sleep: interrompe l'automazione per 2 secondi. Questa è una fase terminale.

Output

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchIstanza. DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

Descrizione

Il runbook ti `AWSSupport-EnableWindowsEC2SerialConsole` aiuta ad abilitare Amazon EC2 Serial Console, Special Admin Console (SAC) e il menu di avvio sulla tua istanza Amazon EC2 Windows. Con la funzionalità Console seriale di Amazon Elastic Compute Cloud (AmazonEC2), hai accesso alla porta seriale dell'EC2istanza Amazon per risolvere problemi di avvio, configurazione di rete e altri problemi. Il runbook automatizza i passaggi necessari per abilitare la funzionalità sulle istanze in stato di esecuzione e gestite da AWS Systems Manager, nonché su quelle in stato interrotto o non gestite da. AWS Systems Manager

Come funziona?

Il runbook di `AWSSupport-EnableWindowsEC2SerialConsole` automazione aiuta ad abilitare SAC e avviare il menu su EC2 istanze Amazon che eseguono Microsoft Windows Server. Per le istanze in esecuzione e gestite da AWS Systems Manager, il runbook esegue uno PowerShell script Run Command per abilitare SAC e AWS Systems Manager avviare il menu. Per le istanze in stato di arresto o non gestite da AWS Systems Manager, il runbook utilizza AWSSupport-Start EC2RescueWorkflow per creare un'EC2istanza Amazon temporanea per eseguire le modifiche richieste offline.

Per ulteriori informazioni, consulta Amazon EC2 Serial Console per istanze Windows.

Important

- Se abiliti SAC su un'istanza, i EC2 servizi Amazon che si basano sul recupero della password non funzioneranno dalla console AmazonEC2. Per ulteriori informazioni, consulta Utilizzare per SAC risolvere i problemi dell'istanza di Windows.
- Per configurare l'accesso alla console seriale, devi concedere l'accesso alla console seriale a livello di account e quindi configurare AWS Identity and Access Management (IAM) le politiche per concedere l'accesso agli utenti. È inoltre necessario configurare un utente con password su ogni istanza in modo che gli utenti possano utilizzare la console seriale per la risoluzione dei problemi. Per ulteriori informazioni, consulta Configurare l'accesso alla Amazon EC2 Serial Console.
- Per verificare se la console seriale è abilitata sul tuo account, consulta Visualizza lo stato di accesso dell'account alla console seriale.
- L'accesso alla console seriale è supportato solo su istanze virtualizzate basate sul sistema Nitro.

Per ulteriori informazioni, consulta i prerequisiti di Amazon EC2 Serial Console.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingInstances",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:Describe*",
                "ec2:createTags",
                "ec2:createImage",
                "ssm:DescribeAutomationExecutions",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetInstanceProfile",
                "ssm:GetParameters",
                "ssm:SendCommand",
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
```

```
                        "arn:${Partition}:ec2:${Region}:${AccountId}:instance/
${InstanceId}",
                        "arn:${Partition}:ec2:${Region}:${AccountId}:volume/
${VolumeId}",
                        "arn:${Partition}:iam::${AccountId}:instance-profile/
${InstanceProfileName}",
                        "arn:${Partition}:ssm:${Region}::parameter/aws/service/*",
                        "arn:${Partition}:ssm:${Region}::automation-definition/
AWSSupport-StartEC2RescueWorkflow:*",
                        "arn:${Partition}:ssm:${Region}::document/AWS-
ConfigureAWSPackage",
                        "arn:${Partition}:ssm:${Region}::document/AWS-
RunPowerShellScript"
                    ]
                },
                {
                    "Effect": "Allow",
                    "Action": [
                        "cloudformation:CreateStack"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringLike": {
                            "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
                        },
                        "ForAllValues:StringEquals": {
                            "aws:TagKeys": [
                                "AWSSupport-EC2Rescue-AutomationExecution",
                                "Name"
                            ]
                        }
                    }
                },
                {
                    "Effect": "Allow",
                    "Action": [
                        "cloudformation:DeleteStack",
                        "cloudformation:DescribeStackEvents",
                        "cloudformation:DescribeStackResource",
                        "cloudformation:DescribeStacks",
                        "ec2:AttachVolume",
                        "ec2:DetachVolume",
                        "ec2:RebootInstances",
                        "ec2:StopInstances",
```

```
                    "ec2:TerminateInstances",
                    "ssm:SendCommand"
                ],
                "Resource": "*",
                "Condition": {
                    "StringLike": {
                        "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "ec2:CreateLaunchTemplate",
                    "ec2:DeleteLaunchTemplate",
                    "ec2:RunInstances"
                ],
                "Resource": "*",
                "Condition": {
                    "ForAnyValue:StringEquals": {
                        "aws:CalledVia": [
                            "cloudformation.amazonaws.com"
                        ]
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "iam:PassRole"
                ],
                "Resource": "*",
                "Condition": {
                    "StringLikeIfExists": {
                        "iam:PassedToService": [
                            "ssm.amazonaws.com",
                            "ec2.amazonaws.com"
                        ]
                    }
                }
            }
        ]
    }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a `AWSSupport-EnableWindowsEC2SerialConsole` nella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - InstanceId: (Obbligatorio)

     L'ID dell'EC2istanza Amazon a cui desideri abilitare la console EC2 seriale Amazon, (SAC) e il menu di avvio.
   - AutomationAssumeRole: (Facoltativo)

     L'Amazon Resource Name (ARN) del IAM ruolo che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - HelperInstanceType: (Condizionale)

     Il tipo di EC2 istanza Amazon fornita dal runbook per configurare la console EC2 seriale Amazon per un'istanza offline.
   - HelperInstanceProfileName: (Condizionale)

     Il nome di un profilo di IAM istanza esistente per l'istanza helper. Se state abilitando SAC un menu di avvio su un'istanza che si trova in stato di arresto o non è gestita da AWS Systems Manager, questo è obbligatorio. Se non viene specificato un profilo di IAM istanza, l'automazione ne crea uno per conto dell'utente.
   - SubnetId: (Condizionale)

     L'ID di sottorete per un'istanza di supporto. Per impostazione predefinita, utilizza la stessa sottorete in cui risiede l'istanza fornita.

     > **Important**
     >
     > Se si fornisce una sottorete personalizzata, questa deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint Systems Manager. Questo

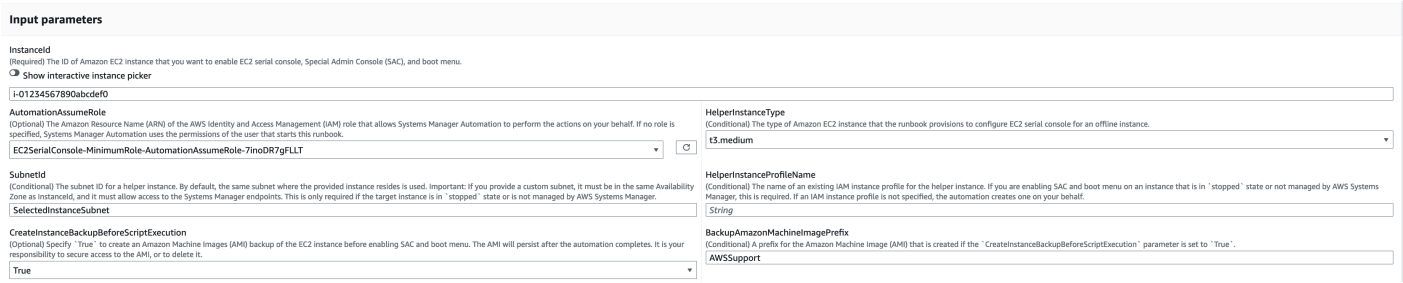
è necessario solo se l'istanza di destinazione è interrotta o non è gestita da. AWS Systems Manager

- CreateInstanceBackupBeforeScriptExecution: (Facoltativo)

  Specificare True per creare un backup Amazon Machine Images (AMI) dell'EC2istanza Amazon prima dell'attivazione SAC e del menu di avvio. AMIPersisterà dopo il completamento dell'automazione. È responsabilità dell'utente garantire l'accesso AMI o eliminarlo.

- BackupAmazonMachineImagePrefix: (Condizionale)

  Un prefisso per Amazon Machine Image (AMI) che viene creato se il `CreateInstanceBackupBeforeScriptExecution` parametro è impostato `True` su.



4. Seleziona Esegui.
5. L'automazione inizia.
6. Il documento esegue le seguenti operazioni:

   - CheckIfEc2SerialConsoleAccessEnabled:

     Verifica se l'accesso ad Amazon EC2 Serial Console è abilitato a livello di account. Nota: l'accesso alla console seriale non è disponibile per impostazione predefinita. Per ulteriori informazioni, consulta Configurare l'accesso alla Amazon EC2 Serial Console.

   - CheckIfEc2InstanceIsWindows:

     Indica se la piattaforma dell'istanza di destinazione è Windows.

   - GetInstanceType:

     Recupera il tipo di istanza dell'istanza di destinazione.

   - CheckIfInstanceTypeIsNitro:

     Verifica se l'hypervisor di tipo di istanza è basato su Nitro. Serial Console Access è supportato solo su istanze virtualizzate basate sul sistema Nitro.

- CheckIfInstanceIsInAutoScalingGroup:

  Verifica se l'EC2istanza Amazon fa parte di un gruppo Amazon EC2 Auto Scaling chiamando il. `DescribeAutoScalingInstances` API Se l'istanza fa parte di un gruppo Amazon EC2 Auto Scaling, assicura che il Porting Assistant per. NETl'istanza è nello stato del ciclo di vita Standby.

- WaitForEc2: InstanceStateStablized

  Attende che l'istanza sia in esecuzione o interrotta.

- GetEc2: InstanceState

  Ottiene lo stato corrente dell'istanza.

- BranchOnEc2InstanceState:

  Rami basati sullo stato dell'istanza recuperato nel passaggio precedente. Se lo stato dell'istanza è in esecuzione, passa al `CheckIfEc2InstanceIsManagedBySSM` passaggio e, in caso contrario, passa al `CheckIfHelperInstanceProfileIsProvided` passaggio.

- CheckIfEc2 InstanceIsManagedBySSM:

  Verifica se l'istanza è gestita da AWS Systems Manager. Se gestito, il runbook abilita SAC un menu di avvio utilizzando un comando PowerShell Run.

- BranchOnPreEC2RescueBackup:

  Rami basati sul parametro `CreateInstanceBackupBeforeScriptExecution` di input.

- CreateAmazonMachineImageBackup:

  Crea un AMI backup dell'istanza.

- E nableSACAndBootMenu:

  Abilita SAC e avvia il menu eseguendo uno script PowerShell Run Command.

- RebootInstance:

  Riavvia l'EC2istanza Amazon per applicare la configurazione. Questo è il passaggio finale se l'istanza è online ed è gestita da AWS Systems Manager.

- CheckIfHelperInstanceProfileIsProvided:

  Verifica se lo `HelperInstanceProfileName` specificato esiste prima di abilitarlo SAC e avvia il menu offline utilizzando un'EC2istanza Amazon temporanea.

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

Esegue `AWSSupport-StartEC2RescueWorkflow` il menu di attivazione SAC e avvio quando l'istanza è interrotta o non è gestita da AWS Systems Manager.

- GetExecutionDetails:

  Recupera l'ID dell'immagine del backup e dell'output dello script offline.

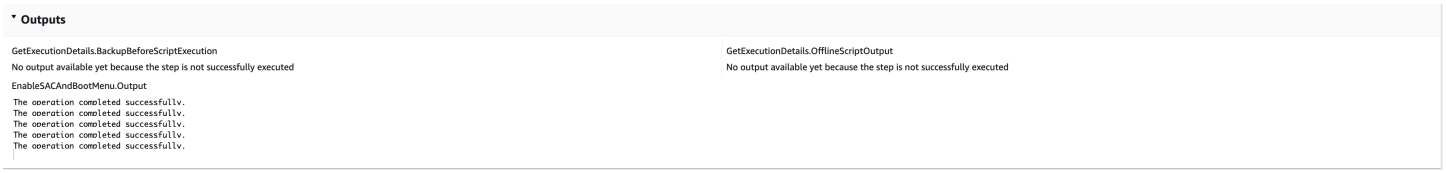
7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:
   - E. Uscita nableSACAndBootMenu:

     Risultato dell'esecuzione del comando nel `EnableSACAndBootMenu` passaggio.
   - GetExecutionDetails.OfflineScriptOutput:

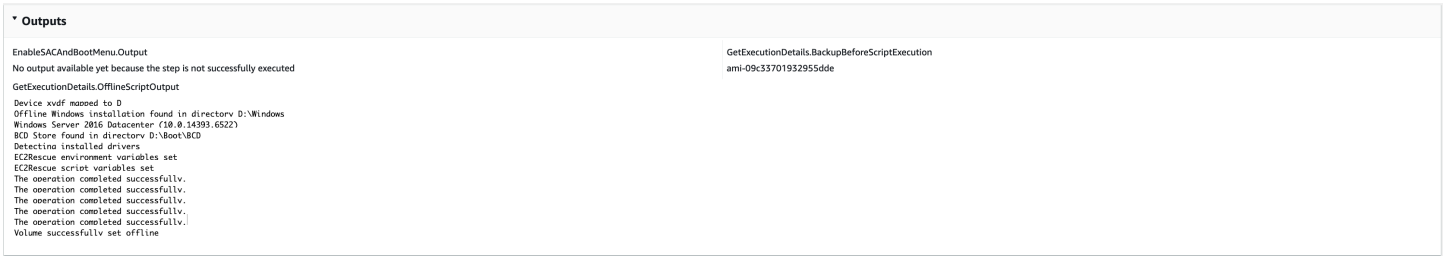
     Output dello script offline eseguito nella `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` fase.
   - GetExecutionDetails.BackupBeforeScriptExecution:

     ID dell'immagine del AMI backup eseguito se il parametro `CreateInstanceBackupBeforeScriptExecution` di input è True.

Output di esecuzione su un'istanza in esecuzione e gestita da AWS Systems Manager



Output dell'esecuzione su un'istanza interrotta o non gestita da AWS Systems Manager



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione

- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWSSupport-ExecuteEC2Rescue

Descrizione

Questo runbook utilizza lo EC2Rescue strumento per risolvere e, ove possibile, riparare i problemi di connettività comuni con l'istanza Amazon Elastic Compute Cloud (Amazon EC2) specificata per Linux o. Windows Server Le istanze con volumi root crittografati non sono supportate.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EC2 RescueInstanceType

  Tipo: String

  Valori validi: t2.small | t2.medium | t2.large

  Impostazione predefinita: t2.small

Descrizione: (Obbligatorio) Il tipo di istanza EC2 per l'EC2Rescueistanza. Dimensioni consigliate: `t2.small`

- LogDestination

  Tipo: String

  Descrizione: (Facoltativo) Nome del bucket Amazon S3 nel tuo account in cui desideri caricare i log di risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- SubnetId

  Tipo: String

  Predefinito: CreateNew VPC

  Descrizione: (Facoltativo) L'ID della sottorete dell'EC2Rescueistanza. Per impostazione predefinita, AWS Systems Manager Automation crea un nuovo VPC. In alternativa, utilizza `SelectedInstanceSubnet` la stessa sottorete dell'istanza o specifica un ID di sottorete personalizzato.

  > **Important**
  >
  > La sottorete deve trovarsi nella stessa `UnreachableInstanceId` zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

- UnreachableInstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza EC2 non raggiungibile.

  > **Important**
  >
  > Systems Manager Automation interrompe questa istanza e crea un'AMI prima di tentare qualsiasi operazione. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico cambierà se non si utilizza un indirizzo IP elastico.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Devi avere almeno `ssm:StartAutomationExecution` ed `ssm:GetAutomationExecution` essere in grado di leggere l'output dell'automazione. Per ulteriori informazioni sulle autorizzazioni richieste, consulta `AWSSupport-StartEC2RescueWorkflow`.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Asserisce se l'istanza fornita èWindows Server:
   a. (EC2RescueperWindows Server) Se l'istanza fornita è un'Windows Serveristanza:
      i. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con lo script EC2Rescue per offline. Windows Server
      ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata.
      iii. `aws:executeAwsApi`- Recupera il riepilogo di EC2Rescue dall'automazione annidata.
   b. (EC2Rescueper Linux) Se l'istanza fornita è un'istanza Linux:
      i. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con gli script offline di EC2Rescue per Linux
      ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata.
      iii. `aws:executeAwsApi`- Recupera il riepilogo di EC2Rescue dall'automazione annidata.

Output

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descrizione

Il `AWSSupport-ListEC2Resources` runbook restituisce informazioni sulle istanze Amazon EC2 e sulle risorse correlate come i volumi Amazon Elastic Block Store (Amazon EBS), gli indirizzi IP elastici e i gruppi Amazon EC2 Auto Scaling da te specificati. Regioni AWS Per impostazione

predefinita, le informazioni vengono raccolte da tutte le regioni e vengono visualizzate nell'output dell'automazione. Facoltativamente, puoi specificare un bucket Amazon Simple Storage Service (Amazon S3) in cui caricare le informazioni come file con valori separati da virgole (.csv).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Bucket

  Tipo: String

  Descrizione: (Facoltativo) Il nome del bucket S3 in cui vengono caricate le informazioni raccolte.
- DisplayResourceDeletionDocumentation

  Tipo: String

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostata su`true`, l'automazione crea collegamenti nell'output alla documentazione relativa all'eliminazione delle risorse.
- RegionsToQuery

Tipo: String

Impostazione predefinita: Tutti

Descrizione: (Facoltativo) Le regioni da cui desideri raccogliere informazioni relative ad Amazon EC2.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Inoltre, per caricare correttamente le informazioni raccolte nel bucket S3 specificato, sono `AutomationAssumeRole` necessarie le seguenti azioni:

- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie le regioni abilitate per l'account.
- `aws:executeScript`- Conferma che le regioni abilitate per l'account supportano le regioni specificate nel `RegionsToQuery` parametro.

- `aws:branch`- Se nessuna regione è abilitata per l'account, l'automazione termina.
- `aws:executeScript`- Elenca tutte le istanze EC2 per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutte le Amazon Machine Images (AMI) per l'account e le regioni specificati.
- `aws:executeScript`- Elenca tutti i volumi EBS per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti gli indirizzi IP elastici per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutte le interfacce di rete elastiche per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti i gruppi di Auto Scaling per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti i sistemi di bilanciamento del carico per l'account e le regioni specificate.
- `aws:executeScript`- Carica le informazioni raccolte nel bucket S3 specificato se fornisci un valore per il parametro. `Bucket`

`AWSSupport-ManageRDPSettings`

Descrizione

Il `AWSSupport-ManageRDPSettings` runbook consente all'utente di gestire impostazioni comuni del Remote Desktop Protocol (RDP), come la porta RDP e l'autenticazione a livello di rete (NLA). Per impostazione predefinita, il runbook legge ed emette i valori delle impostazioni.

> **Important**
>
> Le modifiche alle impostazioni RDP devono essere esaminate attentamente prima di eseguire questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza gestita per la quale gestire le impostazioni RDP.
- NLA SettingAction

  Tipo: String

  Valori validi: Controlla | Abilita | Disabilita

  Impostazione predefinita: Check

  Descrizione: (obbligatorio) operazione da eseguire sulle impostazioni NLA: Check, Enable, Disable.
- RDPPort

  Tipo: String

  Impostazione predefinita: 3389

  Descrizione: (facoltativo) specifica la nuova porta RDP. Utilizzato solo quando l'operazione è impostata su Modify. Il numero di porta deve essere compreso tra 1025 e 65535. Nota: dopo la modifica della porta il servizio RDP viene riavviato.
- RDP PortAction

Tipo: String

Valori validi: Controlla | Modifica

Impostazione predefinita: Check

Descrizione: (Obbligatoria) Un'azione da applicare alla porta RDP.

- RemoteConnections

  Tipo: String

  Valori validi: Controlla | Abilita | Disabilita

  Impostazione predefinita: Check

  Descrizione: (Obbligatoria) Un'azione da eseguire sull'impostazione fdenytsConnections.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

L'istanza EC2 che riceve il comando deve avere un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. L'utente deve avere almeno ssm: SendCommand per inviare il comando all'istanza, più ssm: GetCommandInvocation per poter leggere l'output del comando.

Fasi del documento

`aws:runCommand`- Esegui lo PowerShell script per modificare o controllare le impostazioni RDP sull'istanza di destinazione.

Output

manageRDPSettings.Output

AWSSupport-ManageWindowsService

Descrizione

Il `AWSSupport-ManageWindowsService` runbook consente di interrompere, avviare, riavviare, mettere in pausa o disabilitare qualsiasi servizio Windows sull'istanza di destinazione.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID dell'istanza gestita di cui gestire i servizi.
- ServiceAction

  Tipo: String

  Valori validi: Verifica | Riavvio | Riavvio forzato | Avvio | Arresto | Stop forzato | Pausa

  Impostazione predefinita: Check

  Descrizione: (Obbligatoria) Un'azione da applicare al servizio Windows. Nota che `Force-Restart` and `Force-Stop` può essere usato per riavviare e interrompere un servizio con servizi dipendenti.

- StartupType

  Tipo: String

  Valori validi: Verifica | Auto | Domanda | Disabilitato | DelayedAutoStart

  Impostazione predefinita: Check

  Descrizione: (Obbligatorio) Un tipo di avvio da applicare al servizio Windows.
- WindowsServiceName

  Tipo: String

  Descrizione: (obbligatorio) nome del servizio di Windows valido.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l'istanza EC2 che riceve il comando abbia un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. L'utente deve disporre almeno di ssm: StartAutomationExecution e ssm: SendCommand per eseguire l'automazione e inviare il comando all'istanza, oltre a ssm: GetAutomationExecution per poter leggere l'output dell'automazione.

Fasi del documento

`aws:runCommand`- Esegui lo PowerShell script per applicare la configurazione desiderata al servizio Windows sull'istanza di destinazione.

Output

manageWindowsService.Uscita

AWSSupport-MigrateEC2ClassicToVPC

Descrizione

Il `AWSSupport-MigrateEC2ClassicToVPC` runbook esegue la migrazione di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) da EC2-Classic a un cloud privato virtuale (VPC). Questo runbook supporta la migrazione di istanze Amazon EC2 del tipo di virtualizzazione hardware delle macchine virtuali (HVM) con i volumi root di Amazon Elastic Block Store (Amazon EBS).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- Approva IAM

  Tipo: StringList

  Descrizione: (Facoltativo) I nomi delle risorse Amazon (ARN) degli utenti IAM che possono approvare o rifiutare l'azione. Questo parametro si applica solo se si specifica il `CutOver` valore del `MigrationType` parametro.
- DestinationSecurityGroupId

  Tipo: StringList

  Descrizione: (Facoltativo) L'ID del gruppo di sicurezza che desideri associare all'istanza Amazon EC2 che viene avviata nel tuo VPC. Se non specifichi un valore per questo parametro, l'automazione crea un gruppo di sicurezza nel tuo cloud privato virtuale e copia le regole dal gruppo di sicurezza in EC2-Classic. Se le regole non vengono copiate nel nuovo gruppo di sicurezza, il gruppo di sicurezza predefinito del cloud privato virtuale è associato all'istanza Amazon EC2.
- DestinationSubnetId

Tipo: String

Descrizione: (Facoltativo) L'ID della sottorete verso cui desideri migrare la tua istanza Amazon EC2. Se non specifichi un valore per questo parametro, l'automazione sceglie casualmente una sottorete dal tuo VPC.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 che desideri migrare.

- MigrationType

  Tipo: String

  Valori validi: CutOver | Test

  Descrizione: (Obbligatorio) Il tipo di migrazione che si desidera eseguire.

  L'`CutOver`opzione richiede l'approvazione per interrompere l'istanza Amazon EC2 in esecuzione in EC2-Classic. Dopo l'approvazione di questa azione, l'istanza Amazon EC2 viene interrotta e l'automazione crea un Amazon Machine Image (AMI). Quando lo AMI stato è`available`, viene lanciata una nuova istanza Amazon EC2 da `DestinationSubnetId` quello specificato nel tuo VPC. AMI Se la tua istanza Amazon EC2 in esecuzione in EC2-Classic ha un indirizzo IP elastico collegato, l'istanza verrà spostata nell'istanza Amazon EC2 appena creata nel tuo cloud privato virtuale. Se l'istanza Amazon EC2 che viene avviata nel tuo VPC non viene creata per qualsiasi motivo, viene interrotta e viene richiesta l'approvazione per avviare l'istanza Amazon EC2 in EC2-Classic.

  L'`Test`opzione crea una AMI delle tue istanze Amazon EC2 in esecuzione in EC2-Classic senza riavvio. Poiché l'istanza Amazon EC2 non si riavvia, non possiamo garantire l'integrità del file system dell'immagine creata. Quando lo AMI stato è`available`, viene lanciata una nuova istanza Amazon EC2 da questo AMI punto `DestinationSubnetId` specificato nel tuo VPC. Se la tua istanza Amazon EC2 in esecuzione in EC2-Classic ha un indirizzo IP elastico collegato, l'automazione verifica che quello specificato sia pubblico`DestinationSubnetId`. Se l'istanza Amazon EC2 avviata nel tuo VPC non viene creata per qualsiasi motivo, viene interrotta e l'automazione termina.

- Notifica SNS AR NforApproval

Tipo: String

Descrizione: (Facoltativo) L'argomento ARN di Amazon Simple Notification Service (Amazon SNS) a cui desideri inviare le richieste di approvazione. Questo parametro si applica solo se si specifica il `CutOver` valore del `MigrationType` parametro.

- TargetInstanceType

  Tipo: String

  Predefinito: t2.2xlarge

  Descrizione: (Facoltativo) Il tipo di istanza Amazon EC2 che desideri avviare nel tuo VPC. Sono supportati solo i tipi di istanze basati su Xen, come T2, M4 o C4.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetDocument`
- `ssm:ListDocumentVersions`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:ListSubscriptions`
- `sns:ListTopics`
- `sns:Publish`
- `ec2:AssociateAddress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateImage`
- `ec2:CreateSecurityGroup`
- `ec2:DeleteSecurityGroup`
- `ec2:MoveAddressToVpc`
- `ec2:RunInstances`

- ec2:StopInstances
- ec2:CreateTags
- ec2:DescribeAddresses
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroupReferences
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTags
- ec2:DescribeVpcs
- ec2:DescribeInstanceTypes
- ec2:DescribeImages

Fasi del documento

- aws:executeAwsApi- Raccoglie dettagli sull'istanza Amazon EC2 specificata nel InstanceId parametro.
- aws:assertAwsResourceProperty- Conferma che il tipo di istanza specificato nel TargetInstanceType parametro è basato su Xen.
- aws:assertAwsResourceProperty- Conferma che l'istanza Amazon EC2 specificata nel InstanceId parametro è del tipo di virtualizzazione HVM.
- aws:assertAwsResourceProperty- Conferma che l'istanza Amazon EC2 specificata nel InstanceId parametro ha un volume root di Amazon EBS.
- aws:executeScript- Crea un gruppo di sicurezza in base alle esigenze in base al valore specificato per il DestinationSecurityGroupId parametro.
- aws:branch- Rami in base al valore specificato nel DestinationSubnetId parametro.
- aws:executeAwsApi- Identifica il VPC predefinito nel luogo in Regione AWS cui si esegue questa automazione.
- aws:executeAwsApi- Sceglie casualmente l'ID di una sottorete situata nel VPC predefinito.
- aws:createImage- Crea e AMI senza riavviare l'istanza Amazon EC2.

- `aws:branch`- Rami in base al valore specificato per il `MigrationType` parametro.
- `aws:branch`- Rami in base al valore specificato per il `DestinationSubnetId` parametro.
- `aws:runInstances`- Avvia una nuova istanza dall'istanza AMI creata senza riavviare l'istanza Amazon EC2 in EC2-Classic.
- `aws:changeInstanceState`- Termina l'istanza Amazon EC2 appena lanciata se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:runInstances`- Avvia una nuova istanza dall'istanza AMI creata senza riavviare l'istanza Amazon EC2 in EC2-Classic, se fornito. `DestinationSubnetId`
- `aws:changeInstanceState`- Termina l'istanza Amazon EC2 appena lanciata se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:assertAwsResourceProperty`- Conferma il comportamento di arresto dell'istanza Amazon EC2 in esecuzione in EC2-Classic.
- `aws:approve`- Attende l'approvazione per interrompere l'istanza Amazon EC2.
- `aws:changeInstanceState`- Interrompe l'esecuzione dell'istanza Amazon EC2 in EC2-Classic.
- `aws:changeInstanceState`- Se necessario, la forza interrompe l'esecuzione dell'istanza Amazon EC2 in EC2-Classic.
- `aws:createImage`- Crea un'AMIistanza Amazon EC2 dopo che è stata interrotta.
- `aws:branch`- Rami in base al valore specificato per il `DestinationSubnetId` parametro.
- `aws:runInstances`- Avvia una nuova istanza dalla AMI creazione dell'istanza Amazon EC2 interrotta in EC2-Classic.
- `aws:approve`- Attende l'approvazione per terminare l'istanza appena avviata e avvia l'istanza Amazon EC2 in EC2-Classic se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:changeInstanceState`- Termina l'istanza Amazon EC2 appena lanciata.
- `aws:runInstances`- Avvia una nuova istanza dalla AMI creazione dell'istanza Amazon EC2 interrotta in EC2-Classic a partire dal parametro. `DestinationSubnetId`
- `aws:approve`- Attende l'approvazione per terminare l'istanza appena avviata e avvia l'istanza Amazon EC2 in EC2-Classic se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:changeInstanceState`- Termina l'istanza Amazon EC2 appena lanciata.
- `aws:changeInstanceState`- Avvia l'istanza Amazon EC2 che è stata interrotta in EC2-Classic.
- `aws:branch`- Filiali a seconda che l'istanza Amazon EC2 disponga di un indirizzo IP pubblico.
- `aws:executeAwsApi`- Verifica se l'indirizzo IP pubblico è un indirizzo IP elastico.
- `aws:branch`- Rami in base al valore specificato nel `MigrationType` parametro.

- `aws:executeAwsApi`- Sposta l'indirizzo IP elastico nel tuo VPC.
- `aws:executeAwsApi`- Raccoglie l'ID di allocazione dell'indirizzo IP elastico che è stato spostato nel tuo VPC.
- `aws:branch`- Filiali in base alla sottorete in cui è stata lanciata l'istanza Amazon EC2 in esecuzione nel tuo VPC.
- `aws:executeAwsApi`- Associa l'indirizzo IP elastico all'istanza appena avviata nel tuo VPC.
- `aws:executeScript`- Conferma che la sottorete che la tua istanza Amazon EC2 appena lanciata in esecuzione nel tuo VPC è pubblica.

Output

g `etInstanceProperties.virtualizationType` - Il tipo di virtualizzazione dell'istanza Amazon EC2 in esecuzione in EC2-Classic.

`getInstanceProperties.rootDeviceType`- Il tipo di dispositivo root dell'istanza Amazon EC2 in esecuzione in EC2-Classic.

`createAMIWithoutReboot.ImageId`- L'ID dell'istanza AMI creata senza riavviare l'istanza Amazon EC2 in esecuzione in EC2-Classic.

`getDefaultVPC.VpcId`- L'ID del VPC predefinito su cui viene avviata la nuova istanza Amazon EC2 se non viene fornito un valore per il `DestinationSubnetId` parametro.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- L'ID della sottorete nel VPC predefinito in cui viene avviata la nuova istanza Amazon EC2 se non viene fornito un valore per il `DestinationSubnetId` parametro.

`launchTestInstanceDefaultVPC.InstanceIds`- L'ID dell'istanza Amazon EC2 appena lanciata nel tuo VPC predefinito durante il tipo di `Test` migrazione.

`launchTestInstanceProvidedSubnet.InstanceIds`- L'ID dell'istanza Amazon EC2 appena lanciata corrisponde a `DestinationSubnetId` quello specificato durante il tipo di `Test` migrazione.

`createAMIAfterStoppingInstance.ImageId`- L'ID dell'istanza AMI creata dopo l'interruzione dell'esecuzione dell'istanza Amazon EC2 in EC2-Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- L'ID dell'istanza Amazon EC2 appena lanciata corrisponde a `DestinationSubnetId` quello specificato durante il tipo di `CutOver` migrazione.

`launchCutOverInstanceDefaultVPC.InstanceIds`- L'ID dell'istanza Amazon EC2 appena lanciata nel tuo VPC predefinito durante il tipo di `CutOver` migrazione.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Se la sottorete scelta dall'automazione nel VPC predefinito è pubblica.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Se la sottorete specificata `DestinationSubnetId` è pubblica.

AWSSupport-MigrateXenToNitroLinux

Descrizione

Il `AWSSupport-MigrateXenToNitroLinux` runbook clona, prepara e migra un'istanza Linux Xen di Amazon Elastic Compute Cloud (Amazon EC2) su un tipo di istanza. Nitro Questo runbook fornisce due opzioni per i tipi di operazioni:

- `Clone&Migrate`— Il flusso di lavoro di questa opzione è costituito da controlli preliminari, test e Clone&Migratefasi. Il flusso di lavoro viene eseguito utilizzando il `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` runbook.
- `FullMigration`— Questa opzione esegue il `Clone&Migrate` flusso di lavoro e quindi esegue il passaggio aggiuntivo di Sostituisci i volumi root di Amazon EBS.

> **Important**
>
> L'utilizzo di questo runbook comporta costi sul tuo account per il tempo di esecuzione delle istanze Amazon EC2, la creazione di volumi Amazon Elastic Block Store (Amazon EBS) e. AMIs Per maggiori dettagli, consulta i prezzi di Amazon EC2 e i prezzi di Amazon EBS.

Controlli preliminari

L'automazione esegue i seguenti controlli preliminari prima di continuare con la migrazione. Se uno qualsiasi dei controlli fallisce, l'automazione termina. Questa fase è solo una parte del `Clone&Migrate` flusso di lavoro.

- Verifica se l'istanza di destinazione è già un tipo di Nitro istanza.
- Verifica se l'opzione di acquisto delle istanze Spot è stata utilizzata per l'istanza di destinazione.
- Verifica se i volumi dell'archivio delle istanze sono collegati all'istanza di destinazione.

- Verifica che il sistema operativo (OS) dell'istanza di destinazione sia Linux.
- Verifica se l'istanza di destinazione fa parte di un gruppo Amazon EC2 Auto Scaling. Se fa parte di un gruppo Auto Scaling, l'automazione verifica che l'istanza sia nello `standby` stato.
- Verifica che l'istanza sia gestita daAWS Systems Manager.

Test

L'automazione crea una Amazon Machine Image (AMI) dall'istanza di destinazione e lancia un'istanza di test da quella appena creataAMI. Questa fase fa parte solo del `Clone&Migrate` flusso di lavoro.

Se l'istanza di test supera tutti i controlli di stato, l'automazione si interrompe e l'approvazione dei responsabili designati viene richiesta tramite la notifica di Amazon Simple Notification Service (Amazon SNS). Se viene fornita l'approvazione, l'automazione termina l'istanza di test, arresta l'istanza di destinazione e continua con la migrazione, mentre quella appena creata AMI viene annullata alla fine del flusso di lavoro. `Clone&Migrate`

> **Note**
>
> Prima di fornire l'approvazione, si consiglia di verificare che tutte le applicazioni in esecuzione sull'istanza di destinazione siano state chiuse correttamente.

Clonazione e migrazione

L'automazione ne crea un'altra AMI dall'istanza di destinazione e lancia una nuova istanza per passare a un tipo di Nitro istanza. L'automazione completa i seguenti prerequisiti prima di continuare con la migrazione. Se uno qualsiasi dei controlli fallisce, l'automazione termina. Anche questa fase è solo una parte del `Clone&Migrate` flusso di lavoro.

- Attiva l'attributo Enhanced Networking (ENA).
- Installa la versione più recente dei driver ENA, se non sono già installati, oppure aggiorna la versione dei driver ENA alla versione più recente. Per garantire le massime prestazioni di rete, è necessario l'aggiornamento alla versione più recente del driver ENA se il tipo di Nitro istanza è di sesta generazione.
- Verifica che il modulo NVMe sia installato. Se il modulo è installato, l'automazione verifica che il modulo sia stato caricato. `initramfs`

- Analizza `/etc/fstab` e sostituisce le voci con i nomi dei dispositivi a blocchi (`/dev/sd*o/dev/xvd*`) con i rispettivi UUID. Prima di modificare la configurazione, l'automazione crea un backup del file nel percorso`/etc/fstab*`.
- Disattiva la denominazione prevedibile delle interfacce aggiungendo l'`net.ifnames=0`opzione alla `GRUB_CMDLINE_LINUX` riga del `/etc/default/grub` file, se esiste, o al kernel in. `/boot/grub/menu.lst`
- Rimuove il `/etc/udev/rules.d/70-persistent-net.rules` file, se esiste. Prima di rimuovere il file, l'automazione crea un backup del file nel percorso`/etc/udev/rules.d/`.

Dopo aver verificato tutti i requisiti, il tipo di istanza viene modificato nel tipo di Nitro istanza specificato. L'automazione attende che l'istanza appena creata superi tutti i controlli di stato dopo essere stata avviata come tipo di Nitro istanza. L'automazione attende quindi l'approvazione dei responsabili designati per creare una AMI delle istanze Nitro avviate con successo. Se l'approvazione viene negata, l'automazione termina, lasciando in esecuzione l'istanza appena creata e l'istanza di destinazione rimane interrotta.

Sostituisci il volume Amazon EBS principale

Se scegli `FullMigration` come`OperationType`, l'automazione esegue la migrazione dell'istanza Amazon EC2 di destinazione al tipo di Nitro istanza specificato. L'automazione richiede l'approvazione dei responsabili designati per sostituire il volume root Amazon EBS dell'istanza Amazon EC2 di destinazione con il volume root dell'istanza Amazon EC2 clonata. Una volta completata la migrazione, l'istanza Amazon EC2 clonata viene terminata. Se l'automazione fallisce, il volume root originale di Amazon EBS viene collegato all'istanza Amazon EC2 di destinazione. Se il volume principale di Amazon EBS collegato all'istanza Amazon EC2 di destinazione presenta tag con il `aws:` prefisso applicato, l'`FullMigration`operazione non è supportata.

Prima di iniziare

L'istanza di destinazione deve disporre di un accesso a Internet in uscita. Questo serve per accedere a repository per driver e dipendenze comekernel-devel,gcc,,patch,rpm-build, wget dracutmake, linux-headers e. unzip Se necessario, viene utilizzato il gestore di pacchetti.

È necessario un argomento Amazon SNS per inviare notifiche di approvazioni e aggiornamenti. Per ulteriori informazioni sulla creazione di un argomento Amazon SNS, consulta Creare un argomento Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Questo runbook supporta i seguenti sistemi operativi:

- RHEL7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Server Debian
- Ubuntu Server 18.04 LTS, 20.04 LTS e 20.10 STR
- SUSE Linux Enterprise Server(SUSE 12 SP5, SUSE 15 SP2)

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Riconoscimento

  Tipo: String

  Descrizione: (Obbligatorio) Leggi i dettagli completi delle azioni eseguite da questo runbook di automazione ed entra **`Yes, I understand and acknowledge`** per procedere con l'utilizzo del runbook.
- Approva IAM

  Tipo: String

Descrizione: (Obbligatorio) Gli ARN dei ruoli, degli utenti o dei nomi utente IAM che possono fornire approvazioni all'automazione. È possibile specificare un massimo di 10 approvatori.

- DeleteResourcesOnFailure

  Tipo: Booleano

  Descrizione: (Facoltativo) Determina se l'istanza appena creata e AMI quella per la migrazione vengono eliminate in caso di errore dell'automazione.

  Valori validi: True | False

  Impostazione predefinita: True

- MinimumRequiredApprovals

  Tipo: String

  Descrizione: (Facoltativo) Il numero minimo di approvazioni necessarie per continuare a eseguire l'automazione quando vengono richieste le approvazioni.

  Valori validi: 1-10

  Impostazione predefinita: 1

- NitroInstanceType

  Tipo: String

  Descrizione: (Obbligatorio) Il tipo di Nitro istanza in cui si desidera modificare l'istanza. I tipi di istanza supportati includono M5, M6, C5, C6, R5, R6 e T3.

  Impostazione predefinita: m5.xlarge

- OperationType

  Tipo: String

  Descrizione: (Obbligatorio) L'operazione che si desidera eseguire. L'`FullMigration`opzione esegue le stesse attività `Clone&Migrate` e sostituisce inoltre il volume root dell'istanza di destinazione. Il volume radice dell'istanza di destinazione viene sostituito con il volume radice dell'istanza appena creata dopo il processo di migrazione. L'`FullMigration`operazione non supporta i volumi root definiti da Logical Volume Manager (LVM).

Valori validi: Clone&Migrate | FullMigration

- SNS TopicArn

  Tipo: String

  Descrizione: (Obbligatorio) L'ARN dell'argomento Amazon SNS per la notifica di approvazione. L'argomento Amazon SNS viene utilizzato per inviare le notifiche di approvazione richieste durante l'automazione.

- TargetInstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID delle istanze Amazon EC2 da migrare.

Flusso di lavoro di Clone&Migrate

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`
- `ec2:CreateImage`

- ec2:RunInstances
- ec2:DescribeInstanceStatus
- ec2:DeregisterImage
- ec2:DeleteSnapshot
- ec2:TerminateInstances
- ec2:StartInstances
- ec2:DescribeKeyPairs
- ec2:StopInstances
- kms:CreateGrant*
- kms:ReEncrypt
- ec2:ModifyInstanceAttribute
- autoscaling:DescribeAutoScalingInstances
- iam:passRole
- iam:ListRoles

Fasi del documento

- startOfPreliminaryChecksBranch- Diramazioni al flusso di lavoro dei controlli preliminari.
- getTargetInstanceProperties- Raccoglie i dettagli dall'istanza di destinazione.
- checkIfNitroInstanceTypeIsSupportedInAZ- Determina se il tipo di istanza Amazon EC2 di destinazione è supportato nella stessa zona di disponibilità dell'istanza di destinazione.
- getXenInstanceTypeDetails- Raccoglie dettagli sul tipo di istanza di origine.
- checkIfInstanceHypervisorIsNitroAlready- Verifica se l'istanza di destinazione è già in esecuzione come tipo di Nitro istanza.
- checkIfTargetInstanceLifecycleIsSpot- Verifica se l'opzione di acquisto dell'istanza di destinazione è Spot.
- checkIfOperatingSystemIsLinux- Verifica se il sistema operativo dell'istanza di destinazione è Linux.
- verifySSMConnectivityForTargetInstance- Verifica che l'istanza di destinazione sia gestita da Systems Manager.
- checkIfEphemeralVolumeAreSupported- Verifica se il tipo di istanza corrente dell'istanza di destinazione supporta i volumi di archiviazione delle istanze.

- `verifyIfTargetInstanceHasEphemeralVolumesAttached`- Verifica se all'istanza di destinazione sono collegati i volumi dell'archivio delle istanze.
- `checkIfRootVolumeIsEBS`- Verifica se il tipo di volume root dell'istanza di destinazione è EBS.
- `checkIfTargetInstanceIsInASG`- Verifica se l'istanza di destinazione fa parte di un gruppo Auto Scaling.
- `endOfPreliminaryChecksBranch`- Fine del ramo dei controlli preliminari.
- `startOfTestBranch`- Diramazioni al flusso di lavoro dei test.
- `createTestImage`- Crea un test AMI dell'istanza di destinazione.
- `launchTestInstanceInSameSubnet`- Avvia un'istanza di test dal test AMI utilizzando la stessa configurazione dell'istanza di destinazione.
- `cleanupTestInstance`- Termina l'istanza di test.
- `endOfTestBranch`- Fine del ramo Testing.
- `checkIfTestingBranchSucceeded`- Verifica lo stato del ramo Testing.
- `approvalToStopTargetInstance`- Attende l'approvazione dei responsabili designati per interrompere l'istanza bersaglio.
- `stopTargetEC2Instance`- Arresta l'istanza di destinazione.
- `forceStopTargetEC2Instance`- La forza arresta l'istanza di destinazione solo se il passaggio precedente non riesce a fermare l'istanza.
- `startOfCloneAndMigrateBranch`- Diramazioni al Clone&Migrate flusso di lavoro.
- `createBackupImage`- Crea una AMI delle istanze di destinazione per fungere da backup.
- `launchInstanceInSameSubnet`- Avvia una nuova istanza dal backup AMI utilizzando la stessa configurazione dell'istanza di origine.
- `waitForClonedInstanceToPassStatusChecks`- Attende che l'istanza appena creata superi tutti i controlli di stato.
- `verifySSMConnectivityForClonedInstance`- Verifica che l'istanza appena creata sia gestita da Systems Manager.
- `checkAndInstallENADrivers`- Verifica se i driver ENA sono installati nell'istanza appena creata e installa i driver se necessario.
- `checkAndAddNVMEDrivers`- Verifica se i driver NVMe sono installati nell'istanza appena creata e installa i driver se necessario.
- `checkAndModifyFSTABEntries`- Controlla se i nomi dei dispositivi sono utilizzati `/etc/fstab` e, se necessario, li sostituisce con UUID.

- `stopClonedInstance`- Arresta l'istanza appena creata.
- `forceStopClonedInstance`- Force arresta l'istanza appena creata solo se il passaggio precedente non riesce a fermare l'istanza.
- `checkENAAttributeForClonedInstance`- Verifica se l'attributo di rete avanzato è attivato per l'istanza appena creata.
- `setNitroInstanceTypeForClonedInstance`- Cambia il tipo di istanza per l'istanza appena creata con il tipo di Nitro istanza specificato.
- `startClonedInstance`- Avvia l'istanza appena creata di cui è stato modificato il tipo di istanza.
- `approvalForCreatingImageAfterDriversInstallation`- Se l'istanza viene avviata correttamente come tipo di Nitro istanza, l'automazione attende l'approvazione dei responsabili richiesti. Se viene fornita l'approvazione, AMI viene creato un da utilizzare come GoldenAMI.
- `createImageAfterDriversInstallation`- Crea un AMI oggetto da usare come oroAMI.
- `endOfCloneAndMigrateBranch`- Fine della Clone&Migrate filiale
- `cleanupTestImage`- Annulla la registrazione dei dati AMI creati per il test.
- `failureHandling`- Verifica se hai scelto di terminare le risorse in caso di errore.
- `onFailureTerminateClonedInstance`- Termina l'istanza appena creata se l'automazione fallisce.
- `onFailurecleanupTestImage`- Annulla la registrazione dei dati AMI creati per il test.
- `onFailureApprovalToStartTargetInstance`- Se l'automazione fallisce, attende l'approvazione dei responsabili designati per avviare l'istanza di destinazione.
- `onFailureStartTargetInstance`- Se l'automazione fallisce, avvia l'istanza di destinazione.

Flusso di lavoro di FullMigration

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`

- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations
- ec2:DescribeInstances
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeImages
- ec2:CreateImage
- ec2:RunInstances
- ec2:DescribeInstanceStatus
- ec2:DeregisterImage
- ec2:DeleteSnapshot
- ec2:TerminateInstances
- ec2:StartInstances
- ec2:DescribeKeyPairs
- ec2:StopInstances
- kms:CreateGrant*
- kms:ReEncrypt
- ec2:ModifyInstanceAttribute
- ec2:DetachVolume
- ec2:AttachVolume
- ec2:DescribeVolumes
- autoscaling:DescribeAutoScalingInstances
- iam:PassRole
- ec2:CreateTags
- cloudformation:DescribeStackResources

Fasi del documento

Il `FullMigration` flusso di lavoro esegue gli stessi passaggi del `Clone&Migrate` flusso di lavoro e inoltre esegue i seguenti passaggi:

- `checkConcurrency`- Verifica che esista una sola automazione di questo runbook destinata all'istanza Amazon EC2 specificata. Se il runbook rileva un'altra automazione in corso destinata alla stessa istanza, l'automazione termina.
- `getTargetInstanceProperties`- Raccoglie i dettagli dall'istanza di destinazione.
- `checkRootVolumeTags`- Determina se il volume principale dell'istanza Amazon EC2 di destinazione contiene tag AWS riservati.
- `cloneTargetInstanceAndMigrateToNitro`- Avvia un'automazione per bambini utilizzando il `AWS-CloneXenInstanceToNitro` runbook.
- `branchOnTheOperationType`- Diramazioni in base al valore specificato per il `OperationType` parametro.
- `getClonedInstanceId`- Recupera l'ID dell'istanza appena avviata dall'automazione infantile.
- `checkIfRootVolumeIsBasedOnLVM`- Determina se la partizione root è gestita da LVM.
- `branchOnTheRootVolumeLVMStatus`- Se i responsabili ricevono le approvazioni minime richieste, l'automazione procede con la sostituzione del volume principale.
- `manualInstructionsInCaseOfLVM`- Se il volume root è gestito da LVM, l'automazione invia un output contenente istruzioni su come sostituire manualmente i volumi root.
- `startOfReplaceRootEBSVolumeBranch`- Avvia il flusso di lavoro Replace Root EBS Volume branch.
- `checkIfTargetInstanceIsManagedByCFN`- Determina se l'istanza di destinazione è gestita da uno AWS CloudFormation stack.
- `branchOnCFNStackStatus`- Rami in base allo stato dello CloudFormation stack.
- `approvalForRootVolumesReplacement(WithCFN)`- Se l'istanza di destinazione è stata lanciata daCloudFormation, l'automazione attende l'approvazione dopo il corretto avvio dell'istanza appena avviata come tipo di Nitro istanza. Quando vengono fornite le approvazioni, i volumi Amazon EBS dell'istanza di destinazione vengono sostituiti con i volumi root dell'istanza appena lanciata.
- `approvalForRootVolumesReplacement`- Attende l'approvazione dopo che l'istanza appena avviata viene avviata correttamente come tipo di Nitro istanza. Quando vengono fornite le approvazioni, i volumi Amazon EBS dell'istanza di destinazione vengono sostituiti con i volumi root dell'istanza appena lanciata.
- `assertIfTargetEC2InstanceIsStillStopped`- Verifica che l'istanza di destinazione sia in uno `stopped` stato prima di sostituire il volume principale.

- `stopTargetInstanceForRootVolumeReplacement`- Se l'istanza di destinazione è in esecuzione, l'automazione arresta l'istanza prima di sostituire il volume root.
- `forceStopTargetInstanceForRootVolumeReplacement`- La forza arresta l'istanza di destinazione se il passaggio precedente fallisce.
- `stopClonedInstanceForRootVolumeReplacement`- Interrompe l'istanza appena creata prima di sostituire i volumi Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- La forza arresta l'istanza appena creata se il passaggio precedente fallisce.
- `getBlockDeviceMappings`- Recupera le mappature dei dispositivi a blocchi sia per le istanze di destinazione che per quelle appena create.
- `replaceRootEbsVolumes`- Sostituisce il volume radice dell'istanza di destinazione con il volume radice dell'istanza appena creata.
- `EndOfReplaceRootEBSVolumeBranch`- Fine del flusso di lavoro Replace Root EBS Volume branch.
- `checkENAAttributeForTargetInstance`- Verifica se l'attributo Enhanced Networking (ENA) è attivato per l'istanza Amazon EC2 di destinazione.
- `enableENAAttributeForTargetInstance`- Attiva l'attributo ENA per l'istanza Amazon EC2 di destinazione, se necessario.
- `setNitroInstanceTypeForTargetInstance`- Cambia l'istanza di destinazione con il tipo di Nitro istanza specificato.
- `replicateRootVolumeTags`- Replica i tag sul volume principale di Amazon EBS dall'istanza Amazon EC2 di destinazione.
- `startTargetInstance`- Avvia l'istanza Amazon EC2 di destinazione dopo aver modificato il tipo di istanza.
- `onFailureStopTargetEC2Instance`- Arresta l'istanza Amazon EC2 di destinazione se non viene avviata come tipo di Nitro istanza.
- `onFailureForceStopTargetEC2Instance`- La forza arresta l'istanza Amazon EC2 di destinazione se il passaggio precedente fallisce.
- `OnFailureRevertOriginalInstanceType`- Ripristina l'istanza Amazon EC2 di destinazione al tipo di istanza originale se l'istanza di destinazione non viene avviata come tipo di Nitro istanza.
- `onFailureRollbackRootVolumeReplacement`- Annulla tutte le modifiche apportate `replaceRootEbsVolumes` passo dopo passo, se necessario.

- `onFailureApprovalToStartTargetInstance`- Attende l'approvazione del responsabile designato per avviare l'istanza Amazon EC2 di destinazione dopo aver annullato le modifiche precedenti.
- `onFailureStartTargetInstance`- Avvia l'istanza Amazon EC2 di destinazione.
- `terminateClonedEC2Instance`- Termina l'istanza Amazon EC2 clonata dopo aver sostituito il volume principale di Amazon EBS.

AWSSupport-ResetAccess

Descrizione

Questo runbook utilizzerà lo strumento EC2Rescue sull'istanza EC2 specificata per riattivare la decrittografia della password utilizzando la console EC2 (Windows) o per generare e aggiungere una nuova coppia di chiavi SSH (Linux). In caso di perdita della coppia di chiavi, questa automazione crea un'AMI abilitata mediante password che è possibile utilizzare per avviare una nuova istanza EC2 con una coppia personalizzata di chiavi (Windows).

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EC2 RescueInstanceType

  Tipo: String

  Valori validi: t2.small | t2.medium | t2.large

  Impostazione predefinita: t2.small

  Descrizione: (obbligatorio) tipo di istanza EC2 per l'istanza EC2Rescue. Dimensioni consigliate: t2.small.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza EC2 per la quale si desidera ripristinare l'accesso.

  > **Important**
  >
  > Systems Manager Automation interrompe questa istanza e crea un'AMI prima di tentare qualsiasi operazione. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- SubnetId

  Tipo: String

  Impostazione predefinita: CreateNew VPC

  Descrizione: (facoltativo) ID sottorete dell'istanza EC2Rescue. Per impostazione predefinita, Systems Manager Automation crea un nuovo VPC. In alternativa, utilizza SelectedInstanceSubnet per utilizzare la stessa sottorete della tua istanza o specifica un ID di sottorete personalizzato.

  > **Important**
  >
  > La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Devi avere almeno ssm:StartAutomationExecution, ssm: GetParameter (per recuperare il nome del parametro chiave SSH) e ssm: GetAutomationExecution per poter leggere l'output dell'automazione. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [`AWSSupport-StartEC2RescueWorkflow`].

Fasi del documento

1. `aws:assertAwsResourceProperty`- Afferma se l'istanza fornita è Windows.
   a. (EC2Rescue per Windows) Se l'istanza fornita è Windows:
      i. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con lo script di reimpostazione della password offline di EC2Rescue per Windows
      ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata
      iii. `aws:executeAwsApi`- Recupera l'ID AMI abilitato con password dall'automazione annidata
      iv. `aws:executeAwsApi`- Recupera il riepilogo di EC2Rescue dall'automazione annidata
   b. (EC2Rescue per Linux) Se l'istanza fornita è Linux:
      i. `aws:executeAutomation`- Invoca `AWSSupport-StartEC2RescueWorkflow` con lo script di iniezione di chiavi SSH offline EC2Rescue per Linux
      ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata
      iii. `aws:executeAwsApi`- Recupera il nome del parametro SSM per la chiave SSH iniettata
      iv. `aws:executeAwsApi`- Recupera il riepilogo di EC2Rescue dall'automazione annidata

Output

GetEC2RescueForWindowsResult. Uscita

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

GetEC2RescueForLinuxResult. Uscita

getLinuxBackupAmi. ImageId

getLinuxSSH .Name KeyParameter

AWSSupport-ResetLinuxUserPassword

Descrizione

Il `AWSSupport-ResetLinuxUserPassword` runbook consente di reimpostare la password di un utente del sistema operativo locale (OS). Questo runbook è particolarmente utile per gli utenti che devono accedere alle proprie istanze Amazon Elastic Compute Cloud EC2 (Amazon) utilizzando la console seriale. Il runbook crea un'EC2istanza Amazon temporanea nel tuo ruolo Account AWS e un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni per recuperare un valore AWS Secrets Manager segreto contenente la password.

Il runbook arresta l'EC2istanza Amazon di destinazione, scollega il volume root Amazon Elastic Block Store EBS (Amazon) e lo collega all'istanza Amazon temporanea. EC2 Utilizzando Run Command, viene eseguito uno script sull'istanza temporanea per impostare la password dell'utente del sistema operativo specificato. Quindi, il EBS volume Amazon root viene ricollegato all'istanza di destinazione. Il runbook offre anche la possibilità di creare un'istantanea del volume root all'inizio dell'automazione.

Prima di iniziare

Crea un segreto di Secrets Manager con il valore della password che desideri assegnare all'utente del tuo sistema operativo. Il valore deve essere in testo semplice. Per ulteriori informazioni, consulta Creazione di un segreto AWS Secrets Manager nella Guida per l'utente di AWS Secrets Manager .

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook. Considerate di impostare il valore del `CreateSnapshot` parametro come. **`Yes`**
- La modifica della password dell'utente locale richiede che il runbook interrompa l'istanza. Quando un'istanza viene arrestata, tutti i dati archiviati nella memoria o nei volumi dell'Instance Store vengono persi. Inoltre, tutti IPv4 gli indirizzi pubblici assegnati automaticamente vengono rilasciati. Per ulteriori informazioni su cosa succede quando interrompi un'istanza, consulta Arresta e avvia l'istanza nella Amazon EC2 User Guide.
- Se i EBS volumi Amazon collegati all'EC2istanza Amazon di destinazione sono crittografati con una chiave gestita dal cliente AWS Key Management Service (AWS KMS), assicurati che la AWS KMS chiave non lo sia, `deleted` `disabled` altrimenti l'istanza non si avvierà.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 Linux che contiene la password utente del sistema operativo che desideri reimpostare.
- LinuxUserName

  Tipo: stringa

  Impostazione predefinita: ec2-user

  Descrizione: (Facoltativo) L'account utente del sistema operativo di cui desideri reimpostare la password.
- SecretArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il segreto ARN del Secrets Manager contenente la nuova password.

- SecurityGroupId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID del gruppo di sicurezza da collegare all'EC2istanza Amazon temporanea. Se non fornisci un valore per questo parametro, viene utilizzato il gruppo di sicurezza Amazon Virtual Private Cloud (AmazonVPC) predefinito.

- SubnetId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID della sottorete in cui desideri avviare l'istanza EC2 temporanea di Amazon. Per impostazione predefinita, l'automazione sceglie la stessa sottorete dell'istanza di destinazione. Se si sceglie di fornire una sottorete diversa, questa deve trovarsi nella stessa zona di disponibilità dell'istanza di destinazione e avere accesso agli endpoint Systems Manager.

- CreateSnapshot

  Tipo: stringa

  Valori validi: Sì | No

  Impostazione predefinita: Sì

  Descrizione: (Facoltativo) Determina se viene creata un'istantanea del volume root dell'EC2istanza Amazon di destinazione prima dell'esecuzione dell'automazione.

- StopConsent

  Tipo: stringa

  Valori validi: Sì | No

  Predefinito: No

  Descrizione: inserisci **`Yes`** per confermare che l'EC2istanza Amazon di destinazione verrà interrotta durante questa automazione. Quando l'EC2istanza Amazon viene interrotta, tutti i dati archiviati nella memoria o nei volumi dell'instance store vengono persi e l'IPv4indirizzo pubblico automatico viene rilasciato. Per ulteriori informazioni, consulta Stop and start your istance nella Amazon EC2 User Guide.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeInstanceInformation`
- `ssm:ListTagsForResource`
- `ssm:SendCommand`
- `ec2:AttachVolume`
- `ec2:CreateSnapshot`
- `ec2:CreateSnapshots`
- `ec2:CreateVolume`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeSnapshotAttribute`
- `ec2:DescribeSnapshots`
- `ec2:DescribeSnapshotTierStatus`
- `ec2:DescribeVolumes`
- `ec2:DescribeVolumeStatus`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudformation:CreateStack`
- `cloudformation:DeleteStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStacks`
- `logs:CreateLogDelivery`

- `logs:CreateLogGroup`
- `logs:DeleteLogDelivery`
- `logs:DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`

Fasi del documento

1. `aws:branch`— Succursali a seconda che tu abbia fornito il consenso a interrompere l'EC2istanza Amazon di destinazione.
2. `aws:assertAwsResourceProperty`— Assicura che lo stato dell'EC2istanza Amazon sia in uno `stopped` stato `running` or. In caso contrario, l'automazione termina.
3. `aws:executeAwsApi`— Ottiene le proprietà dell'EC2istanza Amazon.
4. `aws:executeAwsApi`— Ottiene le proprietà del volume principale.
5. `aws:branch`— Suddivide l'automazione a seconda che sia stato fornito un ID di sottorete per l'EC2istanza Amazon temporanea.
6. `aws:assertAwsResourceProperty`— Assicura che la sottorete specificata nel `SubnetId` parametro si trovi nella stessa zona di disponibilità dell'EC2istanza Amazon di destinazione.
7. `aws:assertAwsResourceProperty`— Assicura che il volume root dell'EC2istanza Amazon di destinazione sia un EBS volume Amazon.
8. `aws:assertAwsResourceProperty`— Assicura che l'architettura dell'EC2istanza Amazon sia `arm64` o`x86_64`.
9. `aws:assertAwsResourceProperty`— Assicura che il comportamento di chiusura dell'EC2istanza Amazon sia corretto `stop` e non corretto. `terminate`
10. `aws:branch`— Assicura che l'EC2istanza Amazon non sia un'istanza Spot. Altrimenti, l'automazione termina.
11. `aws:executeScript`— Assicura che l'EC2istanza Amazon non faccia parte di un gruppo di auto scaling. Se l'istanza fa parte di un gruppo di auto scaling, l'automazione conferma che l'EC2istanza Amazon è in uno stato del `Standby` ciclo di vita.
12. `aws:createStack`— Crea un'EC2istanza Amazon temporanea che viene utilizzata per reimpostare la password per l'utente del sistema operativo specificato.

13. `aws:waitForAwsResourceProperty`— Attende l'esecuzione dell'EC2istanza Amazon temporanea appena lanciata.
14. `aws:executeAwsApi`— Ottiene l'ID dell'EC2istanza Amazon temporanea.
15. `aws:waitForAwsResourceProperty`— Attende che l'EC2istanza temporanea di Amazon venga segnalata come gestita da Systems Manager.
16. `aws:changeInstanceState`— Arresta l'EC2istanza Amazon di destinazione.
17. `aws:changeInstanceState`— Forza l'interruzione dell'EC2istanza Amazon di destinazione nel caso in cui rimanga bloccata in uno stato di arresto.
18. `aws:branch`— Suddivide l'automazione a seconda che sia stata richiesta un'istantanea del volume root dell'EC2istanza Amazon di destinazione.
19. `aws:executeAwsApi`— Crea un'istantanea del EBS volume Amazon root dell'EC2istanza Amazon di destinazione.
20. `aws:waitForAwsResourceProperty`— Attende che lo snapshot sia in uno stato. `completed`
21. `aws:executeAwsApi`— Scollega il volume EBS root di Amazon dall'EC2istanza Amazon di destinazione.
22. `aws:waitForAwsResourceProperty`— Attende che il volume EBS root di Amazon venga scollegato dall'istanza Amazon EC2 di destinazione.
23. `aws:executeAwsApi`— Collega il EBS volume Amazon root all'EC2istanza Amazon temporanea.
24. `aws:waitForAwsResourceProperty`— Attende che il volume EBS root di Amazon venga collegato all'EC2istanza Amazon temporanea.
25. `aws:runCommand`— Reimposta la password dell'utente di destinazione eseguendo uno script di shell utilizzando Run Command sull'EC2istanza temporanea di Amazon.
26. `aws:executeAwsApi`— Scollega il volume EBS root di Amazon dall'EC2istanza Amazon temporanea.
27. `aws:waitForAwsResourceProperty`— Attende che il volume EBS root di Amazon venga scollegato dall'istanza Amazon EC2 temporanea.
28. `aws:executeAwsApi`— Scollega il volume EBS root di Amazon dall'EC2istanza Amazon temporanea dopo un errore.
29. `aws:waitForAwsResourceProperty`— Attende che il volume EBS root di Amazon venga scollegato dall'EC2istanza Amazon temporanea dopo un errore.
30. `aws:branch`— Suddivide l'automazione a seconda che sia stata richiesta un'istantanea del volume root per determinare il percorso di ripristino in caso di errore.

31. `aws:executeAwsApi`— Ricollega il EBS volume Amazon root all'istanza Amazon EC2 di destinazione.
32. `aws:waitForAwsResourceProperty`— Attende che il volume EBS root di Amazon venga collegato all'EC2istanza Amazon.
33. `aws:executeAwsApi`— Crea un nuovo EBS volume Amazon dallo snapshot del volume root dell'EC2istanza Amazon di destinazione.
34. `aws:waitForAwsResourceProperty`— Attende che il nuovo EBS volume Amazon sia in uno `available` stato.
35. `aws:executeAwsApi`— Collega il nuovo EBS volume Amazon all'istanza di destinazione come volume root.
36. `aws:waitForAwsResourceProperty`— Attende che il EBS volume Amazon si trovi in uno `attached` stato.
37. `aws:executeAwsApi`— Descrive gli eventi AWS CloudFormation dello stack se i runbook non riescono a creare o aggiornare lo stack. AWS CloudFormation
38. `aws:branch`— Suddivide l'automazione in base allo stato precedente dell'EC2istanza Amazon. Se lo stato era`running`, l'istanza viene avviata. Se era in uno `stopped` stato, l'automazione continua.
39. `aws:changeInstanceState`— Avvia l'EC2istanza Amazon, se necessario.
40. `aws:waitForAwsResourceProperty`— Attende che lo AWS CloudFormation stack assuma lo stato di terminale prima di eliminarlo.
41. `aws:executeAwsApi`— Elimina lo AWS CloudFormation stack, inclusa l'istanza Amazon EC2 temporanea.

AWSPremiumSupport-ResizeNitroInstance

Descrizione

Il `AWSPremiumSupport-ResizeNitroInstance` runbook fornisce una soluzione automatizzata per il ridimensionamento delle istanze Amazon Elastic Compute Cloud (Amazon EC2) basate su Nitro System.

Per ridurre il potenziale rischio di perdita e downtime dei dati, il runbook verifica quanto segue:

- Comportamento di arresto dell'istanza.
- Se l'istanza fa parte di un gruppo Amazon EC2 Auto Scaling e in `standby` modalità.

- Stato dell'istanza e locazione.
- Il tipo di istanza che desideri modificare supporta il numero di interfacce di rete attualmente collegate all'istanza.
- L'architettura del processore e il tipo di virtualizzazione sia per il tipo di istanza corrente che per quello di destinazione sono gli stessi.
- Se l'istanza è in esecuzione, significa che sta superando tutti i controlli di stato.
- Il tipo di istanza da modificare è disponibile nella stessa zona di disponibilità.

Se Amazon EC2 non supera i controlli di stato dopo aver modificato il tipo di istanza, il runbook torna automaticamente al tipo di istanza precedente.

Per impostazione predefinita, questo runbook non modifica il tipo di istanza se è in esecuzione e i volumi dell'archivio delle istanze sono collegati. Inoltre, il runbook non cambierà il tipo di istanza se l'istanza fa parte di uno AWS CloudFormation stack. Se desiderate modificare uno di questi comportamenti, specificate `yes` i `AllowCloudFormationInstances` parametri `AllowInstanceStoreInstances` and.

Il runbook fornisce due modi diversi per specificare il tipo di istanza a cui si desidera passare:

- Per automazioni semplici destinate a una singola istanza, specifica il tipo di istanza che desideri modificare utilizzando il `TargetInstanceTypeFromParameter` parametro.
- Per eseguire automazioni su larga scala per modificare il tipo di istanza di più istanze, specifica il tipo di istanza utilizzando il `TargetInstanceTypeFromTagValue` parametro. Per informazioni sull'esecuzione di automazioni su larga scala, consulta Esegui automazioni su larga scala.

Se non specifichi un valore per nessuno dei due parametri, l'automazione fallisce.

> **Important**
>
> L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, consulta Confronta AWS Support i piani.

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook.

- Per informazioni sulla compatibilità per la modifica dei tipi di istanza, consulta Compatibilità per la modifica del tipo di istanza.
- Se l'automazione fallisce e torna al tipo di istanza originale, consulta Risoluzione dei problemi relativi alla modifica del tipo di istanza.
- La modifica del tipo di istanza richiede che il runbook interrompa l'istanza. Quando un'istanza viene interrotta, tutti i dati archiviati nella memoria o nei volumi di archiviazione di un'istanza vengono persi. Inoltre, vengono rilasciati tutti gli indirizzi IPv4 pubblici assegnati automaticamente. Per ulteriori informazioni su cosa succede quando interrompi un'istanza, consulta Interrompere e avviare l'istanza.
- Utilizzando il `SkipInstancesWithTagKey` parametro, puoi ignorare le istanze a cui è applicata una chiave tag Amazon EC2 specifica.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Accettare

  Tipo: String

Descrizione: (Obbligatorio) Entra **yes** per confermare che l'istanza verrà interrotta se è attualmente in esecuzione.

- AllowInstanceStoreInstances

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se specifichi`yes`, consenti l'esecuzione del runbook su istanze a cui sono associati volumi di archiviazione delle istanze.

- AllowCloudFormationInstances

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se si specifica`yes`, il runbook viene eseguito su istanze che fanno parte di uno AWS CloudFormation stack.

- DryRun

  Tipo: String

  Valori validi: no | sì

  Impostazione predefinita: no

  Descrizione: (Facoltativo) Se si specifica`yes`, il runbook convalida i requisiti di ridimensionamento senza apportare modifiche al tipo di istanza.

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 di cui desideri modificare il tipo.

- SkipInstancesWithTagKey

  Tipo: String

Descrizione: (Facoltativo) L'automazione ignora un'istanza di destinazione se la chiave di tag specificata viene applicata all'istanza.

- SleepTime

  Tipo: String

  Di default: 3

  Descrizione: (Facoltativo) Il numero di secondi in cui questo runbook dovrebbe dormire dopo il completamento.

- TagInstance

  Tipo: String

  Descrizione: (Facoltativo) Etichetta le istanze con la chiave e il valore di tua scelta utilizzando il seguente formato: *Key=ChangingType,* Value=True. Questa opzione consente di tenere traccia delle istanze che sono state prese di mira da questo runbook. i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;

- TargetInstanceTypeFromParameter

  Tipo: String

  Descrizione: (Facoltativo) Il tipo di istanza in cui desideri modificare l'istanza. Lasciate vuoto questo parametro se desiderate utilizzare il valore della chiave del tag fornita nel `TargetInstanceTypeFromTagValue` parametro.

- TargetInstanceTypeFromTagValue

  Tipo: String

  Descrizione: (Facoltativo) La chiave tag applicata alle istanze di destinazione il cui valore contiene il tipo di istanza che desideri modificare. Se si specifica un valore per il `TargetInstanceTypeFromParameter` parametro, questo sostituisce qualsiasi valore specificato per questo parametro.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- autoscaling:DescribeAutoScalingInstances
- cloudformation:DescribeStackResources
- ssm:GetAutomationExecution
- ssm:DescribeAutomationExecutions
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DescribeTags
- ec2:ModifyInstanceAttribute
- ec2:StartInstances
- ec2:StopInstances

Fasi del documento

1. aws:assertAwsResourceProperty: garantisce che l'istanza Amazon EC2 non sia contrassegnata con la chiave del tag di risorsa specificata nel SkipInstancesWithTagKey parametro. Se la chiave del tag viene trovata applicata all'istanza, il passaggio fallisce e l'automazione termina.
2. aws:assertAwsResourceProperty: conferma che lo stato dell'istanza Amazon EC2 di destinazione èrunning, pendingstopped, ostopping. Altrimenti, l'automazione termina.
3. aws:executeAwsApi: raccoglie le proprietà dall'istanza Amazon EC2.
4. aws:executeAwsApi: raccoglie dettagli sul tipo di istanza Amazon EC2 corrente.
5. aws:branch: verifica se il tipo di istanza corrente e il tipo di istanza specificato nel TargetInstanceTypeFromParameter parametro sono gli stessi. Se lo sono, l'automazione termina.
6. aws:assertAwsResourceProperty: assicura che l'istanza sia in esecuzione su Nitro System.
7. aws:branch: Assicura che il tipo di volume principale dell'istanza Amazon EC2 sia un volume Amazon Elastic Block Store (Amazon EBS).
8. aws:assertAwsResourceProperty: conferma che il comportamento di chiusura dell'istanza è stop e non lo è. terminate

9. `aws:branch`: Assicura che l'istanza Amazon EC2 non sia un'istanza Spot.
10. `aws:branch`: Assicura che la tenancy dell'istanza Amazon EC2 sia predefinita e non un host dedicato o un'istanza dedicata.
11. `aws:executeScript`: conferma che esiste una sola automazione di questo runbook destinata all'ID dell'istanza corrente. Se è già in corso un'altra automazione destinata alla stessa istanza, l'automazione restituisce un errore e termina.
12. `aws:branch`: ramifica l'automazione in base allo stato dell'istanza Amazon EC2.
    a. In caso contrario `stoppedstopping`, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino all'arresto completo dell'istanza Amazon EC2.
    b. In caso `running` `pending` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino a quando l'istanza Amazon EC2 non supera i controlli di stato.
13. `aws:assertAwsResourceProperty`: conferma che l'istanza Amazon EC2 non fa parte di un gruppo Auto Scaling richiamando l'operazione `DescribeAutoScalingInstances` API. Se l'istanza fa parte di un gruppo Auto Scaling, verifica che l'istanza Amazon EC2 sia in `standby` modalità.
14. `aws:branch`: ramifica l'automazione a seconda che tu voglia che l'automazione controlli se l'istanza Amazon EC2 fa parte di uno AWS CloudFormation stack:
    a. `aws:executeScript`Assicura che l'istanza Amazon EC2 non faccia parte di uno AWS CloudFormation stack richiamando l'operazione `DescribeStackResources` API.
15. `aws:executeAwsApi`: restituisce un elenco di tipi di istanza con lo stesso tipo di architettura del processore, lo stesso tipo di virtualizzazione e che supporta il numero di interfacce di rete attualmente collegate all'istanza di destinazione.
16. `aws:executeAwsApi`: ottiene il valore del tipo di istanza di destinazione dalla chiave del tag specificata nel `TargetInstanceTypeFromTagValue` parametro.
17. `aws:executeScript`: conferma che i tipi di istanza corrente e di destinazione sono compatibili. Assicura che il tipo di istanza di destinazione sia disponibile nella stessa sottorete. Verifica che il preside che ha avviato il runbook disponga delle autorizzazioni per modificare il tipo di istanza e arrestare e avviare l'istanza se era in esecuzione.
18. `aws:branch`: ramifica l'automazione in base al fatto che il valore del `DryRun` parametro sia impostato su`yes`. Se`yes`, l'automazione termina.
19. `aws:branch`: verifica se il tipo di istanza originale e quello di destinazione sono gli stessi. Se sono uguali, l'automazione termina.

20. `aws:executeAwsApi`: ottiene lo stato corrente dell'istanza.
21. `aws:changeInstanceState`: arresta l'istanza Amazon EC2.
22. `aws:changeInstanceState`: forza l'arresto dell'istanza se è bloccata nello `stopping` stato.
23. `aws:executeAwsApi`: cambia il tipo di istanza nel tipo di istanza di destinazione.
24. `aws:sleep`: attende 3 secondi dopo aver modificato il tipo di istanza per una maggiore coerenza.
25. `aws:branch`: ramifica l'automazione in base allo stato dell'istanza precedente. In caso affermativo`running`, l'istanza viene avviata.
    a. `aws:changeInstanceState`: avvia l'istanza Amazon EC2 se era in esecuzione prima di cambiare il tipo di istanza.
    b. `aws:waitForAwsResourceProperty`: attende che l'istanza Amazon EC2 superi i controlli di stato. Se l'istanza non supera i controlli di stato, viene ripristinata al tipo di istanza originale.
        i. `aws:changeInstanceState`: arresta l'istanza Amazon EC2 prima di cambiarla nel tipo di istanza originale.
        ii. `aws:changeInstanceState`: forza l'arresto dell'istanza Amazon EC2 prima di cambiarla nel tipo di istanza originale nel caso in cui rimanga bloccata in uno stato di arresto.
        iii. `aws:executeAwsApi`: modifica il tipo originale dell'istanza Amazon EC2.
        iv. `aws:sleep`: attende 3 secondi dopo aver modificato il tipo di istanza per una maggiore coerenza.
        v. `aws:changeInstanceState`: avvia l'istanza Amazon EC2 se era in esecuzione prima di cambiare il tipo di istanza.
        vi. `aws:waitForAwsResourceProperty`: attende che l'istanza Amazon EC2 superi i controlli di stato.
26. `aws:sleep`: Attende prima di terminare il runbook.

AWSSupport-RestoreEC2InstanceFromSnapshot

Descrizione

Il `AWSSupport-RestoreEC2InstanceFromSnapshot` runbook ti aiuta a identificare e ripristinare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) da uno snapshot funzionante di Amazon Elastic Block Store (Amazon EBS) del volume root.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EndDate

  Tipo: String

  Descrizione: (Facoltativo) L'ultima data in cui desideri che l'automazione cerchi un'istantanea.
- InplaceSwap

  Tipo: Booleano

  Valori validi: true | false

  Descrizione: (Facoltativo) Se il valore per questo parametro è impostato su`true`, il volume appena creato dall'istantanea sostituisce il volume radice esistente collegato all'istanza.
- InstanceId

  Tipo: String

  Descrizione: (Obbligatorio) L'ID dell'istanza che si desidera ripristinare da un'istantanea.
- LookForInstanceStatusCheck

  Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: true

Descrizione: (Facoltativo) Se il valore per questo parametro è impostato su`true`, l'automazione verifica se i controlli dello stato dell'istanza falliscono sulle istanze di test avviate dalle istantanee.

- SkipSnapshotsBy

  Tipo: String

  Descrizione: (Facoltativo) L'intervallo in cui le istantanee vengono ignorate durante la ricerca di istantanee per ripristinare l'istanza. Ad esempio, se sono disponibili 100 istantanee e si specifica un valore pari a 2 per questo parametro, viene esaminata ogni tre istantanee.

  Di default: 0
- SnapshotId

  Tipo: String

  Descrizione: (Facoltativo) L'ID di un'istantanea da cui si desidera ripristinare l'istanza.
- StartDate

  Tipo: String

  Descrizione: (Facoltativo) La prima data in cui desideri che l'automazione cerchi un'istantanea.
- TotalSnapshotsToLook

  Tipo: String

  Descrizione: (Facoltativo) Il numero di istantanee esaminate dall'automazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`

- ec2:AttachVolume
- ec2:CreateImage
- ec2:CreateTags
- ec2:CreateVolume
- ec2:DeleteTags
- ec2:DeregisterImage
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeImages
- ec2:DescribeSnapshots
- ec2:DescribeVolumes
- ec2:DetachVolume
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudwatch:GetMetricData

Fasi del documento

1. aws:executeAwsApi- Raccoglie dettagli sull'istanza di destinazione.
2. aws:assertAwsResourceProperty- Verifica l'esistenza dell'istanza di destinazione.
3. aws:assertAwsResourceProperty- Verifica che il volume principale sia un volume Amazon EBS.
4. aws:assertAwsResourceProperty- Verifica che non sia già in esecuzione un'altra automazione destinata a questa istanza.
5. aws:executeAwsApi- Contrassegna l'istanza di destinazione.
6. aws:executeAwsApi- Crea una AMI delle varianti.
7. aws:executeAwsApi- Raccoglie i dettagli relativi a ciò che AMI è stato creato nel passaggio precedente.

8. `aws:waitForAwsResourceProperty`- Aspetta che lo AMI stato diventi `available` prima di procedere.
9. `aws:executeScript`- Avvia una nuova istanza da quella appena creataAMI.
10. `aws:assertAwsResourceProperty`- Verifica che lo stato dell'istanza sia`available`.
11. `aws:executeAwsApi`- Raccoglie dettagli sull'istanza appena lanciata.
12. `aws:branch`- Diramazioni in base al fatto che sia stato fornito un valore per il `SnapshotId` parametro.
13. `aws:executeScript`- Restituisce un elenco di istantanee entro il periodo di tempo specificato.
14. `aws:executeAwsApi`- Arresta l'istanza.
15. `aws:waitForAwsResourceProperty`- Attende il raggiungimento dello stato del volume. `available`
16. `aws:waitForAwsResourceProperty`- Attende che sia lo stato dell'istanza. `stopped`
17. `aws:executeAwsApi`- Rimuove il volume della radice.
18. `aws:waitForAwsResourceProperty`- Attende che il volume della radice si stacchi.
19. `aws:executeAwsApi`- Collega il nuovo volume della radice.
20. `aws:waitForAwsResourceProperty`- Attende che il nuovo volume venga allegato.
21. `aws:executeAwsApi`- Avvia l'istanza.
22. `aws:waitForAwsResourceProperty`- Attende che sia lo stato dell'istanza. `available`
23. `aws:waitForAwsResourceProperty`- Attende il superamento dei controlli dello stato del sistema e dell'istanza per l'istanza.
24. `aws:executeScript`- Esegue uno script per trovare un'istantanea che può essere utilizzata per creare correttamente un volume.
25. `aws:executeScript`- Esegue uno script per ripristinare l'istanza utilizzando il volume appena creato dall'istantanea identificata dall'automazione o utilizzando il volume creato dall'istantanea specificata nel `SnapshotId` parametro.
26. `aws:executeScript`- Elimina le risorse create dall'automazione.

Output

launchCloneInstance.InstanceIds

ListSnapshotByDate. Istantanee finali

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot. Istantanea funzionante

InstanceRecovery.risultato

AWSSupport-SendLogBundleToS3Bucket

Descrizione

Il `AWSSupport-SendLogBundleToS3Bucket` runbook carica un pacchetto di log generato dallo strumento EC2Rescue dall'istanza di destinazione al bucket S3 specificato. Il runbook installa la versione specifica della piattaforma di EC2Rescue in base alla piattaforma dell'istanza di destinazione. EC2Rescue viene quindi utilizzato per raccogliere tutti i log del sistema operativo disponibili.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

Tipo: String

Descrizione: (obbligatorio) ID dell'istanza gestita di Windows o Linux da cui si desidera raccogliere i log.

- S3 BucketName

  Tipo: String

  Descrizione: (obbligatorio) bucket S3 in cui caricare i log.

- S3Path

  Tipo: String

  Predefinito:`AWSSupport-SendLogBundleToS3Bucket/`

  Descrizione: (facoltativo) percorso S3 per i log raccolti.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l'istanza EC2 che riceve il comando abbia un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. L'utente deve disporre almeno di ssm: StartAutomationExecution e ssm: SendCommand per eseguire l'automazione e inviare il comando all'istanza, oltre a ssm: GetAutomationExecution per poter leggere l'output dell'automazione.

Fasi del documento

1. `aws:runCommand`- Installare EC2Rescue tramite. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Esegui lo PowerShell script per raccogliere i log della risoluzione dei problemi di Windows con EC2Rescue.
3. `aws:runCommand`- Esegui lo script bash per raccogliere i log di risoluzione dei problemi di Linux con EC2Rescue.

Output

collectAndUploadWindowsLogBundle.Uscita

collectAndUploadLinuxLogBundle.Uscita

AWSSupport-StartEC2RescueWorkflow

Descrizione

Il `AWSSupport-StartEC2RescueWorkflow` runbook esegue lo script con codifica base64 fornito (Bash o Powershell) su un'istanza helper creata per salvare l'istanza. Il volume root dell'istanza è collegato e montato sull'istanza helper, nota anche come istanza. EC2Rescue Se l'istanza è Windows, specificare uno script Powershell. In caso contrario, utilizzare Bash. Il runbook imposta alcune variabili di ambiente che è possibile utilizzare nello script. Le variabili di ambiente contengono informazioni sull'input fornito, nonché informazioni sul volume root offline. Il volume offline è già montato e pronto all'uso. Ad esempio, è possibile salvare il file di configurazione dello stato desiderato in un volume root di Windows offline o eseguire il comando chroot e passare a un volume root di Linux offline ed eseguire la correzione offline.

Esegui questa automazione (console)

> **Important**
>
> EC2Le istanze Amazon create da Marketplace Amazon Machine Images (AMIs) non sono supportate da questa automazione.

Informazioni aggiuntive

Per applicare la codifica base64 a uno script, è possibile utilizzare Powershell o Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

Ecco un elenco di variabili di ambiente che è possibile utilizzare negli script offline, a seconda del sistema operativo di destinazione.

Windows:

Variabile	Descrizione	Valore di esempio
$env: _ _ID EC2RESCUE ACCOUNT	{{globale: ACCOUNT _ID}}	123456789012
$env: _ EC2RESCUE DATE	{{globale:DATE}}	2018-09-07
$env: _ _ EC2RESCUE DATE TIME	{{globale: DATE _TIME}}	2018-09-07_18.09.59
$env: _ _ EC2RESCUE EC2RW DIR	EC2Rescueper il percorso di installazione di Windows	C:\Program Files\ Amazon\ EC2Rescue
$ env: _ _ EC2RESCUE EC2RW DIR	EC2Rescueper il percorso di installazione di Windows	C:\Program Files\ Amazon\ EC2Rescue
$ env: _ _ID EC2RESCUE EXECUTION	{{automazione: EXECUTION _ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
$env: EC2RESCUE _ _ _ OFFLINE CURRENT CONTROL SET	Percorso dell'insieme di controlli corrente di Windows offline	`HKLM:\AWSTempSystem \ControlSet001`
$env: _ _ EC2RESCUE OFFLINE DRIVE	Lettera di unità di Windows offline	D:\
$env: _ _ _ EC2RESCUE OFFLINE EBS DEVICE	Dispositivo con volume root offline EBS	xvdf
$env: EC2RESCUE _ _ _ OFFLINE KERNEL VER	Versione del kernel di Windows offline	6.1.7601.24214
$env: _ _OS_ EC2RESCUE OFFLINE ARCHITECTURE	Architettura di Windows offline	AMD64
$env: _ _OS_ EC2RESCUE OFFLINE CAPTION	Didascalia di Windows offline	Windows Server 2008 R2 Datacenter

Variabile	Descrizione	Valore di esempio
$env: _ _OS_ EC2RESCUE OFFLINE TYPE	Tipo di sistema operativo Windows offline	Server
$env: _ _ _ EC2RESCUE OFFLINE PROGRAM FILES DIR	Percorso della directory dei file di programma di Windows offline	D:\Program Files
$env: EC2RESCUE _ _ _ _X86_ OFFLINE PROGRAM FILES DIR	Percorso della directory dei file di programma x86 di Windows offline	D:\Program Files (x86)
$env: _ _ _ EC2RESCUE OFFLINE REGISTRY DIR	Percorso della directory del Registro di sistema di Windows offline	D:\Windows\System32\config
$env: _ _ _ EC2RESCUE OFFLINE SYSTEM ROOT	Percorso della directory radice di sistema di Windows offline	D:\Windows
$env: _ EC2RESCUE REGION	{{globale:REGION}}	us-west-1
$env: _S3_ EC2RESCUE BUCKET	{{S3}} BucketName	bucket dimostrativo amzn-s3
$env: _S3_ EC2RESCUE PREFIX	{{ S3Prefix }}	myprefix/
$env: EC2RESCUE _ _ SOURCE INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$ script: _ _ _ EC2RESCUE OFFLINE WINDOWS INSTALL	Metadati di installazione di Windows offline	Oggetto Powershell del cliente

Linux:

Variabile	Descrizione	Valore di esempio
EC2RESCUE_ _ID ACCOUNT	{{globale: ACCOUNT _ID}}	123456789012
EC2RESCUE_DATE	{{globale:DATE}}	2018-09-07
EC2RESCUE_DATE_TIME	{{globale: DATE _TIME}}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	EC2Rescueper il percorso di installazione di Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_ EXECUTION _ID	{{automazione: EXECUTION _ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_ DEVICE	Nome del dispositivo offline	/dev/xvdf1
EC2RESCUE_OFFLINE_ EBS_DEVICE	Dispositivo con volume EBS root offline	/dev/sdf
EC2RESCUE_OFFLINE_ SYSTEM_ROOT	Punto di montaggio del volume radice offline	/mnt/mount
EC2RESCUE_PYTHON	Versione di Python	python2.7
EC2RESCUE_REGION	{{global:REGION}}	us-west-1
EC2RESCUE_S3_ BUCKET	{{S3}} BucketName	bucket dimostrativo amzn-s3
EC2RESCUE_S3_ PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_I NSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AMIPrefix

  Tipo: stringa

  Impostazione predefinita: `AWSSupport-EC2Rescue`

  Descrizione: (Facoltativo) Un prefisso per il AMI nome del backup.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CreatePostEC2RescueBackup

  Tipo: stringa

  Valori validi: true | false

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Impostalo su per `true` creare un file AMI di InstanceId dopo aver eseguito lo script, prima di avviarlo. AMIPersisterà dopo il completamento dell'automazione. È responsabilità dell'utente garantire l'accesso al AMI file o eliminarlo.

- CreatePreEC2RescueBackup

  Tipo: stringa

  Valori validi: true | false

  Impostazione predefinita: false

Descrizione: (Facoltativo) Impostalo `true` per creare un AMI of InstanceId prima di eseguire lo script. AMIPersisterà dopo il completamento dell'automazione. È responsabilità dell'utente garantire l'accesso al AMI file o eliminarlo.

- EC2RescueInstanceType

  Tipo: stringa

  Valori validi: t2.small | t2.medium | t2.large

  Impostazione predefinita: t2.small

  Descrizione: (Facoltativo) Il tipo di istanza per l'istanzaEC2. EC2Rescue

- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) ID dell'EC2istanza. IMPORTANT: AWS Systems Manager L'automazione interrompe questa istanza. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- OfflineScript

  Tipo: stringa

  Descrizione: (obbligatorio) script con codifica Base64 da eseguire sull'istanza helper. Usa Bash se la tua istanza di origine è Linux e PowerShell se è Windows.

- S3 BucketName

  Tipo: stringa

  Descrizione: (facoltativo) nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- S3Prefix

  Tipo: stringa

  Impostazione predefinita: `AWSSupport-EC2Rescue`

  Descrizione: (facoltativo) prefisso dei log S3.

- SubnetId

  Tipo: stringa

  Predefinito: SelectedInstanceSubnet

  Descrizione: (Facoltativo) L'ID di sottorete per l'EC2Rescueistanza. Per impostazione predefinita, viene utilizzata la stessa sottorete in cui si trova l'istanza specificata. IMPORTANT: Se si fornisce una sottorete personalizzata, questa deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint. SSM

- UniqueId

  Tipo: stringa

  Impostazione predefinita: {{automation: EXECUTION _ID}}

  Descrizione: (Facoltativo) Un identificatore univoco per l'automazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia all'utente che esegue l'automazione di avere allegata la policy IAM gestita A mazonSSMAutomation Role. Oltre a tale policy l'utente deve disporre di quanto segue:

```
{
                "Version": "2012-10-17",
                "Statement": [
                   {
                      "Action": [
                         "lambda:InvokeFunction",
                         "lambda:DeleteFunction",
                         "lambda:GetFunction"
                      ],
                      "Resource": "arn:aws:lambda:*:An-AWS-Account-
ID:function:AWSSupport-EC2Rescue-*",
                      "Effect": "Allow"
                   },
                   {
                      "Action": [
                         "s3:GetObject",
```

```
                        "s3:GetObjectVersion"
                    ],
                    "Resource": [
                        "arn:aws:s3:::awssupport-ssm.*/*.template",
                        "arn:aws:s3:::awssupport-ssm.*/*.zip"
                    ],
                    "Effect": "Allow"
                },
                {
                    "Action": [
                        "iam:CreateRole",
                        "iam:CreateInstanceProfile",
                        "iam:GetRole",
                        "iam:GetInstanceProfile",
                        "iam:PutRolePolicy",
                        "iam:DetachRolePolicy",
                        "iam:AttachRolePolicy",
                        "iam:PassRole",
                        "iam:AddRoleToInstanceProfile",
                        "iam:RemoveRoleFromInstanceProfile",
                        "iam:DeleteRole",
                        "iam:DeleteRolePolicy",
                        "iam:DeleteInstanceProfile"
                    ],
                    "Resource": [
                        "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
                        "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport-
EC2Rescue-*"
                    ],
                    "Effect": "Allow"
                },
                {
                    "Action": [
                        "lambda:CreateFunction",
                        "ec2:CreateVpc",
                        "ec2:ModifyVpcAttribute",
                        "ec2:DeleteVpc",
                        "ec2:CreateInternetGateway",
                        "ec2:AttachInternetGateway",
                        "ec2:DetachInternetGateway",
                        "ec2:DeleteInternetGateway",
                        "ec2:CreateSubnet",
                        "ec2:DeleteSubnet",
                        "ec2:CreateRoute",
```

```
                    "ec2:DeleteRoute",
                    "ec2:CreateRouteTable",
                    "ec2:AssociateRouteTable",
                    "ec2:DisassociateRouteTable",
                    "ec2:DeleteRouteTable",
                    "ec2:CreateVpcEndpoint",
                    "ec2:DeleteVpcEndpoints",
                    "ec2:ModifyVpcEndpoint",
                    "ec2:Describe*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
```

Fasi del documento

1. `aws:executeAwsApi`- Descrivi l'istanza fornita
2. `aws:executeAwsApi`- Descrivi il volume principale dell'istanza fornita
3. `aws:assertAwsResourceProperty`- Verifica che il tipo di dispositivo del volume principale sia EBS
4. `aws:assertAwsResourceProperty`- Verifica che il volume root non sia crittografato
5. `aws:assertAwsResourceProperty`- Controlla l'ID di sottorete fornito
   a. (Usa la sottorete dell'istanza corrente) - Se * SubnetId = SelectedInstanceSubnet *, esegui `aws:createStack` per distribuire lo stack EC2Rescue CloudFormation
   b. (Crea nuovoVPC) - Se * SubnetId = CreateNew VPC * allora esegui `aws:createStack` per distribuire lo stack EC2Rescue CloudFormation
   c. (Utilizzo della sottorete personalizzata): in tutti gli altri casi:

      `aws:assertAwsResourceProperty`- Verifica che la sottorete fornita si trovi nella stessa zona di disponibilità dell'istanza fornita

      `aws:createStack`- Distribuisci lo stack EC2Rescue CloudFormation
6. `aws:invokeLambdaFunction`- Esegui una convalida aggiuntiva degli input
7. `aws:executeAwsApi`- Aggiorna lo EC2Rescue CloudFormation stack per creare l'EC2Rescueistanza helper

8. `aws:waitForAwsResourceProperty`- Attendi il completamento dell'aggiornamento EC2Rescue CloudFormation dello stack
9. `aws:executeAwsApi`- Descrivi l'output EC2Rescue CloudFormation dello stack per ottenere l'ID dell'istanza EC2Rescue helper
10. `aws:waitForAwsResourceProperty`- Attendi che l'istanza EC2Rescue helper diventi un'istanza gestita
11. `aws:changeInstanceState`- Arresta l'istanza fornita
12. `aws:changeInstanceState`- Arresta l'istanza fornita
13. `aws:changeInstanceState`- Arresta forzatamente l'istanza fornita
14. `aws:assertAwsResourceProperty`- Controlla il valore CreatePre EC2RescueBackup di input
    a. (Crea un EC2Rescue pre-backup) - If* CreatePre EC2RescueBackup = true*
    b. `aws:executeAwsApi`- Crea un AMI backup dell'istanza fornita
    c. `aws:createTags`- Etichetta il AMI backup
15. `aws:runCommand`- Installa EC2Rescue sull'istanza EC2Rescue helper
16. `aws:executeAwsApi`- Scollega il volume root dall'istanza fornita
17. `aws:assertAwsResourceProperty`- Controlla la piattaforma di istanza fornita
    a. (L'istanza è Windows):

       `aws:executeAwsApi`- Collega il volume root all'istanza EC2Rescue helper come *xvdf*

       `aws:sleep`- Dormi 10 secondi

       `aws:runCommand`- Esegui lo script offline fornito in Powershell
    b. (L'istanza è Linux):

       `aws:executeAwsApi`- Collega il volume root EC2Rescue all'istanza di supporto come */dev/sdf*

       `aws:sleep`- Dormi 10 secondi

       `aws:runCommand`- Esegui lo script offline fornito in Bash
18. `aws:changeInstanceState`- Interrompi l'istanza EC2Rescue helper
19. `aws:changeInstanceState`- Arresta forzatamente l'istanza EC2Rescue helper
20. `aws:executeAwsApi`- Stacca il volume root dall'istanza helper EC2Rescue

21. `aws:executeAwsApi`- Ricollega il volume root all'istanza fornita
22. `aws:assertAwsResourceProperty`- Controlla il valore CreatePost EC2RescueBackup di input
    a. (Crea un EC2Rescue post-backup) - If* CreatePost EC2RescueBackup = true*
    b. `aws:executeAwsApi`- Crea un AMI backup dell'istanza fornita
    c. `aws:createTags`- Etichetta il AMI backup
23. `aws:executeAwsApi`- Ripristina l'eliminazione iniziale allo stato di terminazione per il volume principale dell'istanza fornita
24. `aws:changeInstanceState`- Ripristina lo stato iniziale dell'istanza fornita (in esecuzione/interrotta)
25. `aws:deleteStack`- Elimina lo stack EC2Rescue CloudFormation

Output

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descrizione

Il `AWSPremiumSupport-TroubleshootEC2DiskUsage` runbook ti aiuta a indagare e potenzialmente a risolvere i problemi relativi all'utilizzo del disco root e non root delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Se possibile, il runbook tenta di risolvere i problemi estendendo il volume e il relativo file system. Per eseguire queste attività, questo runbook orchestra l'esecuzione di diversi runbook in base al sistema operativo dell'istanza interessata.

Il primo runbook, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` o`AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, determina se i problemi del disco possono essere mitigati espandendo il volume.

Il secondo runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` o`AWSPremiumSupport-ExtendVolumesOnLinux`, utilizza l'output del primo runbook per eseguire codice Python che

modifica il volume. Dopo la modifica del volume, il runbook estende la partizione e il file system dei volumi interessati.

> **Important**
>
> L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, consulta Confronta AWS Support i piani.

Questo documento è stato creato in collaborazione con AWS Managed Services (AMS). AMS ti aiuta a gestire la tua AWS infrastruttura in modo più efficiente e sicuro. AMS offre inoltre flessibilità operativa, sicurezza e conformità migliorate, ottimizzazione della capacità e identificazione con riduzione dei costi. Per ulteriori informazioni, consulta AWS Managed Services.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- InstanceId

  Tipo: String

  Valori consentiti: ^i- [a-z0-9] {8,17} $

  Descrizione: (obbligatorio) ID della tua istanza Amazon EC2.
- VolumeExpansionEnabled

  Tipo: Booleano

  Descrizione: (Facoltativo) Contrassegna per controllare se il documento estenderà i volumi e le partizioni interessati.

Impostazione predefinita: true

- VolumeExpansionUsageTrigger

  Tipo: String

  Descrizione: (Facoltativo) Utilizzo minimo dello spazio della partizione richiesto per attivare l'estensione (in percentuale).

  Valori consentiti: ^ [0-9] {1,2} $

  Predefinito: 85

- VolumeExpansionCapSize

  Tipo: String

  Descrizione: (Facoltativo) Dimensione massima a cui verrà aumentato il volume di Amazon Elastic Block Store (Amazon EBS) (in GiB).

  Valori consentiti: ^ [0-9] {1,4} $

  Predefinito: 2048

- VolumeExpansionGibIncrease

  Tipo: String

  Descrizione: (Facoltativo) Aumento di GiB del volume. Verrà utilizzato l'aumento netto maggiore tra VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease verrà utilizzato.

  Valori consentiti: ^ [0-9] {1,4} $

  Di default: 20

- VolumeExpansionPercentageIncrease

  Tipo: String

  Descrizione: (Facoltativo) Aumento della percentuale del volume. Verrà utilizzato l'aumento netto maggiore tra VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease verrà utilizzato.

  Valori consentiti: ^ [0-9] {1,2} $

Di default: 20

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeVolumes`
- `ec2:DescribeVolumesModifications`
- `ec2:ModifyVolume`
- `ec2:DescribeInstances`
- `ec2:CreateImage`
- `ec2:DescribeImages`
- `ec2:DescribeTags`
- `ec2:CreateTags`
- `ec2:DeleteTags`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeAutomationExecutions`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`

Fasi del documento

1. `aws:assertAwsResourceProperty`- Controlla se l'istanza è gestita da Systems Manager
2. `aws:executeAwsApi`- Descrive l'istanza per accedere alla piattaforma.
3. `aws:branch`- Automazione delle filiali basata sulla piattaforma dell'istanza.
   a. Se l'istanza è Windows:
      i. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` runbook per diagnosticare i problemi di utilizzo del disco sull'istanza.
      ii. `aws:executeAwsApi`- Ottiene l'output dell'automazione precedente.
      iii. `aws:branch`- Filiali in base all'output della diagnostica e in presenza di volumi che possono essere espansi per mitigare l'avviso.
         A. Non ci sono volumi da espandere: basta con l'automazione.
         B. Ci sono volumi che devono essere ampliati:
            I. `aws:executeAwsApi`- Crea una Amazon Machine Image (AMI) dell'istanza.
            II. `aws:waitForAwsResourceProperty`- Aspetta che lo AMI stato lo sia. `available`
            III. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-ExtendVolumesOnWindows` runbook per eseguire la modifica del volume e i passaggi necessari nel sistema operativo (OS) per rendere disponibile il nuovo spazio.
   b. (La piattaforma non è Windows) Se l'istanza di input non è Windows:
      i. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` runbook per diagnosticare i problemi di utilizzo del disco sull'istanza.
      ii. `aws:executeAwsApi`- Ottiene l'output dell'automazione precedente.
      iii. `aws:branch`- Filiali in base all'output della diagnostica e in presenza di volumi che possono essere espansi per mitigare l'avviso.
         A. Non ci sono volumi da espandere: basta con l'automazione.
         B. Ci sono volumi che devono essere ampliati:
            I. `aws:executeAwsApi`- Crea una AMI delle istanze.
            II. `aws:waitForAwsResourceProperty`- Aspetta che lo AMI stato sia. `available`
            III. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-ExtendVolumesOnLinux` runbook per eseguire la modifica del volume e i passaggi necessari nel sistema operativo per rendere disponibile il nuovo spazio.

Output

diagnoseDiskUsageAlertOnWindows.Uscita

extendVolumesOnWindows. Uscita

diagnoseDiskUsageAlertOnLinux.Uscita

extendVolumesOnUscita Linux

Esegui il backup di AmiLinux. ImageId

Esegui il backup su Windows. ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Descrizione

`AWSSupport-TroubleshootEC2InstanceConnect`l'automazione aiuta ad analizzare e rilevare gli errori che impediscono la connessione a un'istanza Amazon Elastic Compute Cloud (AmazonEC2) utilizzando Amazon EC2 Instance Connect. Identifica i problemi causati da Amazon Machine Image (AMI) non supportata, installazione o configurazione di pacchetti a livello di sistema operativo mancanti, autorizzazioni mancanti AWS Identity and Access Management (IAM) o problemi di configurazione di rete.

Come funziona?

Il runbook richiede l'ID dell'EC2istanza Amazon, il nome utente, la modalità di connessione, l'IP di origineCIDR, la SSH porta e Amazon Resource Name (ARN) per il IAM ruolo o l'utente che riscontra problemi con Amazon EC2 Instance Connect. Verifica quindi i prerequisiti per la connessione a un'EC2istanza Amazon utilizzando Amazon EC2 Instance Connect:

- L'istanza è in esecuzione ed è integra.
- L'istanza si trova in una AWS regione supportata da Amazon EC2 Instance Connect.
- AMIdell'istanza è supportata da Amazon EC2 Instance Connect.
- L'istanza può raggiungere l'Instance Metadata Service (IMDSv2).
- Il pacchetto Amazon EC2 Instance Connect è installato e configurato correttamente a livello di sistema operativo.
- La configurazione di rete (gruppi di sicurezzaACL, rete e regole della tabella di routing) consente la connessione all'istanza tramite Amazon EC2 Instance Connect.

- Il IAM ruolo o l'utente utilizzato per sfruttare Amazon EC2 Instance Connect ha accesso alle chiavi push per l'EC2istanza Amazon.

> **Important**
>
> - Per verificare l'istanzaAMI, IMDSv2 la raggiungibilità e l'installazione del pacchetto Amazon EC2 Instance Connect, l'istanza deve essere SSM gestita. Altrimenti, salta questi passaggi. Per ulteriori informazioni, consulta Perché la mia EC2 istanza Amazon non viene visualizzata come nodo gestito.
> - Il controllo della rete rileverà solo se il gruppo di sicurezza e ACL le regole di rete bloccano il traffico quando SourceIp CIDR viene fornito come parametro di input. Altrimenti, mostrerà solo le regole SSH relative.
> - Le connessioni che utilizzano Amazon EC2 Instance Connect Endpoint non sono convalidate in questo runbook.
> - Per le connessioni private, l'automazione non verifica se il SSH client è installato sulla macchina di origine e se può raggiungere l'indirizzo IP privato dell'istanza.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`

- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a AWSSupport-TroubleshootEC2InstanceConnectnella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - InstanceId (Obbligatorio):

     L'ID dell'EC2istanza Amazon di destinazione a cui non sei riuscito a connetterti utilizzando Amazon EC2 Instance Connect.
   - AutomationAssumeRole (Facoltativo):

     Il ARN IAM ruolo che consente a Systems Manager Automation di eseguire le azioni per conto dell'utente. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - Nome utente (obbligatorio):

     Il nome utente utilizzato per connettersi all'EC2istanza Amazon tramite Amazon EC2 Instance Connect. Viene utilizzato per valutare se IAM l'accesso è concesso a questo particolare utente.
   - EC2InstanceConnectRoleOrUser(Obbligatorio):

     Il IAM ruolo o ARN l'utente che utilizza Amazon EC2 Instance Connect per inviare le chiavi all'istanza.
   - SSHPort(Facoltativo):

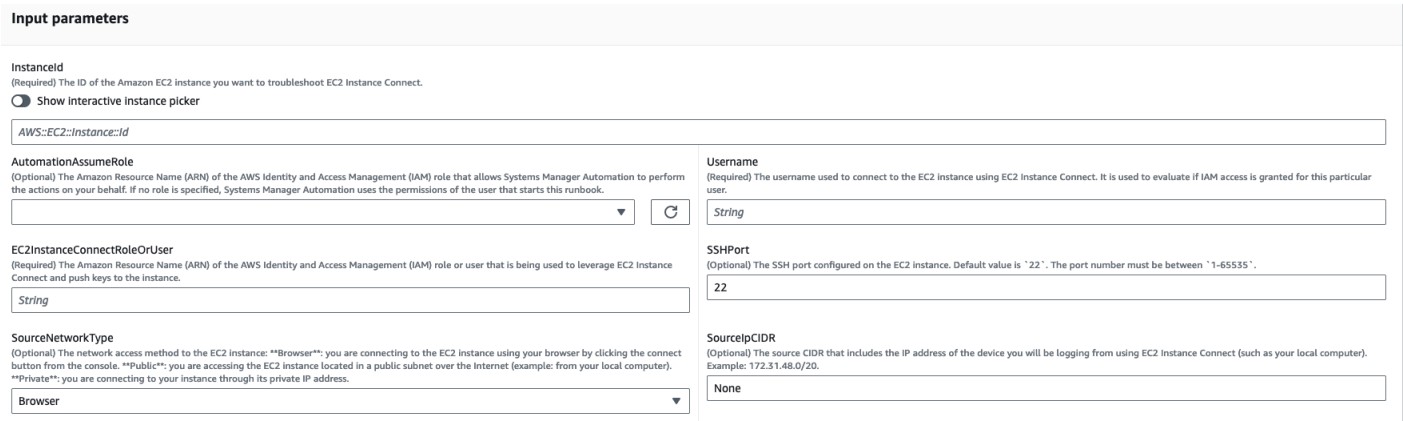
La SSH porta configurata sull'EC2istanza Amazon. Il valore predefinito è 22. Il numero di porta deve essere compreso tra1-65535.

- SourceNetworkType (Facoltativo):

  Il metodo di accesso alla rete all'EC2istanza Amazon:

  - Browser: ti connetti dalla console AWS di gestione.
  - Pubblica: ti connetti all'istanza situata in una sottorete pubblica su Internet (ad esempio, il computer locale).
  - Privato: ti connetti tramite l'indirizzo IP privato dell'istanza.
- SourceIpCIDR(Facoltativo):

  La fonte CIDR che include l'indirizzo IP del dispositivo (ad esempio il computer locale) da cui effettuerai l'accesso utilizzando Amazon EC2 Instance Connect. Esempio: 172.31.48.6/32. Se non viene fornito alcun valore con la modalità di accesso pubblico o privato, il runbook non valuterà se il gruppo di sicurezza dell'EC2istanza Amazon e ACL le regole di rete consentono il SSH traffico. Mostrerà invece SSH le regole relative.



4. Seleziona Esegui.
5. L'automazione inizia.
6. Il documento esegue le seguenti operazioni:

   - AssertInitialState:

     Assicura che lo stato dell'EC2istanza Amazon sia in esecuzione. Altrimenti, l'automazione termina.
   - GetInstanceProperties:

Ottiene le proprietà correnti dell'EC2istanza Amazon (PlatformDetails PublicIpAddress, VpcId, SubnetId e MetadataHttpEndpoint).

- GatherInstanceInformationFromSSM:

  Ottiene lo stato del ping dell'istanza di Systems Manager e i dettagli del sistema operativo se l'istanza è SSM gestita.

- CheckIfAWSRegionSupported:

  Verifica se l'EC2istanza Amazon si trova in una AWS regione supportata da Amazon EC2 Instance Connect.

- BranchOnIfAWSRegionSupported:

  Continua l'esecuzione se la AWS regione è supportata da Amazon EC2 Instance Connect. Altrimenti, crea l'output ed esce dall'automazione.

- CheckIfInstanceAMIIsSupported:

  Verifica se l'elemento AMI associato all'istanza è supportato da Amazon EC2 Instance Connect.

- BranchOnIfInstanceAMIIsSupported:

  Se l'istanza AMI è supportata, esegue i controlli a livello di sistema operativo, come la raggiungibilità dei metadati e l'installazione e la configurazione del pacchetto Amazon EC2 Instance Connect. Altrimenti, verifica se i HTTP metadati sono abilitati all'utilizzo AWS API, quindi passa alla fase di controllo della rete.

- C: heckIMDSReachability FromOs

  Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se è in grado di raggiungere ilIMDSv2.

- heckEICPackageInstallazione C:

  Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se il pacchetto Amazon EC2 Instance Connect è installato e configurato correttamente.

- C: heckSSHConfig FromOs

  Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se la SSH porta configurata corrisponde al parametro di input `. SSHPort `

- CheckMetadataHTTPEndpointIsEnabled:

Verifica se l'HTTPendpoint del servizio di metadati dell'istanza è abilitato.

- Accesso C: heckEICNetwork

  Verifica se la configurazione di rete (gruppi di sicurezzaACL, rete e regole della tabella di routing) consente la connessione all'istanza tramite Amazon EC2 Instance Connect.

- C heckIAMRoleOrUserPermissions:

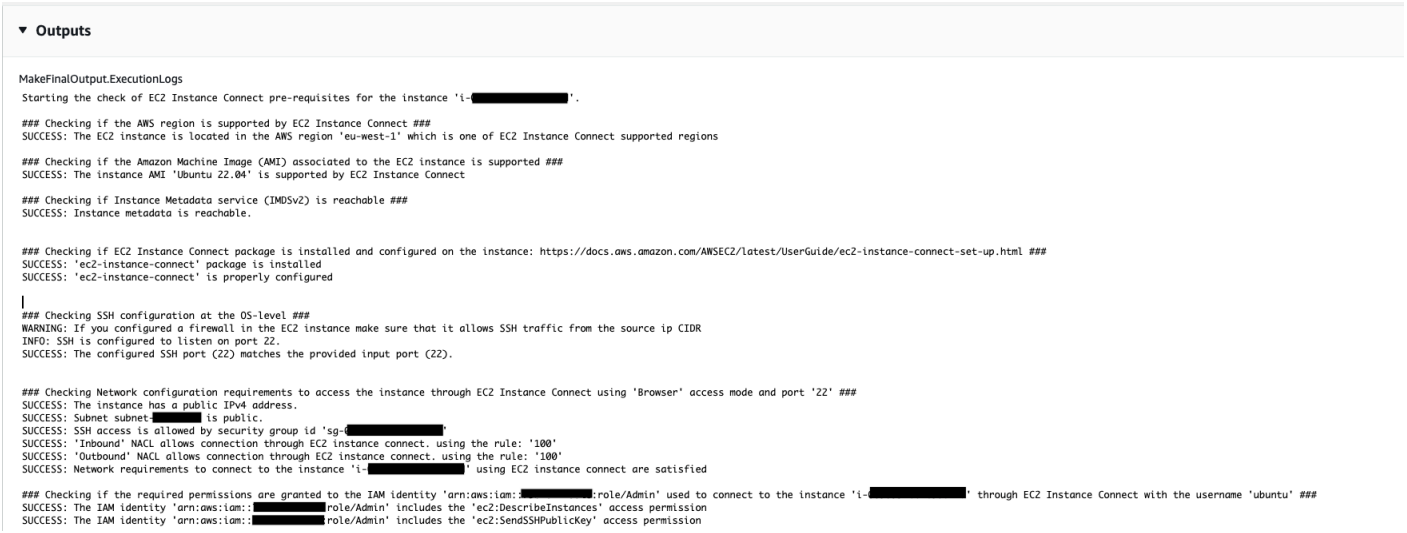
  Verifica se il IAM ruolo o l'utente utilizzato per sfruttare Amazon EC2 Instance Connect ha accesso alle chiavi push per l'EC2istanza Amazon utilizzando il nome utente fornito.

- MakeFinalOutput:

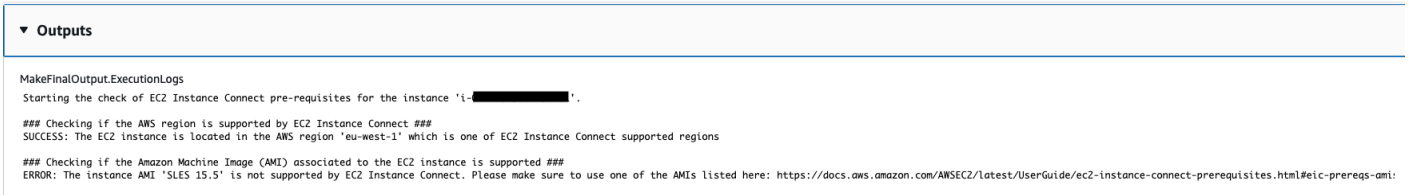
  Consolida l'output di tutti i passaggi precedenti.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

   Esecuzione in cui l'istanza di destinazione presenta tutti i prerequisiti richiesti:



   Esecuzione in cui l'istanza AMI di destinazione non è supportata:



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Come posso risolvere i problemi di connessione alla mia istanza Amazon utilizzando Amazon EC2 Instance EC2 Connect?

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Descrizione

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`il runbook di automazione viene utilizzato per rilevare errori comuni durante l'installazione degli agenti di replica AWS Application Migration Service (AWS MGN) e AWS Elastic Disaster Recovery (AWS DRS) nei server Linux per migrare i server di origine sul cloud. AWS

Come funziona?

Il runbook utilizza il `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs` percorso Amazon Simple Storage Service (Amazon S3) in cui il log `aws_replication_agent_installer.log` di AWS DRS installazione AWS MGN o viene caricato come parametro. Quindi, esegue le seguenti attività:

- Convalida: verifica se il file di registro fornito è valido e che contenga almeno un'installazione dell'agente.
- Analisi: analizza accuratamente l'installazione dell'agente più recente nel file di registro per individuare eventuali errori o errori noti AWS MGN. AWS DRS
- Rilevamento e risoluzione degli errori: in base all'analisi, rileva ed elenca eventuali errori o problemi durante il processo di installazione dell'agente. Per ogni errore rilevato, il runbook fornisce passaggi dettagliati per aiutare a risolvere o mitigare il problema.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `s3:GetObject`
- `s3:ListBucket`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo):

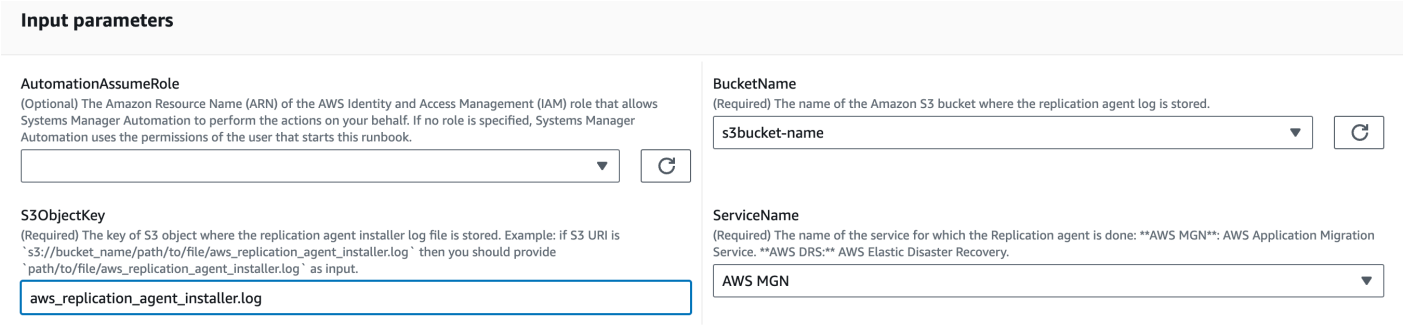
     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - BucketName (Obbligatorio):

     Il nome del bucket Amazon S3 in cui è archiviato il log dell'agente di replica.
   - S3 (richiesto): ObjectKey

La chiave dell'oggetto Amazon S3 in cui è archiviato il file di registro del programma di installazione dell'agente di replica. Esempio: se Amazon S3 lo URI è`s3://bucket_name/path/to/file/aws_replication_agent_installer.log`, allora dovresti inserire. `path/to/file/aws_replication_agent_installer.log`

- ServiceName (Obbligatorio):

  Il nome del servizio per il quale è installato l'agente di replica. Valori consentiti: `AWS MGN` o `AWS DRS`



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:

   - **`ValidateInput`**

     Assicura che il file di registro dell'agente di replica sia valido e accessibile utilizzando il nome e il percorso del bucket Amazon S3 forniti all'oggetto, quindi restituisce il numero di byte dell'ultima installazione dell'agente.

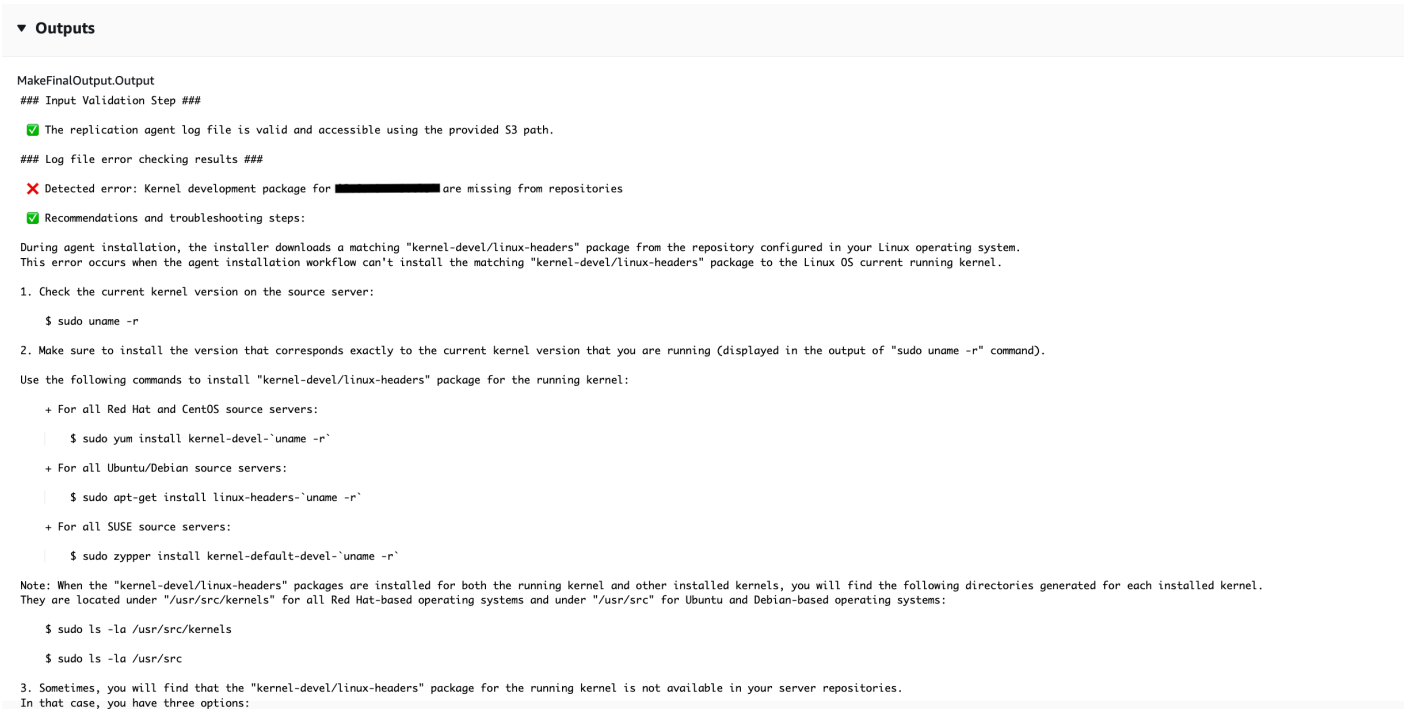
   - **`CheckReplicationAgentLogErrors`**

     Legge il file di registro dell'agente di replica a partire dal byte di installazione più recente e cerca eventuali errori noti. AWS MGN AWS DRS

   - **`MakeFinalOutput`**

     Crea l'output dei controlli precedenti, incluse informazioni sugli errori rilevati e consigli per la risoluzione dei problemi.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:



Outputs

MakeFinalOutput.Output

```
### Input Validation Step ###

✅ The replication agent log file is valid and accessible using the provided S3 path.

### Log file error checking results ###

❌ Detected error: Kernel development package for [redacted] are missing from repositories

✅ Recommendations and troubleshooting steps:

During agent installation, the installer downloads a matching "kernel-devel/linux-headers" package from the repository configured in your Linux operating system.
This error occurs when the agent installation workflow can't install the matching "kernel-devel/linux-headers" package to the Linux OS current running kernel.

1. Check the current kernel version on the source server:

    $ sudo uname -r

2. Make sure to install the version that corresponds exactly to the current kernel version that you are running (displayed in the output of "sudo uname -r" command).

Use the following commands to install "kernel-devel/linux-headers" package for the running kernel:

    + For all Red Hat and CentOS source servers:

        $ sudo yum install kernel-devel-`uname -r`

    + For all Ubuntu/Debian source servers:

        $ sudo apt-get install linux-headers-`uname -r`

    + For all SUSE source servers:

        $ sudo zypper install kernel-default-devel-`uname -r`

Note: When the "kernel-devel/linux-headers" packages are installed for both the running kernel and other installed kernels, you will find the following directories generated for each installed kernel.
They are located under "/usr/src/kernels" for all Red Hat-based operating systems and under "/usr/src" for Ubuntu and Debian-based operating systems:

    $ sudo ls -la /usr/src/kernels

    $ sudo ls -la /usr/src

3. Sometimes, you will find that the "kernel-devel/linux-headers" package for the running kernel is not available in your server repositories.
In that case, you have three options:
```

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWSSupport-TroubleshootRDP

Descrizione

Il `AWSSupport-TroubleshootRDP` runbook consente all'utente di controllare o modificare le impostazioni comuni sull'istanza di destinazione che possono influire sulle connessioni RDP (Remote Desktop Protocol), come la porta RDP, i profili Network Layer Authentication (NLA) e Windows Firewall. Facoltativamente, le modifiche possono essere applicate offline arrestando e avviando l'istanza, se l'utente autorizza in modo esplicito la correzione offline. Per impostazione predefinita, il runbook legge ed emette i valori delle impostazioni.

> **Important**
>
> Le modifiche alle impostazioni RDP, al servizio RDP e ai profili di Windows Firewall devono essere esaminate attentamente prima di utilizzare questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Windows

Parametri

- Operazione

  Tipo: String

  Valori validi: CheckAll | FixAll | Personalizzato

  Impostazione predefinita: Custom

  Descrizione: (Facoltativo) [Personalizzato] Utilizza i valori di Firewall, RDPServiceStartupType, RDP ServiceActionPortAction, NLA SettingAction e RemoteConnections per gestire le impostazioni. [CheckAll] Leggi i valori delle impostazioni senza modificarli. [FixAll] Ripristina le impostazioni predefinite RDP e disabilita Windows Firewall.
- AllowOffline

  Tipo: String

  Valori validi: true | false

  Di default: false

Descrizione: (facoltativo) solo per la correzione: impostare su True se è abilitata la correzione RDP offline e la risoluzione dei problemi online ha esito negativo oppure se l'istanza specificata non è un'istanza gestita. Nota: per la correzione offline, SSM Automation arresta l'istanza e crea un'AMI prima di provare altre operazioni.

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Firewall

  Tipo: String

  Valori validi: Controlla | Disabilita

  Impostazione predefinita: Check

  Descrizione: (facoltativo) controlla o disabilita Windows Firewall (tutti i profili).

- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) ID dell'istanza gestita per la quale risolvere i problemi relativi alle impostazioni RDP.

- NLA SettingAction

  Tipo: String

  Valori validi: Controlla | Disabilita

  Impostazione predefinita: Check

  Descrizione: (facoltativo) controlla o disabilita l'autenticazione NLA (Network Layer Authentication).

- RDP PortAction

  Tipo: String

Valori validi: Controlla | Modifica

Impostazione predefinita: Check

Descrizione: (facoltativo) controlla la porta corrente utilizzata per le connessioni RDP oppure modifica la porta RDP reimpostandola su 3389 e riavvia il servizio.

- RDP ServiceAction

  Tipo: String

  Valori validi: Verifica | Avvia | Riavvia | Riavvio forzato

  Impostazione predefinita: Check

  Descrizione: (Facoltativo) Controlla, avvia, riavvia o riavvia forzatamente il servizio RDP (). TermService

- RDP ServiceStartupType

  Tipo: String

  Valori validi: Verifica | Auto

  Impostazione predefinita: Check

  Descrizione: (facoltativo) controlla o imposta l'avvio automatico del servizio RDP all'avvio di Windows.

- RemoteConnections

  Tipo: String

  Valori validi: Controlla | Abilita

  Impostazione predefinita: Check

  Descrizione: (facoltativo) operazione da eseguire sulle impostazioni fDenyTSConnections: Check, Enable.

- S3 BucketName

  Tipo: String

Descrizione: (facoltativo) solo offline: nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- SubnetId

  Tipo: String

  Predefinito: SelectedInstanceSubnet

  Descrizione: (facoltativo) solo offline - ID sottorete dell'istanza EC2Rescue utilizzata per eseguire la risoluzione dei problemi offline. Se non viene specificato alcun ID sottorete, AWS Systems Manager Automation creerà un nuovo VPC. IMPORTANTE: la sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l'istanza EC2 che riceve il comando abbia un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. Per la correzione online, l'utente deve disporre almeno di ssm:DescribeInstanceInformation, ssm: StartAutomationExecution e ssm: SendCommand per eseguire l'automazione e inviare il comando all'istanza, più ssm: GetAutomationExecution per poter leggere l'output dell'automazione. Per la correzione offline, l'utente deve disporre almeno di ssm:, ssm: DescribeInstanceInformation, ec2: StartAutomationExecutionDescribeInstances, più ssm: GetAutomationExecution per poter leggere l'output dell'automazione. `AWSSupport-TroubleshootRDP`chiamate `AWSSupport-ExecuteEC2Rescue` per eseguire la correzione offline: verifica le autorizzazioni per `AWSSupport-ExecuteEC2Rescue` assicurarti di poter eseguire correttamente l'automazione.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Controlla se l'istanza è un'Windows Serveristanza
2. `aws:assertAwsResourceProperty`- Controlla se l'istanza è un'istanza gestita
3. (Risoluzione dei problemi online) Se l'istanza è un'istanza gestita:
   a. `aws:assertAwsResourceProperty`- Controlla il valore dell'azione fornito
   b. (Controllo online) Se l'azione = CheckAll, allora:

`aws:runPowerShellScript`- Esegue lo PowerShell script per ottenere lo stato dei profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per ottenere lo stato del servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per ottenere le impostazioni RDP.

c. (Correzione online) Se l'azione = FixAll, allora:

`aws:runPowerShellScript`- Esegue lo PowerShell script per disattivare tutti i profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per avviare il servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per abilitare le connessioni remote e disabilitare l'NLA.

d. (Gestione online) Se Action = Custom:

`aws:runPowerShellScript`- Esegue lo PowerShell script per gestire i profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per gestire il servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per gestire le impostazioni RDP.

4. (Correzione offline) Se l'istanza non è un'istanza gestita:

a. `aws:assertAwsResourceProperty`- Asserzione AllowOffline= vero

b. `aws:assertAwsResourceProperty`- Asserisci azione = FixAll

c. `aws:assertAwsResourceProperty`- Afferma il valore di SubnetId

(Usa la sottorete dell'istanza fornita) Se SubnetId è SELECTED_INSTANCE_SUBNET

`aws:executeAwsApi`- Recupera la sottorete dell'istanza corrente.

`aws:executeAutomation`- Esegui `AWSSupport-ExecuteEC2Rescue` con la sottorete dell'istanza fornita.

d. (Usa la sottorete personalizzata fornita) Se non SubnetId è SELECTED_INSTANCE_SUBNET

`aws:executeAutomation`- Esegui `AWSSupport-ExecuteEC2Rescue` con SubnetId il valore fornito.

Output

manageFirewallProfiles.Uscita

Gestore DP. ServiceSettings Output

manageRDPSettings.Output

checkFirewallProfiles.Uscita

Controlla RDP. ServiceSettings Uscita

checkRDPSettings.Output

disableFirewallProfiles.Uscita

RDP predefinito. Output ServiceSettings

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

Risoluzione dei problemi relativi OfflineWithSubnetId a RDP .Output

AWSSupport-TroubleshootSSH

Descrizione

Il `AWSSupport-TroubleshootSSH` runbook installa lo strumento Amazon EC2Rescue per Linux, quindi utilizza lo strumento EC2Rescue per verificare o tentare di risolvere problemi comuni che impediscono una connessione remota alla macchina Linux tramite SSH. Facoltativamente, le modifiche possono essere applicate offline arrestando e avviando l'istanza, se l'utente autorizza in modo esplicito la correzione offline. Per impostazione predefinita, il runbook funziona in modalità di sola lettura.

Esegui questa automazione (console)

Per informazioni sull'utilizzo del `AWSSupport-TroubleshootSSH` runbook, consulta questo argomento relativo `AWSSupport-TroubleshootSSH` alla risoluzione dei problemi di AWS Premium Support.

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- Operazione

  Tipo: String

  Valori validi: CheckAll | FixAll

  Predefinito: CheckAll

  Descrizione: (obbligatorio) specifica se individuare la presenza di problemi senza risolverli oppure se individuare e risolvere automaticamente i problemi rilevati.
- AllowOffline

  Tipo: String

  Valori validi: true | false

  Di default: false

  Descrizione: (facoltativo) solo per la correzione: impostare su True se è abilitata la correzione SSH offline e la risoluzione dei problemi online ha esito negativo oppure se l'istanza specificata non è un'istanza gestita. Nota: per la correzione offline, SSM Automation arresta l'istanza e crea un'AMI prima di provare altre operazioni.

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (obbligatoria) ID dell'istanza EC2 per Linux.
- S3 BucketName

  Tipo: String

  Descrizione: (facoltativo) solo offline: nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.
- SubnetId

  Tipo: String

  Predefinito: SelectedInstanceSubnet

  Descrizione: (facoltativo) solo offline - ID sottorete dell'istanza EC2Rescue utilizzata per eseguire la risoluzione dei problemi offline. Se non viene specificato alcun ID sottorete, AWS Systems Manager Automation creerà un nuovo VPC.

  > **Important**
  >
  > La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l'istanza EC2 che riceve il comando abbia un ruolo IAM con la policy gestita di ManagedInstanceCore Amazon di AmazonSSM allegata. Per la correzione online, l'utente deve disporre almeno di ssm:DescribeInstanceInformation, ssm: StartAutomationExecution e ssm: SendCommand per eseguire l'automazione e inviare il comando all'istanza, più ssm: GetAutomationExecution per poter leggere l'output dell'automazione. Per la correzione offline, l'utente deve disporre almeno di ssm:, ssm: DescribeInstanceInformation, ec2: StartAutomationExecutionDescribeInstances, più ssm: GetAutomationExecution per poter leggere l'output dell'automazione. `AWSSupport-TroubleshootSSH`chiamate `AWSSupport-ExecuteEC2Rescue` per eseguire la correzione offline: verifica le autorizzazioni per `AWSSupport-ExecuteEC2Rescue` assicurarti di poter eseguire correttamente l'automazione.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Controlla se l'istanza è un'istanza gestita
   a. (Correzione online) Se l'istanza è un'istanza gestita:
      i. `aws:configurePackage`- Installare EC2Rescue per Linux tramite. `AWS-ConfigureAWSPackage`
      ii. `aws:runCommand`- Esegui lo script bash per eseguire EC2Rescue per Linux.
   b. (Correzione offline) Se l'istanza non è un'istanza gestita:
      i. `aws:assertAwsResourceProperty`- Asserzione AllowOffline= vero
      ii. `aws:assertAwsResourceProperty`- Asserisci azione = FixAll
      iii. `aws:assertAwsResourceProperty`- Afferma il valore di SubnetId
      iv. (Usa la sottorete dell'istanza fornita) Spetta `aws:executeAutomation` a SelectedInstanceSubnet noi eseguire `AWSSupport-ExecuteEC2Rescue` con la sottorete dell'istanza fornita. SubnetId
      v. (Usa la sottorete personalizzata fornita) If non SubnetId viene SelectedInstanceSubnet utilizzato `aws:executeAutomation` per funzionare `AWSSupport-ExecuteEC2Rescue` con il SubnetId valore fornito.

Output

troubleshootSSH.Output

troubleshootSSHOffline.Output

Risoluzione dei problemi relativi OfflineWithSubnetId a SSH .Output

AWSSupport-TroubleshootSUSERegistration

Descrizione

Il `AWSSupport-TroubleshootSUSERegistration` runbook ti aiuta a identificare il motivo per cui la registrazione di un'SUSE Linux Enterprise Serveristanza Amazon Elastic Compute Cloud (Amazon EC2) con SUSE Update Infrastructure non è riuscita. L'output dell'automazione fornisce i passaggi per risolvere o aiuta a risolvere il problema. Se l'istanza supera tutti i controlli durante l'automazione, viene registrata con SUSE Update Infrastructure.

Esegui questa automazione (console)

Tipo di documento

Automazione di

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: String

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: String

  Descrizione: (obbligatorio) L'ID dell'istanza Amazon EC2 che desideri risolvere.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Fasi del documento

- `aws:assertAwsResourceProperty`- Verifica se l'istanza Amazon EC2 è gestita daAWS Systems Manager.
- `aws:runCommand`- Verifica se la piattaforma di istanza Amazon EC2 lo èSLES.
- `aws:runCommand`- Controlla se la `cloud-regionsrv-client` versione del pacchetto è maggiore o uguale alla versione richiesta 9.0.10.
- `aws:runCommand`- Controlla se il collegamento simbolico per il prodotto base è interrotto e corregge il collegamento in caso di interruzione.
- `aws:runCommand`- Controlla se il file hosts (`/etc/hosts`) contiene record per`smt-ec2-suscloud.net`. L'automazione rimuove eventuali voci duplicate.
- `aws:runCommand`- Verifica se il `curl` comando è installato.
- `aws:runCommand`- Verifica se l'istanza Amazon EC2 può accedere all'indirizzo Instance Metadata Service (IMDS) 169.254.169.254.
- `aws:runCommand`- Verifica se l'istanza Amazon EC2 ha un codice di fatturazione o un codice Marketplace AWS prodotto.
- `aws:runCommand`- Verifica se l'istanza Amazon EC2 può raggiungere almeno 1 server regionale tramite HTTPS.
- `aws:runCommand`- Verifica se l'istanza Amazon EC2 può raggiungere i server Subscription Management Tool (SMT) tramite HTTP.
- `aws:runCommand`- Verifica se l'istanza Amazon EC2 può raggiungere i server Subscription Management Tool (SMT) tramite HTTPS.

- `aws:runCommand`- Verifica se l'istanza Amazon EC2 può raggiungere l'`smt-ec2.susecloud.net`indirizzo tramite HTTPS.
- `aws:runCommand`- Registra l'istanza Amazon EC2 con SUSE Update Infrastructure.
- `aws:executeScript`- Raccoglie ed emette l'output di tutti i passaggi precedenti.

`AWSSupport-TroubleshootWindowsPerformance`

Descrizione

Il runbook `AWSSupport-TroubleshootWindowsPerformance` aiuta a risolvere i problemi di prestazioni in corso sull'istanza Windows di Amazon Elastic Compute Cloud (AmazonEC2). Il runbook acquisisce i log dall'istanza di destinazione e analizza i parametri prestazionali della memoriaCPU, del disco e della rete. Facoltativamente, l'automazione può acquisire un dump del processo per aiutarti a determinare la potenziale causa del peggioramento delle prestazioni. L'automazione acquisisce anche i registri degli eventi e del sistema utilizzando `EC2Rescue`lo strumento più recente, se consenti a questo runbook di installarlo.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica i prerequisiti dell'EC2istanza Amazon.
- Genera log delle prestazioni nel disco principale dell'istanza Amazon EC2 Windows
- Memorizza i log acquisiti nella cartella `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Se viene fornito un bucket Amazon Simple Storage Service (Amazon S3) e il ruolo di automazione assume le autorizzazioni necessarie, i log acquisiti vengono caricati nel bucket Amazon S3.
- Installa `EC2Rescue` lo strumento più recente sull'istanza di Amazon EC2 Windows per acquisire eventi e log di sistema se scegli di installarlo, ma non analizza il dump del processo e i log acquisiti da. `EC2Rescue`

> **Important**
>
> - Per eseguire questo runbook, l'istanza Amazon EC2 Windows deve essere gestita da AWS Systems Manager. Per ulteriori informazioni, consulta Perché la mia EC2 istanza Amazon non viene visualizzata come nodo gestito.

- Per eseguire questo runbook, l'istanza Amazon EC2 Windows deve essere in esecuzione su versioni Windows 8.1 /Windows Server 2012 R2 (6.3) o successive con PowerShell 4.0 o versioni successive. Per ulteriori informazioni, consulta la versione del sistema operativo Windows.
- Per la generazione di registri delle prestazioni, sono necessari almeno 10 GB di spazio libero sul dispositivo root. Se il disco principale è più grande di 100 GB, lo spazio libero deve essere superiore al 10% della dimensione del disco. Se si esegue il dump di un processo durante l'esecuzione, lo spazio libero deve essere superiore a 10 GB più la dimensione totale della memoria consumata dal processo quando il processo consuma più di 10 GB di memoria.
- I log generati sul dispositivo root non vengono eliminati automaticamente.
- Il runbook non disinstalla lo `EC2Rescue` strumento. Per ulteriori informazioni, consulta Use `EC2Rescue` for Windows Server.
- È consigliabile eseguire questa automazione durante un impatto sulle prestazioni. È inoltre possibile eseguirla periodicamente utilizzando un'associazione AWS Systems Manager State Manager o pianificando AWS Systems Manager Maintenance Windows.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`

- ssm:DescribeAutomationExecutions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand
- s3:ListBucket
- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:PutObject
- s3:GetBucketAcl
- s3:GetAccountPublicAccessBlock

(Facoltativo) Il IAM ruolo associato al profilo dell'istanza o IAM all'utente configurato sull'istanza richiede le seguenti azioni per caricare i log nel bucket Amazon S3 specificato per il parametro: *LogUploadBucketName*

- s3:PutObject
- s3:GetObject
- s3:ListBucket

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere AWSSupport-TroubleshootWindowsPerformancea Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene

specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId (Obbligatorio):

  L'ID dell'istanza Amazon EC2 Windows di destinazione in cui desideri eseguire l'automazione. L'istanza deve essere gestita da Systems Manager per eseguire l'automazione.

- CaptureProcessDump (Facoltativo):

  Il tipo di dump del processo da acquisire. L'automazione può acquisire un dump del processo che potenzialmente causa l'impatto sulle prestazioni all'inizio dell'automazione. Il volume root dell'istanza richiede almeno 10 GB di spazio libero (più del 10% della dimensione del disco quando la dimensione del volume principale è superiore a 100 GB e 10 GB più la dimensione totale della memoria consumata dal processo quando il processo consuma più di 10 GB di memoria).

- LogCaptureDuration (Facoltativo):

  Il numero di minuti, tra `1` e`15`, durante i quali questa automazione acquisirà i registri mentre il problema è presente. Il valore predefinito è `5`.

- LogUploadBucketName (Facoltativo):

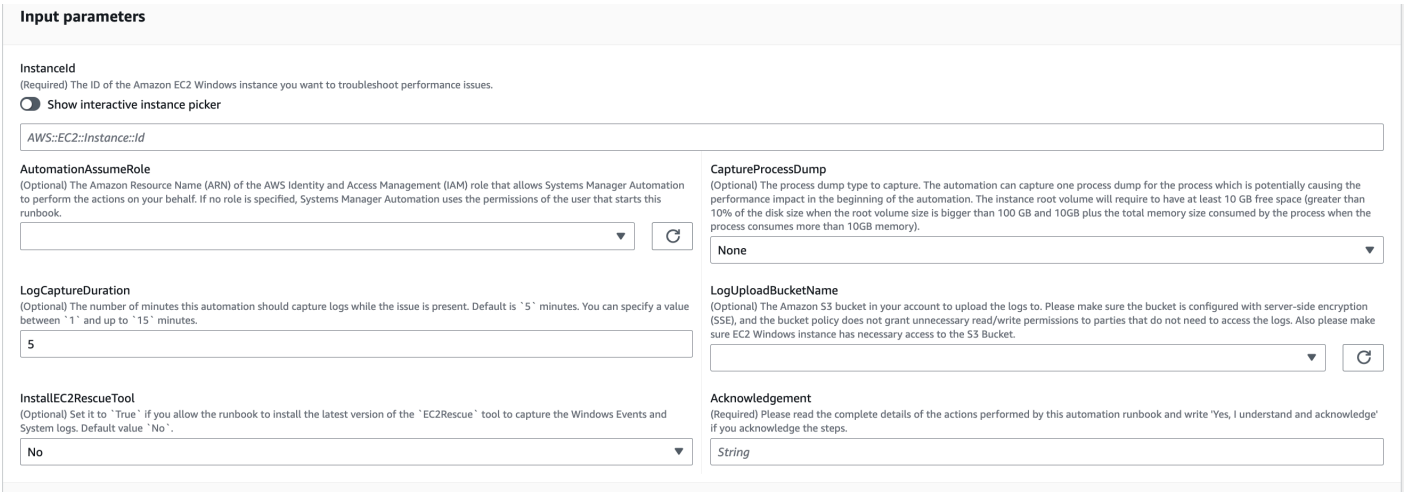
  Il bucket Amazon S3 nel tuo account in cui desideri caricare i log. Il bucket deve essere configurato con la crittografia lato server (SSE) e la policy del bucket non deve concedere autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log acquisiti. L'istanza Amazon EC2 Windows deve avere accesso al bucket Amazon S3.

- Installazione EC2RescueTool (opzionale):

  Impostato per consentire `Yes` al runbook di installare la versione più recente `EC2Rescue` dello strumento per acquisire gli eventi di Windows e i registri di sistema. Il valore predefinito è `No`.

- Riconoscimento (obbligatorio):

  Leggi i dettagli completi delle azioni eseguite da questo runbook di automazione e, se sei d'accordo, digita. `Yes, I understand and acknowledge`



4. Seleziona Esegui.
5. L'automazione si avvia.
6. Il documento esegue le seguenti operazioni:
   - **`CheckConcurrency:`**

     Assicura che esista una sola esecuzione di questo runbook destinata all'istanza. Se il runbook trova un'altra esecuzione destinata alla stessa istanza, restituisce un errore e termina.
   - **`AssertInstanceIsWindows:`**

     Afferma che l'EC2istanza Amazon è in esecuzione sul sistema operativo Windows. In caso contrario, l'automazione termina.
   - **`AssertInstanceIsManagedInstance:`**

     Afferma che l'EC2istanza Amazon è gestita da AWS Systems Manager. Altrimenti l'automazione termina.
   - **`VerifyPrerequisites:`**

     Verifica la PowerShell versione sul sistema operativo dell'istanza e assicura che l'istanza possa essere connessa tramite Systems Manager per eseguire PowerShell i comandi. Questa automazione supporta la PowerShell versione 4.0 e successive in esecuzione su versioni Windows 8.1 /Server 2012 R2 (6.3) o successive. Se la versione è precedente, l'automazione fallisce. Quando scegli di caricare i log nel bucket Amazon S3, questa automazione verifica che AWS il modulo Tools PowerShell for sia disponibile. In caso contrario, l'automazione termina.
   - **`BranchOnProcessDump:`**

Le filiali si basano su se è stata impostata per acquisire il dump dei processi che hanno influito sulle prestazioni.

- **CaptureProcessDump:**

  Verifica se l'istanza ha spazio sufficiente per eseguire questa automazione (quando scegli HighestCPU/Memory).

- **CapturePerformanceLogs:**

  Controlla nuovamente lo spazio su disco ed esegue lo PowerShell script sull'istanza per creare contatori perfmon e avviare la registrazione di Performance Monitor e Windows Performance Recorder. Lo script si interrompe dopo il raggiungimento del valore definito. `LogCaptureDuration`

- **SummarizePerformanceLogs:**

  Riepiloga il XML rapporto generato nel passaggio precedente`CapturePerformanceLogs`, per individuare il processo responsabile che consuma più WorkingSet 64 (memoria) e% di tempo del processore (CPU) indicati come output dell'automazione. Genera informazioni simili per l'utilizzo di Interfaccia di rete LogicalDisk TCPv4IPv4, Memoria UDPv4 e le salva `analysis_output.log` nella cartella di output.

- **BranchOnInstallEC2Rescue:**

  Branches se lo imposti per installare lo `EC2Rescue` strumento più recente nell'EC2istanza Amazon.

- **InstallEC2RescueTool:**

  Installa lo `EC2Rescue` strumento nel sistema operativo dell'istanza per acquisire `EC2Rescue` i log utilizzando. `AWS-ConfigureAWSPackage`

- **RunEC2RescueTool:**

  Esegue lo `EC2Rescue` strumento nel sistema operativo dell'istanza per acquisire tutti i log necessari. `EC2Rescue`acquisisce solo i log necessari per risparmiare spazio.

- **BranchOnIfS3BucketProvided:**

  I rami si basano sull'input dell'utente `LogUploadBucketName` per verificare se è disponibile un nome di bucket per caricare i log.

- **GetS3BucketPublicStatus:**

Determina se viene fornito un bucket Amazon S3 e, in tal caso, conferma che il bucket Amazon S3 non è pubblico ed è configurato con. SSE

- **`UploadLogResult:`**

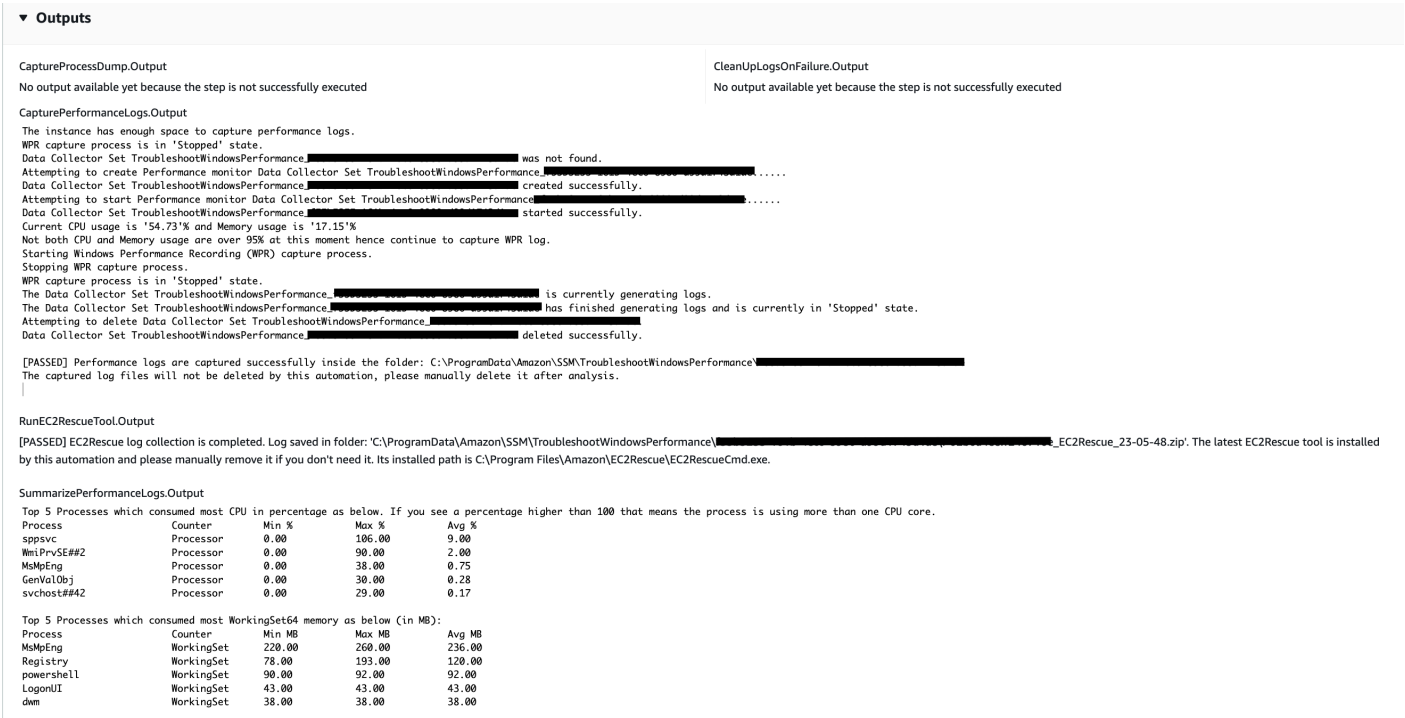
  Carica i log nel bucket Amazon S3 fornito. Se la PowerShell versione è 5.0 o successiva, comprime i log in un archivio e li carica. ZIP Elimina il ZIP file al termine del caricamento. Se la PowerShell versione è inferiore alla 5.0, carica i file direttamente in una cartella.

- **`CleanUpLogsOnFailure:`**

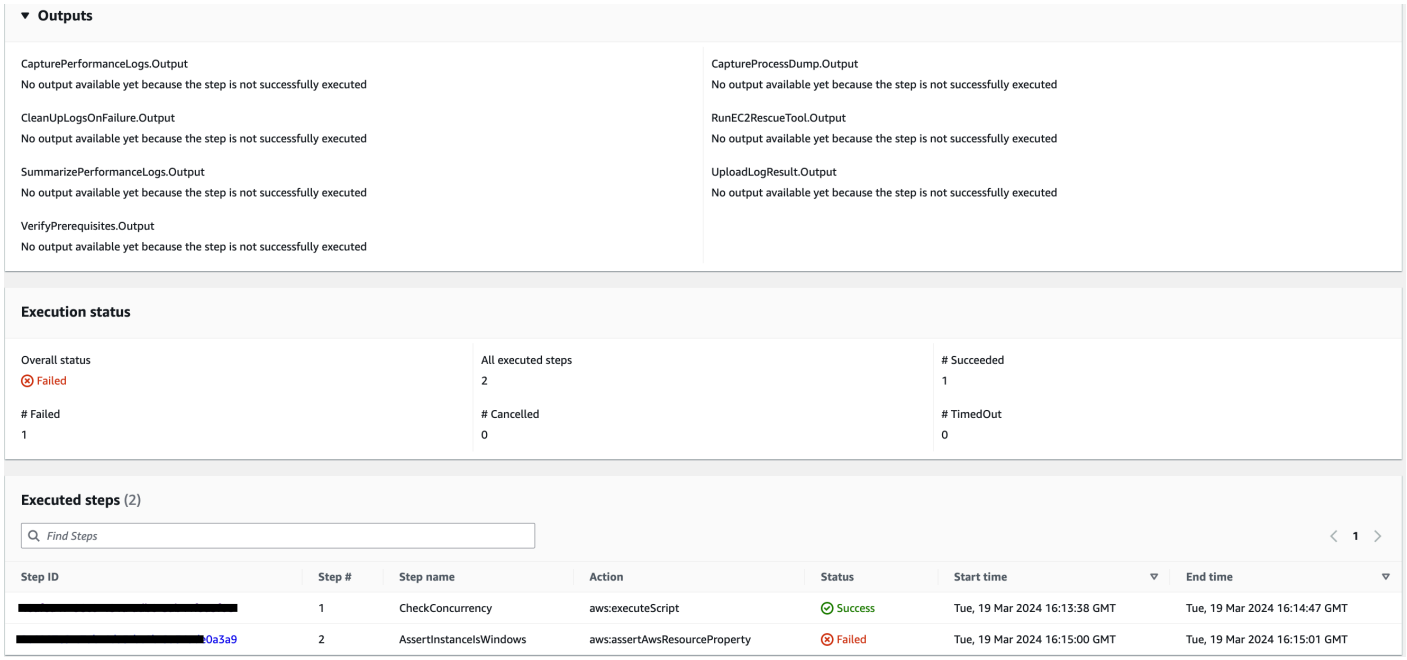
  Pulisce tutti i log generati dal `CapturePerformanceLogs` passaggio in caso di errore. Il `CleanUpLogsOnFailure` passaggio potrebbe non riuscire o scadere se SSM l'agente non funziona correttamente o il sistema Windows non risponde.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

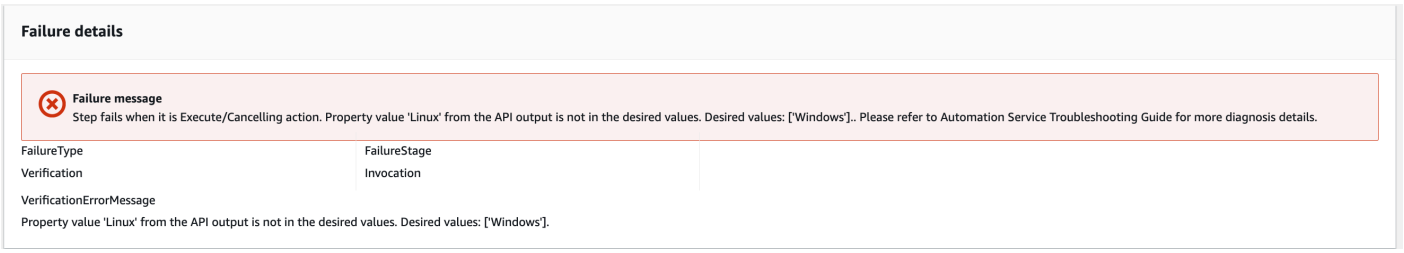
Esecuzione in cui l'istanza di destinazione presenta tutti i prerequisiti richiesti.



Esecuzione in cui l'istanza di destinazione si trova sulla piattaforma Linux e l'esecuzione non è riuscita. È necessario selezionare l'ID del passaggio per visualizzare i dettagli dell'errore.



I dettagli dell'errore della fase`AssertInstanceIsWindows`.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

`AWSSupport-TroubleshootWindowsUpdate`

Descrizione

Il `AWSSupport-TroubleshootWindowsUpdate` runbook viene utilizzato per identificare problemi che potrebbero fallire negli aggiornamenti di Windows per le istanze Windows di Amazon Elastic Compute Cloud (Amazon EC2).

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica se l'istanza Amazon EC2 di destinazione è gestita da. AWS Systems Manager
- Verifica se le versioni AWS Systems Manager Agent (SSM Agent) e Windows Server sono supportate per le operazioni di patching di Systems Manager.
- Verifica lo spazio disponibile su disco consigliato per gli aggiornamenti di Windows e se è in sospeso un riavvio. Un riavvio in sospeso indica in genere che gli aggiornamenti sono in sospeso ed è necessario un riavvio prima di eseguire aggiornamenti aggiuntivi.
- Configura le impostazioni del proxy a livello di sistema operativo, il che può aiutare a risolvere i problemi di connettività.
- Esegue un test di connettività degli endpoint Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e richiama `GetDeployablePatchSnapshotForInstance`l'operazione API per recuperare lo snapshot corrente per la patch baseline utilizzata dal nodo gestito.
- Se la connessione fallisce, offre la possibilità di eseguire il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook per analizzare la connettività dell'istanza agli endpoint Amazon S3.
- Convalida la configurazione degli aggiornamenti di Windows e verifica Windows Server Update Services (WSUS) (se applicabile).

Important

- I controller di dominio Active Directory non sono supportati.
- La versione 2008 R2 di Windows Server o le versioni precedenti non sono supportate.
- SSM Agent 1.2.371 o versioni precedenti non sono supportate.
- Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook viene utilizzato `VPC Reachability Analyzer`per analizzare la connettività di rete tra un endpoint di origine e un endpoint di servizio. Ti viene addebitato un costo per ogni analisi eseguita tra

un'origine e una destinazione. Per ulteriori dettagli, consulta la pagina dei prezzi di Amazon VPC.

- Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook non è disponibile in tutte le regioni in cui è supportato Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Per eseguire il runbook secondario`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, aggiungete le autorizzazioni elencate in questo documento.

Istruzioni

Segui questi passaggi per configurare l'automazione:

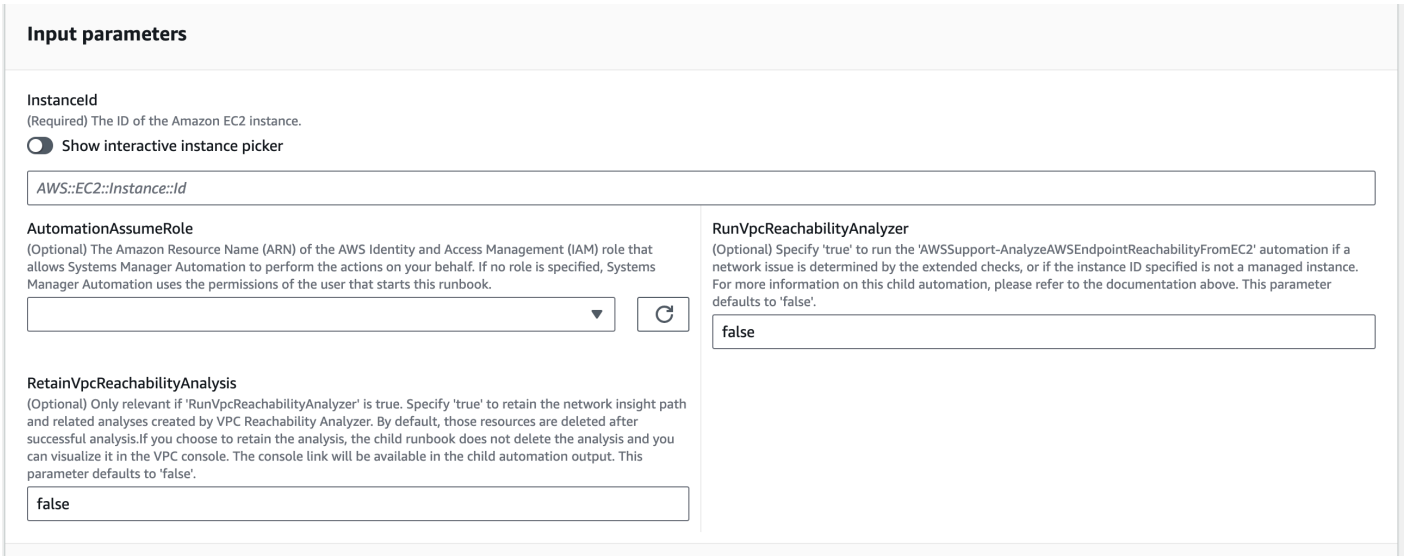
1. Accedere AWSSupport-TroubleshootWindowsUpdatea Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - InstanceId (Obbligatorio):

     Inserisci l'ID dell'istanza Amazon EC2 in cui l'aggiornamento di Windows non è riuscito.
   - RunVpcReachabilityAnalyzer(Facoltativo):

     Specificate di `true` eseguire l'`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`automazione se un problema di rete è determinato dai controlli estesi o se l'ID di istanza specificato non è un'istanza gestita. Per ulteriori informazioni su questa automazione secondaria, consulta la documentazione. Il valore predefinito è `false`.
   - RetainVpcReachabilityAnalysis(Facoltativo):

     Rilevante solo se lo `RunVpcReachabilityAnalyzer` è`true`. `true`Specificare di conservare il percorso di analisi della rete e le relative analisi create da`Reachability Analyzer`. Per impostazione predefinita, tali risorse vengono eliminate dopo un'analisi riuscita. Se scegli di conservare l'analisi, il runbook secondario non elimina l'analisi e puoi visualizzarla nella console Amazon VPC. Il collegamento alla console sarà disponibile nell'output di automazione secondaria. Il valore predefinito`false`.



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:
   - **`getWindowsServerAndSSMAgentVersion:`**

     Verifica che l'istanza di destinazione sia gestita da AWS Systems Manager e ottiene dettagli sulla versione di SSM Agent e sulla versione Windows.
   - **`assertifInstanceIsSsmManaged:`**

     Assicura che l'istanza Amazon EC2 sia gestita da AWS Systems Manager (SSM), altrimenti l'automazione termina.
   - **`CheckProxy:`**

     Verifica la presenza di tutti i tipi di proxy per l'istanza Windows.
   - **`CheckPrerequisites:`**

     Ottiene la versione dell'agente SSM e la versione di Windows e determina se si tratta di un controller di dominio Active Directory (DC). Se l'istanza è un DC o la versione SSM Agent o Windows non è supportata, il runbook si interrompe.
   - **`CheckDiskSpace:`**

     Recupera e convalida lo spazio su disco disponibile sull'istanza di Windows se è sufficiente per eseguire l'aggiornamento di Windows.
   - **`CheckPendingReboot:`**

Verifica la presenza di eventuali riavvii in sospeso sull'istanza di Windows.

- **CheckS3Connectivity:**

  Verifica se l'istanza può raggiungere gli endpoint Amazon S3 per. `Patchbaseline`

- **branchOnRunVpcReachabilityAnalyzer:**

  Se `RunVpcReachabilityAnalyzer` è vero, allora ramifica l'automazione per eseguire un'analisi più approfondita per il debug della connettività Amazon S3.

- **GenerateEndpoints:**

  Genera un endpoint per un controllo esteso della connettività per l'endpoint Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

  Richiama il runbook di automazione,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. per verificare la raggiungibilità dell'istanza selezionata verso gli endpoint richiesti.

- **CheckWindowsUpdateServices:**

  Verifica lo stato del servizio Windows Update e il tipo di avvio.

- **CheckWindowsUpdateSettings:**

  Verifica i criteri di Windows Update configurati sull'istanza di Windows.

- **CheckWSUSSettings:**

  Verifica se l'aggiornamento di Windows è configurato con WSUS o Microsoft Update Catalog e verifica la connettività.

- **CheckWUGlobalSettings:**

  Verifica le impostazioni globali di Windows Update configurate sull'istanza di Windows.

- **GenerateLogs:**

  Scarica i registri di Windows Update e i registri CBS sul desktop dell'istanza e verifica che i registri degli eventi di Windows non presentino errori.

- **FinalReport:**

  Genera un report completo di tutti i passaggi.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

```
FinalReport.Results
"
==================================================Prerequisites Check==================================================
Result: ✅ [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

==================================================Disk Space Check==================================================
Result: ✅ [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

==================================================Pending Reboot Check==================================================
Result: ✅ [PASSED]
INFO: There is no pending reboot.

==============================================Amazon S3 Connectivity Check==============================================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

================================AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2================================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

============================================Windows Update Services Status============================================
Result: ✅ [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

==============================================Windows Proxy Settings==============================================
Result: ✅ [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.


==============================================Windows Update Settings==============================================
Result: ✅ [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\\Adminisrative Template\\Windows Component\\Windows
Update\\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

==============================================Windows Update Global Settings==============================================
Result: ✅ [PASSED]
Windows Update Client has no restrictions

=========================================Copy of Windows Update and CBS logs=========================================
Result: ✅ [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\\Windows\\TEMP\\c176a507-d074-4402-8a5b-631dd643f33a folder
"
```

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione

- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

Documentazione relativa al servizio AWS

- Per ulteriori informazioni, consulta l'articolo TroubleShoot Windows Update.

AWSSupport-UpgradeWindowsAWSDrivers

Descrizione

Il `AWSSupport-UpgradeWindowsAWSDrivers` runbook aggiorna o ripara i AWS driver di archiviazione e di rete sull'istanza EC2 specificata. Il runbook tenta di installare le versioni più recenti dei AWS driver online chiamando SSM Agent. Se SSM Agent non è contattabile, il runbook può eseguire un'installazione offline dei driver se richiesto esplicitamente. AWS

> **Note**
>
> Sia l'aggiornamento online che quello offline creeranno un'AMI prima di tentare qualsiasi operazione, che persisterà dopo il completamento dell'automazione. È responsabilità dell'utente proteggere l'accesso all'AMI oppure eliminarla. Il metodo online riavvia l'istanza nell'ambito del processo di aggiornamento, mentre il metodo offline richiede l'arresto e il riavvio dell'istanza EC2 specificata.

> **Important**
>
> Se le istanze si connettono AWS Systems Manager tramite endpoint VPC, questo runbook fallirà a meno che non venga utilizzato nella regione us-east-1. Questo runbook fallirà anche su un controller di dominio. Per aggiornare i driver di AWS PV in un controller di dominio, consulta Aggiornamento di un controller di dominio (aggiornamento di AWS PV).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AllowOffline

  Tipo: stringa

  Valori validi: true | false

  Impostazione predefinita: false

  Descrizione: (facoltativo) impostare su True se si autorizza l'aggiornamento offline dei driver nel caso in cui risulti impossibile eseguire l'installazione online. Nota: il metodo offline richiede l'arresto e il successivo avvio dell'istanza EC2 specificata. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ForceUpgrade

  Tipo: stringa

  Valori validi: true | false

  Impostazione predefinita: false

  Descrizione: (facoltativo) solo offline: impostare su True se si autorizza il proseguimento dell'aggiornamento offline dei driver anche se nell'istanza corrente sono già stati installati i driver più recenti.

- InstanceId

  Tipo: stringa

  Descrizione: (obbligatoria) ID dell'istanza EC2 per Windows Server.

- SubnetId

  Tipo: stringa

  Impostazione predefinita: SelectedInstanceSubnet

  Descrizione: (facoltativo) solo offline - ID sottorete dell'istanza EC2Rescue utilizzata per eseguire l'aggiornamento dei driver offline. Se non viene specificato alcun ID di sottorete, Systems Manager Automation creerà un nuovo VPC.

  > **Important**
  >
  > La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

L'istanza EC2 che riceve il comando deve avere almeno un ruolo IAM che includa le autorizzazioni per ssm: StartAutomationExecution e ssm: per SendCommand eseguire l'automazione e inviare il comando all'istanza, più ssm: GetAutomationExecution per poter leggere l'output dell'automazione. Puoi allegare la politica gestita `AmazonSSMManagedInstanceCore` Amazon al tuo ruolo IAM per fornire queste autorizzazioni. È tuttavia consigliabile utilizzare il ruolo IAM Automation `AmazonSSMAutomationRole` per questo scopo. Per ulteriori informazioni, consulta Utilizzare IAM per configurare i ruoli per l'automazione.

Se si sta eseguendo un aggiornamento offline, controlla le autorizzazioni richieste da `AWSSupport-StartEC2RescueWorkflow`.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Verifica che l'istanza di input sia Windows.

2. `aws:assertAwsResourceProperty`- Verifica che l'istanza di input sia un'istanza gestita. In questo caso, viene avviato l'aggiornamento online. In caso contrario, viene valutato l'aggiornamento offline.
   a. (Aggiornamento online) Se l'istanza di input è un'istanza gestita:
      i. `aws:createImage`- Crea un backup AMI.
      ii. `aws:createTags`- Contrassegna il backup AMI.
      iii. `aws:runCommand`- Installa il driver di rete ENA tramite`AWS-ConfigureAWSPackage`.
      iv. `aws:runCommand`- Installa il driver NVMe tramite. `AWS-ConfigureAWSPackage`
      v. `aws:runCommand`- Installa il driver PV tramiteAWS. `AWS-ConfigureAWSPackage`
   b. (Aggiornamento offline) Se l'istanza di input non è un'istanza gestita:
      i. `aws:assertAwsResourceProperty`- Verifica che il AllowOffline flag sia impostato su. `true` In tal caso, viene avviato l'aggiornamento offline, altrimenti l'automazione termina.
      ii. `aws:changeInstanceState`- Arresta l'istanza di origine.
      iii. `aws:changeInstanceState`- Arresta forzatamente l'istanza di origine.
      iv. `aws:createImage`- Crea un backup AMI dell'istanza di origine.
      v. `aws:createTags`- Etichetta il backup AMI dell'istanza di origine.
      vi. `aws:executeAwsApi`- Abilita ENA per l'istanza
      vii. `aws:assertAwsResourceProperty`- Afferma la ForceUpgrade bandiera.
      viii Forza l'aggiornamento offline) Se ForceUpgrade = true, `aws:executeAutomation` esegui l'invocazione `AWSSupport-StartEC2RescueWorkflow` con lo script di forzatura dell'aggiornamento del driver. Ciò consente di installare il driver indipendentemente dalla versione corrente installata.
      ix. (Aggiornamento offline) Se ForceUpgrade = false, `aws:executeAutomation` esegui l'invocazione `AWSSupport-StartEC2RescueWorkflow` con lo script di aggiornamento dei driver.

Output

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Uscita

forceUpgradeDriversOutput offline

Amazon ECS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Container Service. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

`AWSSupport-CollectECSInstanceLogs`

Descrizione

Il `AWSSupport-CollectECSInstanceLogs` runbook raccoglie i file di log relativi al sistema operativo e ad Amazon Elastic Container Service (AmazonECS) da un'istanza Amazon Elastic Compute Cloud (AmazonEC2) per aiutarti a risolvere i problemi più comuni di Amazon. ECS Mentre l'automazione raccoglie i file di log associati, vengono apportate modifiche al file system. Queste modifiche includono la creazione di directory temporanee e di una directory di registro, la copia dei file di registro in queste directory e la compressione dei file di registro in un archivio.

Se specifichi un valore per il `LogDestination` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dalla tua EC2 istanza Amazon, se lo stato della policy `isPublic` è impostato su o se l'access control list (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di `All Users` Amazon S3, i log non vengono caricati. `true` Inoltre, se il bucket fornito

non è disponibile nel tuo account, i log non vengono caricati. Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ECSInstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza da cui si desidera raccogliere i log. L'istanza specificata deve essere gestita da Systems Manager.
- LogDestination

  Tipo: stringa

  Descrizione: (Facoltativo) Il bucket Amazon S3 in cui Account AWS caricare i log archiviati.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Consigliamo che l'EC2istanza Amazon specificata nel `ECSInstanceId` parametro abbia un IAM ruolo con la policy gestita di `AmazonSSMManagedInstanceCore` Amazon allegata. Per caricare l'archivio di log nel bucket Amazon S3 specificato nel `LogDestination` parametro, devi aggiungere le seguenti autorizzazioni:

- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`

Fasi del documento

- `assertInstanceIsManaged`- Verifica se l'istanza specificata nel `ECSInstanceId` parametro è gestita da Systems Manager.
- `getInstancePlatform`- Ottiene informazioni sulla piattaforma del sistema operativo (OS) dell'istanza specificata nel `ECSInstanceId` parametro.
- `verifyInstancePlatform`- Suddivide l'automazione in base alla piattaforma OS.
- `runLogCollectionScriptOnLinux`- Raccoglie i file di registro ECS relativi al sistema operativo e ad Amazon su istanze Linux e crea un file di archivio nella `/var/log/collectECSlogs` directory.
- `runLogCollectionScriptOnWindows`- Raccoglie i file di registro ECS relativi al sistema operativo e ad Amazon sulle istanze di Windows e crea un file di archivio nella `C:\ProgramData\collectECSlogs` directory.
- `verifyIfS3BucketProvided`- Verifica se è stato specificato un valore per il parametro. `LogDestination`

- `runUploadScript`- Suddivide la fase di automazione in base alla piattaforma del sistema operativo.
- `runUploadScriptOnLinux`- Carica l'archivio di log nel bucket Amazon S3 specificato nel parametro ed elimina `LogDestination` il file di registro archiviato dal sistema operativo.
- `runUploadScriptOnWindows`- Carica l'archivio di log nel bucket Amazon S3 specificato nel parametro ed elimina `LogDestination` il file di registro archiviato dal sistema operativo.

`AWS-InstallAmazonECSAgent`

Descrizione

Il `AWS-InstallAmazonECSAgent` runbook installa l'agente Amazon Elastic Container Service (AmazonECS) sull'istanza Amazon Elastic Compute Cloud (AmazonEC2) specificata. Questo runbook supporta solo istanze Amazon Linux e Amazon Linux 2.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceIds

Tipo: StringList

Descrizione: (Obbligatorio) Le IDs EC2 istanze Amazon su cui desideri installare l'ECSagente Amazon.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Fasi del documento

`aws:executeScript`- Installa l'ECSagente Amazon sulle EC2 istanze Amazon specificate nel `InstanceIds` parametro.

Output

InstallAmazonECSAgent. SuccessfulInstances - L'ID dell'istanza in cui l'installazione dell'ECSagente Amazon è riuscita.

InstallAmazonECSAgent. FailedInstances - L'ID dell'istanza in cui l'installazione dell'ECSagente Amazon non è riuscita.

InstallAmazonECSAgent. InProgressInstances - L'ID dell'istanza in cui è in corso l'installazione dell'ECSagente Amazon.

AWS-ECSRunTask

Descrizione

Il `AWS-ECSRunTask` runbook esegue il task Amazon Elastic Container Service (AmazonECS) specificato dall'utente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- capacityProviderStrategy

  Tipo: stringa

  Descrizione: (Facoltativo) La strategia del provider di capacità da utilizzare per l'attività.
- cluster

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome breve o ARN del cluster su cui eseguire l'attività. Se non si specifica un cluster, viene utilizzato il cluster predefinito.
- count

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero di istanze dell'attività specificata da inserire nel cluster. È possibile specificare fino a 10 attività per ogni richiesta.
- enableECSManagedTag

Tipo: Booleano

Descrizione: (Facoltativo) Specifica se utilizzare i tag ECS gestiti da Amazon per l'attività. Per ulteriori informazioni, consulta Tagging your Amazon ECS Resources nella Amazon Elastic Container Service Developer Guide.

- enableExecuteCommand

  Tipo: Booleano

  Descrizione: (Facoltativo) Determina se attivare la funzionalità del comando di esecuzione per i contenitori in questa attività. Se impostato su true, ciò attiva la funzionalità di esecuzione dei comandi su tutti i contenitori dell'attività.

- gruppo

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del gruppo di attività da associare all'attività. Il valore predefinito è il cognome della definizione dell'attività. Ad esempio `family:my-family-name`.

- launchType

  Tipo: stringa

  Valori validi: EC2 | FARGATE | EXTERNAL

  Descrizione: (Facoltativo) L'infrastruttura su cui eseguire l'attività autonoma.

- networkConfiguration

  Tipo: stringa

  Descrizione: (Facoltativo) La configurazione di rete per l'attività. Questo parametro è necessario per le definizioni delle attività che utilizzano la modalità di `awsvpc` rete per ricevere la propria interfaccia di rete elastica e non è supportato per altre modalità di rete.

- sovrascrive

  Tipo: stringa

  Descrizione: (Facoltativo) Un elenco di sostituzioni dei contenitori in un JSON formato che specifica il nome di un contenitore nella definizione dell'attività specificata e le sostituzioni che deve ricevere. Puoi sovrascrivere il comando predefinito per un contenitore specificato nella definizione dell'attività

o nell'immagine Docker con un comando override. Puoi anche sovrascrivere le variabili di ambiente esistenti specificate nella definizione dell'attività o nell'immagine Docker su un contenitore. Inoltre, puoi aggiungere nuove variabili di ambiente con un'override di ambiente.

- placementConstraints

  Tipo: stringa

  Descrizione: (Facoltativo) Una serie di oggetti con vincoli di posizionamento da utilizzare per l'attività. È possibile specificare fino a 10 vincoli per ogni attività, inclusi i vincoli nella definizione dell'attività e quelli specificati in fase di esecuzione.

- placementStrategy

  Tipo: stringa

  Descrizione: (Facoltativo) Gli oggetti della strategia di posizionamento da utilizzare per l'attività. È possibile specificare un massimo di 5 regole strategiche per ogni attività.

- platformVersion

  Tipo: stringa

  Descrizione: (Facoltativo) La versione della piattaforma utilizzata dall'attività. Una versione della piattaforma è specificata solo per le attività ospitate su Fargate. Se non è specificata, di default viene utilizzata la versione della piattaforma `LATEST`.

- propagateTags

  Tipo: stringa

  Descrizione: (Facoltativo) Determina se i tag si propagano dalla definizione dell'attività all'attività. Se non viene specificato alcun valore, i tag non vengono propagati. I tag possono essere propagati all'attività solo durante la creazione della stessa.

- referenceId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID di riferimento da utilizzare per l'attività. L'ID di riferimento può avere una lunghezza massima di 1024 caratteri.

- startedBy

  Tipo: stringa

Descrizione: (Facoltativo) Un tag opzionale specificato all'avvio di un'attività. Ciò consente di identificare quali attività appartengono a un lavoro specifico filtrando i risultati di un'`ListTasks`APIoperazione. Sono consentiti fino a 36 lettere (maiuscole e minuscole), numeri, trattini (-) e caratteri di sottolineatura (_).

- tags

  Tipo: stringa

  Descrizione: (Facoltativo) Metadati che desideri applicare all'attività per aiutarti a classificare e organizzare le attività. Ogni tag è costituito da una chiave e da un valore definiti dall'utente.

- taskDefinition

  Tipo: stringa

  Descrizione: (Facoltativo) La definizione `family` e `revision` (`family:revision`) o completa ARN dell'attività da eseguire. Se non viene specificata una revisione, viene utilizzata la `ACTIVE` revisione più recente.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ecs:RunTask`

Fasi del documento

`aws:executeScript`- Esegue il ECS task Amazon in base ai valori specificati per i parametri di input del runbook.

AWSSupport-TroubleshootECSContainerInstance

Descrizione

Il `AWSSupport-TroubleshootECSContainerInstance` runbook ti aiuta a risolvere i problemi di un'istanza Amazon Elastic Compute Cloud (AmazonEC2) che non riesce a registrarsi con un cluster Amazon. ECS Questa automazione verifica se i dati utente per l'istanza contengono le

informazioni corrette sul cluster, se il profilo dell'istanza contiene le autorizzazioni richieste e i problemi di configurazione della rete.

> **Important**
>
> Per eseguire correttamente questa automazione, lo stato dell'EC2istanza Amazon deve essere `running` e lo stato del ECS cluster Amazon deve essere lo stesso`ACTIVE`.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del ECS cluster Amazon con cui l'istanza non è riuscita a registrarsi.
- InstanceId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'EC2istanza Amazon che desideri risolvere.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`

Fasi del documento

aws:executeScript: Verifica se l'EC2istanza Amazon soddisfa i prerequisiti necessari per la registrazione in un ECS cluster Amazon.

AWSSupport-TroubleshootECSTaskFailedToStart

Descrizione

Il `AWSSupport-TroubleshootECSTaskFailedToStart` runbook ti aiuta a risolvere il motivo per cui un'attività di Amazon Elastic Container Service (AmazonECS) in un ECS cluster Amazon non è riuscita ad avviarsi. È necessario eseguire questo runbook nello stesso modo in cui l'attività Regione AWS non è stata avviata. Il runbook analizza i seguenti problemi comuni che possono impedire l'avvio di un'attività:

- Connettività di rete al registro dei contenitori configurato
- IAMAutorizzazioni mancanti richieste dal ruolo di esecuzione dell'attività
- VPCconnettività degli endpoint
- configurazione delle regole del gruppo di sicurezza
- AWS Secrets Manager riferimenti segreti
- Configurazione della registrazione

> **Note**
>
> Se l'analisi determina che è necessario testare la connettività di rete, nell'account vengono creati una funzione Lambda e IAM il ruolo richiesto. Queste risorse vengono utilizzate per simulare la connettività di rete dell'operazione non riuscita. L'automazione elimina queste risorse quando non sono più necessarie. Tuttavia, se l'automazione non riesce a eliminare le risorse, è necessario farlo manualmente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del ECS cluster Amazon in cui l'attività non è stata avviata.

- CloudwatchRetentionPeriod

  Tipo: integer

  Descrizione: (Facoltativo) Il periodo di conservazione, in giorni, per i log delle funzioni Lambda da archiviare in Amazon Logs. CloudWatch Ciò è necessario solo se l'analisi determina che la connettività di rete deve essere testata.

  Valori validi: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Impostazione predefinita: 30

- TaskId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'operazione non riuscita. Utilizza l'ultima operazione non riuscita.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudtrail:LookupEvents`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`

- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ecr:DescribeImages
- ecr:GetRepositoryPolicy
- ecs:DescribeContainerInstances
- ecs:DescribeServices
- ecs:DescribeTaskDefinition
- ecs:DescribeTasks
- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:GetFunctionConfiguration
- lambda:InvokeFunction
- lambda:TagResource
- logs:DescribeLogGroups
- logs:PutRetentionPolicy
- secretsmanager:DescribeSecret

- `ssm:DescribeParameters`
- `sts:GetCallerIdentity`

Fasi del documento

- `aws:executeScript`- Verifica che l'utente o il ruolo che ha avviato l'automazione disponga delle autorizzazioni richieste. IAM Se non disponi di autorizzazioni sufficienti per utilizzare questo runbook, le autorizzazioni richieste mancanti vengono incluse nell'output dell'automazione.
- `aws:branch`- Suddivisione in base alla disponibilità o meno delle autorizzazioni per tutte le azioni richieste per il runbook.
- `aws:executeScript`- Crea una funzione Lambda nel tuo computer VPC se l'analisi determina che la connettività di rete deve essere testata.
- `aws:branch`- Filiali basate sui risultati del passaggio precedente.
- `aws:executeScript`- Analizza le possibili cause del mancato avvio dell'attività.
- `aws:executeScript`- Elimina le risorse create da questa automazione.
- `aws:executeScript`- Formatta l'output dell'automazione per restituire i risultati dell'analisi alla console. È possibile rivedere l'analisi dopo questo passaggio prima del completamento dell'automazione.
- `aws:branch`- Rami in base al fatto che la funzione Lambda e le risorse associate siano state create e debbano essere eliminate.
- `aws:sleep`- Dorme per 30 minuti in modo che l'interfaccia di rete elastica per la funzione Lambda possa essere eliminata.
- `aws:executeScript`- Elimina l'interfaccia di rete della funzione Lambda.
- `aws:executeScript`- Formatta l'output della fase di eliminazione dell'interfaccia di rete della funzione Lambda.

AWS-UpdateAmazonECSAgent

Descrizione

Il `AWS-UpdateAmazonECSAgent` runbook aggiorna l'agente Amazon Elastic Container Service (AmazonECS) sull'istanza Amazon Elastic Compute Cloud EC2 (Amazon) specificata. Questo runbook supporta solo istanze Amazon Linux e Amazon Linux 2.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Cluster ARN

  Tipo: StringList

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ECS cluster Amazon in cui sono registrate le tue istanze di container.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeImage`

- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Fasi del documento

`aws:executeScript`- Aggiorna l'ECSagente Amazon sul ECS cluster Amazon specificato nei `ClusterARN` parametri.

Output

UpdateAmazonECSAgent. UpdatedContainers - L'ID dell'istanza in cui l'aggiornamento dell'ECSagente Amazon è riuscito.

UpdateAmazonECSAgent. FailedContainers - L'ID dell'istanza in cui l'aggiornamento dell'ECSagente Amazon non è riuscito.

UpdateAmazonECSAgent. InProgressContainers - L'ID dell'istanza in cui è in corso l'aggiornamento dell'ECSagente Amazon.

Amazon EFS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic File System. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-CheckAndMountEFS

`AWSSupport-CheckAndMountEFS`

Descrizione

Il `AWSSupport-CheckAndMountEFS` runbook verifica i prerequisiti per montare il file system Amazon Elastic File System (AmazonEFS) e monta il file system sull'istanza Amazon Elastic

Compute Cloud (EC2Amazon) specificata. Questo runbook supporta il montaggio EFS del file system Amazon con il DNS nome o l'utilizzo dell'indirizzo IP del target di montaggio.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Azione

  Tipo: stringa

  Valori validi: Check | CheckAndMount

  Descrizione: (Obbligatorio) Determina se il runbook verifica i prerequisiti oppure verifica i prerequisiti e installa il file system.
- EfsId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del file system che si desidera montare.
- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'EC2istanza Amazon su cui desideri montare il file system.

- MountOptions

  Tipo: stringa

  Descrizione: (Facoltativo) Le opzioni supportate dall'assistente di EFS montaggio di Amazon che desideri utilizzare per il montaggio del file system. Se specifichi l'`tls`opzione, verifica che stunnel sia stato aggiornato sull'istanza di destinazione.

- MountPoint

  Tipo: stringa

  Descrizione: (Facoltativo) La directory in cui si desidera montare il file system. Se si specifica il `Check` valore per il `Action` parametro, questo parametro non deve essere specificato.

- MountTargetIP

  Tipo: stringa

  Descrizione: (Facoltativo) L'indirizzo IP del target di montaggio. Il montaggio per indirizzo IP funziona in ambienti in cui DNS è disabilitato, come i cloud privati virtuali (VPCs) con DNS nomi host disabilitati. Inoltre, puoi utilizzare questa opzione se il tuo ambiente utilizza un DNS provider diverso da Amazon Route 53 (Route 53).

- Regione

  Tipo: stringa

  Descrizione: (Obbligatorio) La posizione Regione AWS in cui si trovano l'EC2istanza e il file system di Amazon.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`

- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:StartAutomationExecution
- iam:ListRoles
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- elasticfilesystem:DescribeFileSystemPolicy
- elasticfilesystem:DescribeMountTargets
- elasticfilesystem:DescribeMountTargetSecurityGroups
- resource-groups:*

Fasi del documento

- aws:executeScript- Raccoglie dettagli sull'EC2istanza Amazon specificata nel InstanceId parametro.
- aws:executeScript- Raccoglie dettagli sul file system specificato nel EfsId parametro.
- aws:executeScript- Verifica che il gruppo di sicurezza associato al file system consenta il traffico sulla porta 2049 dall'EC2istanza Amazon specificata nel InstanceId parametro.
- aws:assertAwsResourceProperty- Verifica che l'EC2istanza Amazon specificata nel InstanceId parametro sia gestita da Systems Manager e che lo stato sia0nline.
- aws:branch- Filiali in base al valore specificato per il Action parametro.
- aws:runCommand- Verifica i prerequisiti per il montaggio del file system specificato nel EfsId parametro.
- aws:runCommand- Verifica i prerequisiti per il montaggio del file system specificato nel EfsId parametro e monta il file system sull'EC2istanza Amazon specificata nel parametro. InstanceId

Amazon EKS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Kubernetes Service. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWSSupport-CollectEKSInstanceLogs`

Descrizione

Il `AWSSupport-CollectEKSInstanceLogs` runbook raccoglie i file di log relativi al sistema operativo e ad Amazon Elastic Kubernetes Service EKS (Amazon) da un'istanza Amazon Elastic Compute Cloud EC2 (Amazon) per aiutarti a risolvere i problemi più comuni. Mentre l'automazione raccoglie i file di registro associati, vengono apportate modifiche alla struttura del file system, tra cui la creazione di directory temporanee, la copia dei file di registro nelle directory temporanee e la compressione dei file di registro in un archivio. Questa attività può comportare un aumento dell'istanza`CPUUtilization`. EC2 Per ulteriori informazioni`CPUUtilization`, consulta le metriche delle istanze nella Amazon CloudWatch User Guide.

Se specifichi un valore per il `LogDestination` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dall'EC2istanza, se lo stato della policy `isPublic` è impostato su o se l'access control list (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di `All`

`Users` Amazon S3, i log non vengono caricati. `true` Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> Questa automazione richiede almeno il 10% dello spazio su disco disponibile sul volume root Amazon Elastic Block Store (AmazonEBS) collegato all'EC2istanza. Se lo spazio su disco disponibile sul volume principale non è sufficiente, l'automazione si interrompe.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EKSInstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) ID dell'EKSEC2istanza Amazon da cui desideri raccogliere i log.
- LogDestination

Tipo: stringa

Descrizione: (Facoltativo) Il bucket S3 nel tuo account in cui caricare i log archiviati.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`

Consigliamo che l'EC2istanza che riceve il comando abbia un IAM ruolo con la policy gestita di mazonSSMManaged InstanceCore Amazon A allegata. Per caricare l'archivio di log nel bucket S3 specificato nel `LogDestination` parametro, devi aggiungere l'`s3:PutObject`autorizzazione.

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il sistema operativo del valore specificato nel `EKSInstanceId` parametro è Linux.
- `aws:runCommand`- Raccoglie i file di registro EKS relativi al sistema operativo e ad Amazon, comprimendoli in un archivio nella `/var/log` directory.
- `aws:branch`- Conferma se è stato specificato un valore per il `LogDestination` parametro.
- `aws:runCommand`- Carica l'archivio di log nel bucket S3 specificato nel parametro. `LogDestination`

`AWS-CreateEKSClusterWithFargateProfile`

Descrizione

Il `AWS-CreateEKSClusterWithFargateProfile` runbook crea un cluster Amazon Elastic Kubernetes Service EKS (Amazon) utilizzando un. AWS Fargate

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Un nome univoco per il cluster.
- ClusterRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN IAM ruolo che fornisce le autorizzazioni al piano di controllo di Kubernetes per effettuare chiamate alle AWS API operazioni per tuo conto.
- FargateProfileName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del profilo Fargate.
- FargateProfileRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il IAM ruolo ARN di esecuzione di Amazon EKS Pod.

- FargateProfileSelectors

  Tipo: stringa

  Descrizione: (Obbligatorio) I selettori per abbinare i pod al profilo Fargate.

- SubnetIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Le IDs sottoreti che desideri utilizzare per il tuo cluster AmazonEKS. Amazon EKS crea interfacce di rete elastiche in queste sottoreti per la comunicazione tra i nodi e il piano di controllo Kubernetes. È necessario specificare almeno due sottoreti. IDs

- EKSEndpointPrivateAccess

  Tipo: Booleano

  Impostazione predefinita: True

  Descrizione: (Facoltativo) Imposta questo valore per `True` consentire l'accesso privato all'endpoint del server Kubernetes API del cluster. Se abiliti l'accesso privato, le API richieste Kubernetes provenienti dall'interno del cluster utilizzano l'endpoint privato. VPC VPC Se disabiliti l'accesso privato e hai nodi o AWS Fargate pod nel cluster, assicurati che `publicAccessCidrs` includano i CIDR blocchi necessari per la comunicazione con i nodi o i pod Fargate.

- EKSEndpointPublicAccess

  Tipo: Booleano

  Impostazione predefinita: False

  Descrizione: (Facoltativo) Imposta questo valore su per `False` disabilitare l'accesso pubblico all'endpoint del server API Kubernetes del cluster. Se disabiliti l'accesso pubblico, il API server Kubernetes del cluster può ricevere richieste solo dall'interno del luogo in cui è stato avviato. VPC

- PublicAccessCIDRs

  Tipo: StringList

  Descrizione: (Facoltativo) I CIDR blocchi a cui è consentito l'accesso all'endpoint del server Kubernetes API pubblico del cluster. La comunicazione all'endpoint da indirizzi esterni ai CIDR blocchi specificati è negata. Se hai disabilitato l'accesso privato agli endpoint e hai nodi o pod Fargate nel cluster, assicurati di specificare i blocchi necessari. CIDR

- SecurityGroupIds

  Tipo: StringList

  Descrizione: (Facoltativo) Specificate uno o più gruppi di sicurezza da associare alle interfacce di rete elastiche create nel vostro account da AmazonEKS.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:CreateCluster`
- `eks:CreateFargateProfile`
- `eks:DescribeCluster`
- `eks:DescribeFargateProfile`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Fasi del documento

- reateEKSCluster (Caws:executeAwsApi) - Crea un EKS cluster Amazon.
- V erifyEKSCluster IsActive (aws: waitForAwsResourceProperty) - Verifica che lo stato del cluster sia`ACTIVE`.
- CreateFargateProfile (aws:executeAwsApi) - Crea un Fargate per il cluster.
- VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty) - Verifica che lo stato del profilo Fargate sia. `ACTIVE`

Output

`CreateEKSCluster.CreateClusterResponse`

Descrizione: risposta ricevuta dalla `CreateCluster` API chiamata.

`CreateFargateProfile.CreateFargateProfileResponse`

Descrizione: risposta ricevuta dalla `CreateFargateProfile` API chiamata.

AWS-CreateEKSClusterWithNodegroup

Descrizione

Il `AWS-CreateEKSClusterWithNodegroup` runbook crea un cluster Amazon Elastic Kubernetes Service EKS (Amazon) utilizzando un gruppo di nodi per la capacità.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Un nome univoco per il cluster.

- ClusterRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN IAM ruolo che fornisce le autorizzazioni al piano di controllo di Kubernetes per effettuare chiamate alle AWS API operazioni per tuo conto.

- NodegroupName

  Tipo: stringa

  Descrizione: (Obbligatorio) Un nome univoco per il gruppo di nodi.

- NodegroupRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN IAM ruolo da associare al gruppo di nodi. Il daemon kubelet del nodo di EKS lavoro di Amazon effettua chiamate a AWS APIs tuo nome. I nodi ricevono le autorizzazioni per queste API chiamate tramite un profilo di IAM istanza e le politiche associate. Prima di poter avviare i nodi e registrarli in un cluster, è necessario creare un IAM ruolo per tali nodi da utilizzare al momento dell'avvio.

- SubnetIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Le IDs sottoreti che desideri utilizzare per il tuo cluster AmazonEKS. Amazon EKS crea interfacce di rete elastiche in queste sottoreti per la comunicazione tra i nodi e il piano di controllo Kubernetes. È necessario specificare almeno due sottoreti. IDs

- EKSEndpointPrivateAccess

  Tipo: Booleano

  Impostazione predefinita: True

  Descrizione: (Facoltativo) Imposta questo valore per `True` consentire l'accesso privato all'endpoint del server Kubernetes API del cluster. Se abiliti l'accesso privato, le API richieste Kubernetes

provenienti dall'interno del cluster utilizzano l'endpoint privato. VPC VPC Se disabiliti l'accesso privato e hai nodi o AWS Fargate pod nel cluster, assicurati che `publicAccessCidrs` includano i CIDR blocchi necessari per la comunicazione con i nodi o i pod Fargate.

- EKSEndpointPublicAccess

  Tipo: Booleano

  Impostazione predefinita: False

  Descrizione: (Facoltativo) Imposta questo valore su per `False` disabilitare l'accesso pubblico all'endpoint del server API Kubernetes del cluster. Se disabiliti l'accesso pubblico, il API server Kubernetes del cluster può ricevere richieste solo dall'interno del luogo in cui è stato avviato. VPC
- PublicAccessCIDRs

  Tipo: StringList

  Descrizione: (Facoltativo) I CIDR blocchi a cui è consentito l'accesso all'endpoint del server Kubernetes API pubblico del cluster. La comunicazione all'endpoint da indirizzi esterni ai CIDR blocchi specificati è negata. Se hai disabilitato l'accesso privato agli endpoint e hai nodi o pod Fargate nel cluster, assicurati di specificare i blocchi necessari. CIDR
- SecurityGroupIds

  Tipo: StringList

  Descrizione: (Facoltativo) Specificate uno o più gruppi di sicurezza da associare alle interfacce di rete elastiche create nel vostro account da AmazonEKS.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`

- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Fasi del documento

- reateEKSCluster (Caws:executeAwsApi) - Crea un EKS cluster Amazon.
- V erifyEKSCluster IsActive (aws: waitForAwsResourceProperty) - Verifica che lo stato del cluster sia`ACTIVE`.
- CreateNodegroup (aws:executeAwsApi) - Crea un gruppo di nodi per il cluster.
- VerifyNodegroupIsActive (aws: waitForAwsResourceProperty) - Verifica che lo stato del gruppo di nodi sia`ACTIVE`.

Output

- `CreateEKSCluster.CreateClusterResponse`: Risposta ricevuta dalla `CreateCluster` API chiamata.
- `CreateNodegroup.CreateNodegroupResponse`: Risposta ricevuta dalla `CreateNodegroup` API chiamata.

AWS-DeleteEKSCluster

Descrizione

Questo runbook elimina le risorse associate a un EKS cluster Amazon, inclusi i gruppi di nodi e i profili Fargate. Facoltativamente, puoi scegliere di eliminare tutti i nodi autogestiti, gli AWS CloudFormation stack utilizzati per creare i nodi e lo stack per il cluster. VPC CloudFormation Per ulteriori informazioni sull'eliminazione di un cluster, consulta la sezione Eliminazione di un cluster nella Amazon EKS User Guide.

> **Note**
>
> Se nel cluster sono presenti servizi attivi associati a un sistema di bilanciamento del carico, è necessario eliminare tali servizi prima di eliminare il cluster. In caso contrario, il sistema

non può eliminare i sistemi di bilanciamento del carico. Utilizzare la procedura seguente per trovare ed eliminare i servizi prima di eseguire il `AWS-DeleteEKSCluster` runbook.

Per individuare ed eliminare i servizi nel cluster

1. Installa l'utilità da riga di comando Kubernetes,. `kubectl` Per ulteriori informazioni, consulta Installazione di kubectl nella Amazon EKS User Guide.
2. Esegui il comando seguente per elencare tutti i servizi in esecuzione nel tuo cluster.

```
kubectl get svc --all-namespaces
```

3. Esegui il comando seguente per eliminare tutti i servizi a cui è associato un valore EXTERNAL - IP. Questi servizi sono gestiti da un sistema di bilanciamento del carico ed è necessario eliminarli in Kubernetes per consentire il corretto rilascio del sistema di bilanciamento del carico e delle risorse associate.

```
kubectl delete svc
service-name
```

Ora puoi eseguire il runbook. `AWS-DeleteEKSCluster`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EKSClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del EKS cluster Amazon da eliminare.

- VPCCloudFormationStack

  Tipo: stringa

  Descrizione: (Facoltativo) nome AWS CloudFormation dello stack VPC per il EKS cluster da eliminare. Ciò elimina lo AWS CloudFormation stack VPC e tutte le risorse create dallo stack.

- VPCCloudFormationStackRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il IAM ruolo che AWS CloudFormation presuppone l'eliminazione ARN dello stack. VPC CloudFormation AWS CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto.

- SelfManagedNodeStacks

  Tipo: stringa

  Descrizione: (Facoltativo) Elenco separato da virgole di nomi di AWS CloudFormation stack per i nodi autogestiti. Questo eliminerà gli stack per i nodi autogestiti. AWS CloudFormation

- SelfManagedNodeStacksRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il IAM ruolo che AWS CloudFormation presuppone l'eliminazione ARN degli stack di nodi autogestiti. AWS CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn:DeleteStack`

Fasi del documento

- `aws:executeScript`- DeleteNodeGroups: Trova ed elimina tutti i gruppi di nodi nel EKS cluster.
- `aws:executeScript`- DeleteFargateProfiles: Trova ed elimina tutti i profili Fargate nel EKS cluster.
- `aws:executeScript`- DeleteSelfManagedNodes: Elimina tutti i nodi autogestiti e gli CloudFormation stack utilizzati per creare i nodi.
- `aws:executeScript`- DeleteEKSCluster: elimina EKS il cluster.
- `aws:executeScript`- D eleteVPCCloudFormationStack: elimina lo VPC CloudFormation stack.

AWS-MigrateToNewEKSSelfManagedNodeGroup

Descrizione

Il `AWS-MigrateToNewEKSSelfManagedNodeGroup` runbook ti aiuta a creare un nuovo gruppo di nodi Linux Amazon Elastic Kubernetes Service EKS (Amazon) su cui migrare l'applicazione esistente. Per ulteriori informazioni, consulta la sezione Migrazione a un nuovo gruppo di nodi nella Amazon EKS User Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- OldStackName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome o l'ID dello stack esistente. AWS CloudFormation
- NewStackName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del nuovo AWS CloudFormation stack creato per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, il nome dello stack viene creato utilizzando il formato:. `NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*
- ClusterControlPlaneSecurityGroup

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID del gruppo di sicurezza che desideri che i nodi utilizzino per comunicare con il piano di EKS controllo di Amazon. Se non specifichi un valore per questo parametro, viene utilizzato il gruppo di sicurezza specificato nello AWS CloudFormation stack esistente.
- NodeInstanceType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di istanza che desideri utilizzare per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, viene utilizzato il tipo di istanza specificato nello AWS CloudFormation stack esistente.

- NodeGroupName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del nuovo gruppo di nodi. Se non si specifica un valore per questo parametro, viene utilizzato il nome del gruppo di nodi specificato nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero desiderato di nodi su cui scalare quando viene creato il nuovo stack. Questo numero deve essere maggiore o uguale al `NodeAutoScalingGroupMinSize` valore e minore o uguale a. `NodeAutoScalingGroupMaxSize` Se non si specifica un valore per questo parametro, viene utilizzata la capacità desiderata del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupMaxSize

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi può essere scalato orizzontalmente. Se non specifichi un valore per questo parametro, viene utilizzata la dimensione massima del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupMinSize

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero minimo di nodi fino a cui il gruppo di nodi può scalare. Se non specifichi un valore per questo parametro, viene utilizzata la dimensione minima del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeImageId

  Tipo: stringa

Descrizione: (Facoltativo) L'ID del Amazon Machine Image (AMI) che desideri venga utilizzato dal gruppo di nodi.

- NodeImageIdSSMParam

  Tipo: stringa

  Descrizione: (Facoltativo) Il parametro pubblico Systems Manager AMI che si desidera venga utilizzato dal gruppo di nodi.

- NodeVolumeSize

  Tipo: stringa

  Descrizione: (Facoltativo) La dimensione del volume root per i nodi in GiB. Se non si specifica un valore per questo parametro, viene utilizzata la dimensione del volume del nodo specificata nello AWS CloudFormation stack esistente.

- NodeVolumeType

  Tipo: stringa

  Descrizione: (Facoltativo) Il tipo di EBS volume Amazon che desideri utilizzare per il volume root dei tuoi nodi. Se non specifichi un valore per questo parametro, viene utilizzato il tipo di volume specificato nello AWS CloudFormation stack esistente.

- KeyName

  Tipo: stringa

  Descrizione: (Facoltativo) La coppia di chiavi che desideri assegnare ai tuoi nodi. Se non si specifica un valore per questo parametro, viene utilizzata la coppia di chiavi specificata nello AWS CloudFormation stack esistente.

- Sottoreti

  Tipo: StringList

  Descrizione: (Facoltativo) Un elenco separato da virgole della sottorete IDs da utilizzare per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, vengono utilizzate le sottoreti specificate nello stack esistente. AWS CloudFormation

- D 1 isableIMDSv

Tipo: Booleano

Descrizione: (Facoltativo) `true` Specificare la disattivazione del servizio di metadati dell'istanza versione 1 (IMDSv1). Per impostazione predefinita, i nodi supportano IMDSv1 eIMDSv2.

- BootstrapArguments

  Tipo: stringa

  Descrizione: (Facoltativo) Argomenti aggiuntivi da passare allo script di bootstrap del nodo.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `autoscaling:CreateAutoScalingGroup`
- `autoscaling:CreateOrUpdateTags`
- `autoscaling:DeleteTags`
- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `autoscaling:DescribeScheduledActions`
- `autoscaling:SetDesiredCapacity`
- `autoscaling:TerminateInstanceInAutoScalingGroup`
- `autoscaling:UpdateAutoScalingGroup`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AuthorizeSecurityGroupEgress`

- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateLaunchTemplateVersion
- ec2:CreateLaunchTemplate
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteLaunchTemplate
- ec2:DeleteSecurityGroup
- ec2:DescribeAvailabilityZones
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstanceStatus
- ec2:DescribeInstances
- ec2:DescribeKeyPairs
- ec2:DescribeLaunchTemplateVersions
- ec2:DescribeLaunchTemplates
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:GetInstanceProfile
- iam:GetRole

- `iam:PassRole`

Fasi del documento

- DetermineParameterValuesForNewNodeGroup (aws:executeScript) - Raccoglie i valori dei parametri da utilizzare per il nuovo gruppo di nodi.
- CreateStack (aws:createStack) - Crea lo AWS CloudFormation stack per il nuovo gruppo di nodi.
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - Ottiene il ruolo dell'istanza del nodo.
- GetNewStackSecurityGroup (aws:executeAwsApi) - Il passaggio ottiene il gruppo di sicurezza del nodo.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - Aggiunge regole di ingresso al gruppo di sicurezza appena creato in modo che possa accettare il traffico proveniente da quello assegnato al gruppo di nodi precedente.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) - Aggiunge regole di ingresso al gruppo di sicurezza precedente in modo che possa accettare il traffico proveniente da quello assegnato al gruppo di nodi appena creato.
- VerifyStackComplete (aws: assertAwsResource Property) - Verifica che il nuovo stato dello stack sia. `CREATE_COMPLETE`

Output

DetermineParameterValuesForNewNodeGroup. NewStackParameters - I parametri utilizzati per creare il nuovo stack.

GetNewStackNodeInstanceRole. NewNodeInstanceRole - Il ruolo dell'istanza del nodo per il nuovo gruppo di nodi.

GetNewStackSecurityGroup. NewNodeSecurityGroup - L'ID del gruppo di sicurezza per il nuovo gruppo di nodi.

DetermineParameterValuesForNewNodeGroup. NewStackName - Il nome AWS CloudFormation dello stack per il nuovo gruppo di nodi.

CreateStack. StackId - L'ID AWS CloudFormation dello stack per il nuovo gruppo di nodi.

AWSPremiumSupport-TroubleshootEKSCluster

Descrizione

Il `AWSPremiumSupport-TroubleshootEKSCluster` runbook diagnostica i problemi più comuni relativi a un cluster Amazon Elastic Kubernetes Service EKS (Amazon), all'infrastruttura sottostante e fornisce i passaggi di correzione consigliati.

> **Important**
>
> L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, consulta Compare AWS Support Plans.

Se specifichi un valore per il `S3BucketName` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dall'EC2istanza, se lo stato della policy `isPublic` è impostato su o se l'access control list (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di `All Users` Amazon S3, i log non vengono caricati. `true` Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del EKS cluster Amazon di cui desideri risolvere i problemi.

- S3 BucketName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del bucket Amazon S3 privato in cui caricare il report generato dal runbook.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkAcls`
- `iam:GetInstanceProfile`
- `iam:ListInstanceProfiles`
- `iam:ListAttachedRolePolicies`
- `eks:DescribeCluster`
- `eks:ListNodegroups`
- `eks:DescribeNodegroup`

- `autoscaling:DescribeAutoScalingGroups`

Inoltre, la policy AWS Identity and Access Management (IAM) allegata all'utente o al ruolo che avvia l'automazione deve consentire il `ssm:GetParameter` funzionamento con i seguenti AWS Systems Manager parametri pubblici per ottenere l'ultima versione di Amazon EKS Amazon Machine Image (AMI) consigliata per i nodi di lavoro.

- `arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2/recommended/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/ami-windows-latest/Windows_Server-1909-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm:::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2-gpu/recommended/image_id`

Per caricare il report generato dal runbook in un bucket Amazon S3, sono necessarie le seguenti autorizzazioni per il bucket Amazon S3 specificato.

- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`
- `s3:PutObject`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli per il EKS cluster Amazon specificato.
- `aws:executeScript`- Raccoglie i dettagli delle istanze Amazon Elastic Compute Cloud EC2 (Amazon), dei gruppi di Auto Scaling e dei tipi di istanze AMI grafiche Amazon. EC2 GPU
- `aws:executeScript`- Raccoglie i dettagli del cloud privato virtuale (VPC), delle sottoreti, dei gateway di traduzione degli indirizzi di rete (NAT), dei percorsi di sottorete, dei gruppi di sicurezza e delle liste di controllo degli accessi alla rete () ACLs del cluster Amazon. EKS
- `aws:executeScript`- Raccoglie i dettagli dei profili delle istanze allegati e delle politiche dei ruoliIAM.

- `aws:executeScript`- Raccoglie i dettagli del bucket Amazon S3 specificato nel parametro. `S3BucketName`
- `aws:executeScript`- Classifa le VPC sottoreti Amazon come pubbliche o private.
- `aws:executeScript`- Controlla le VPC sottoreti Amazon per i tag necessari come parte di un cluster AmazonEKS.
- `aws:executeScript`- Controlla nelle VPC sottoreti Amazon i tag necessari per le sottoreti Elastic Load Balancing.
- `aws:executeScript`- Verifica se le istanze Amazon del nodo di lavoro utilizzano EC2 le ultime istanze EKS ottimizzate per AMI Amazon
- `aws:executeScript`- Verifica se i gruppi VPC di sicurezza Amazon sono collegati ai nodi di lavoro per i tag richiesti.
- `aws:executeScript`- Verifica le regole di ingresso consigliate nel EKS cluster Amazon e nel nodo di lavoro del gruppo di VPC sicurezza Amazon per verificare le regole di ingresso consigliate per il EKS cluster Amazon.
- `aws:executeScript`- Verifica le regole del gruppo di VPC sicurezza Amazon del EKS cluster Amazon e del nodo di lavoro per verificare le regole di uscita consigliate dal EKS cluster Amazon.
- `aws:executeScript`- Verifica la ACL configurazione di rete delle VPC sottoreti Amazon.
- `aws:executeScript`- Verifica se le EC2 istanze Amazon del nodo di lavoro dispongono delle politiche gestite richieste.
- `aws:executeScript`- Verifica se i gruppi Auto Scaling dispongono dei tag necessari per la scalabilità automatica del cluster.
- `aws:executeScript`- Verifica se le EC2 istanze Amazon del nodo di lavoro sono connesse a Internet.
- `aws:executeScript`- Genera un rapporto basato sugli output dei passaggi precedenti. Se viene specificato un valore per il `S3BucketName` parametro, il report generato viene caricato nel bucket Amazon S3.

AWSSupport-TroubleshootEKSWorkerNode

Descrizione

Il `AWSSupport-TroubleshootEKSWorkerNode` runbook analizza un nodo di lavoro Amazon Elastic Compute Cloud (AmazonEC2) e un cluster Amazon Elastic Kubernetes Service EKS

(Amazon) per aiutarti a identificare e risolvere le cause più comuni che impediscono ai nodi di lavoro di entrare a far parte di un cluster. Il runbook fornisce indicazioni per aiutarti a risolvere eventuali problemi identificati.

> **Important**
>
> Per eseguire correttamente questa automazione, lo stato del tuo nodo EC2 di lavoro Amazon deve essere `running` e lo stato del EKS cluster Amazon deve essere`ACTIVE`.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del EKS cluster Amazon.
- WorkerID

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del nodo di EC2 lavoro Amazon che non è riuscito a entrare a far parte del cluster.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeDhcpOptions`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

- `ssm:SendCommand`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il EKS cluster Amazon specificato nel `ClusterName` parametro esiste e si trova in uno `ACTIVE` stato.
- `aws:assertAwsResourceProperty`- Conferma che il EC2 nodo di lavoro Amazon specificato nel `WorkerID` parametro esiste e si trova in uno `running` stato.
- `aws:executeScript`- Esegue uno script Python che aiuta a identificare le possibili cause del mancato ingresso del nodo di lavoro nel cluster.

AWS-UpdateEKSCluster

Descrizione

Il `AWS-UpdateEKSCluster` runbook ti aiuta ad aggiornare il cluster Amazon Elastic Kubernetes Service EKS (Amazon) alla versione Kubernetes che desideri utilizzare.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del tuo EKS cluster Amazon.

- Versione

  Tipo: stringa

  Descrizione: (Obbligatoria) La versione di Kubernetes a cui desideri aggiornare il cluster.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

Fasi del documento

- `aws:executeAwsApi`- Aggiorna la versione di Kubernetes utilizzata dal tuo cluster Amazon. EKS
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'aggiornamento sia. `Successful`

AWS-UpdateEKSManagedNodeGroup

Descrizione

Il `AWS-UpdateEKSManagedNodeGroup` runbook ti aiuta ad aggiornare un gruppo di nodi gestiti di Amazon Elastic Kubernetes Service EKS (Amazon). Puoi scegliere o aggiornare. `Version` `Configuration`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del cluster di cui si desidera aggiornare il gruppo di nodi.
- NodeGroupName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del gruppo di nodi da aggiornare.
- UpdateType

  Tipo: stringa

  Valori validi: Aggiorna la versione del gruppo di nodi | Aggiorna le configurazioni del gruppo di nodi

  Impostazione predefinita: aggiorna la versione del gruppo di nodi

  Descrizione: (Obbligatorio) Il tipo di aggiornamento che si desidera eseguire sul gruppo di nodi.

I seguenti parametri si applicano solo al tipo di `Version` aggiornamento:

- AMIReleaseVersion

  Tipo: stringa

  Descrizione: (Facoltativa) La versione EKS ottimizzata di Amazon AMI che desideri utilizzare. Per impostazione predefinita viene utilizzata la versione più recente.
- ForceUpgrade

  Tipo: Booleano

  Descrizione: (Facoltativo) Se impostato su true, l'aggiornamento non fallirà a causa di una violazione del budget di interruzione del pod.
- KubernetesVersion

  Tipo: stringa

  Descrizione: (Facoltativo) La versione di Kubernetes a cui aggiornare il gruppo di nodi.
- LaunchTemplateId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID del modello di lancio.
- LaunchTemplateName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del modello di lancio.
- LaunchTemplateVersion

  Tipo: stringa

  Descrizione: (Facoltativo) La versione del modello di lancio di Amazon Elastic Compute Cloud (AmazonEC2). Questo parametro è valido solo se un gruppo di nodi è stato creato da un modello di lancio.

I seguenti parametri si applicano solo al tipo di `Configuration` aggiornamento:

- AddOrUpdateNodeGroupLabels

  Tipo: StringMap

Descrizione: (Facoltativo) etichette Kubernetes che desideri aggiungere o aggiornare.

- AddOrUpdateKubernetesTaintsEffect

  Tipo: StringList

  Descrizione: (Facoltativo) I taint Kubernetes che desideri aggiungere o aggiornare.

- MaxUnavailableNodeGroups

  Tipo: integer

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) Il numero massimo di nodi che non sono disponibili contemporaneamente durante un aggiornamento della versione.

- MaxUnavailablePercentageNodeGroup

  Tipo: integer

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) La percentuale di nodi che non sono disponibili durante un aggiornamento della versione.

- NodeGroupDesiredSize

  Tipo: integer

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) Il numero di nodi che il gruppo di nodi gestiti deve mantenere.

- NodeGroupMaxSize

  Tipo: integer

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi gestiti può scalare orizzontalmente.

- NodeGroupMinSize

  Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero minimo di nodi in cui il gruppo di nodi gestiti può scalare.

- RemoveKubernetesTaintsEffect

  Tipo: StringList

  Descrizione: (Facoltativo) Le taint Kubernetes che desideri rimuovere.

- RemoveNodeGroupLabels

  Tipo: StringList

  Descrizione: (Facoltativo) Un elenco di etichette separate da virgole che desideri rimuovere.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Fasi del documento

- `aws:executeScript`- Aggiorna un gruppo di nodi del EKS cluster Amazon in base ai valori specificati per i parametri di input del runbook.
- `aws:waitForAwsResourceProperty`- Attende che lo stato di aggiornamento del cluster sia. `Successful`

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descrizione

Il `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook aggiorna i gruppi di nodi gestiti in modo automatico nel cluster Amazon Elastic Kubernetes Service EKS (Amazon) utilizzando uno stack. AWS CloudFormation

Se il tuo cluster utilizza la scalabilità automatica, ti consigliamo di ridimensionare la distribuzione fino a due repliche prima di utilizzare questo runbook.

Per scalare una distribuzione a due repliche

1. Installa l'utilità della riga di comando Kubernetes,. `kubectl` Per ulteriori informazioni, consulta Installazione kubectl nella Amazon EKS User Guide.
2. Esegui il comando seguente.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Esegui il `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook.
4. Ridimensiona la distribuzione al numero di repliche desiderato eseguendo il comando seguente.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del EKS cluster Amazon.

- NodeGroupName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del gruppo di nodi gestito.

- ClusterControlPlaneSecurityGroup

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza del piano di controllo.

- D isableIMDSv 1.

  Tipo: Booleano

  Descrizione: (Facoltativo) Determina se si desidera consentire la versione 1 del servizio di metadati dell'istanza (IMDSv1) eIMDSv2.

- KeyName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome chiave per le istanze.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero di nodi che il gruppo di nodi deve mantenere.

- NodeAutoScalingGroupMaxSize

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi può scalare orizzontalmente.

- NodeAutoScalingGroupMinSize

  Tipo: stringa

Descrizione: (Facoltativo) Il numero minimo di nodi in cui il gruppo di nodi può scalare.

- NodeInstanceType

  Tipo: stringa

  Impostazione predefinita: t3.large

  Descrizione: (Facoltativo) Il tipo di istanza che desideri utilizzare per il gruppo di nodi.

- NodeImageId

  Tipo: stringa

  Descrizione: (Facoltativo) L'ID del Amazon Machine Image (AMI) che desiderate venga utilizzato dal gruppo di nodi.

- NodeImageIdSSMParam

  Tipo: stringa

  Predefinito: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Descrizione: (Facoltativo) Il parametro pubblico Systems Manager AMI che si desidera venga utilizzato dal gruppo di nodi.

- StackName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dello AWS CloudFormation stack utilizzato per aggiornare il gruppo di nodi.

- Sottoreti

  Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole delle IDs sottoreti che desideri vengano utilizzate dal cluster.

- VpcId

  Tipo: stringa

  Impostazione predefinita: Default

Descrizione: (Obbligatorio) Il cloud privato virtuale (VPC) in cui viene distribuito il cluster.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Fasi del documento

- `aws:executeScript`- Aggiorna un gruppo di nodi del EKS cluster Amazon in base ai valori specificati per i parametri di input del runbook.
- `aws:waitForAwsResourceProperty`- Attende che venga restituito lo stato di aggiornamento dello AWS CloudFormation stack.

Elastic Beanstalk

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Elastic Beanstalk Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-CollectElasticBeanstalkLogs

- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

AWSSupport-CollectElasticBeanstalkLogs

Descrizione

Il `AWSSupport-CollectElasticBeanstalkLogs` runbook raccoglie i file di log AWS Elastic Beanstalk correlati da un'Windows Serveristanza Amazon Elastic Compute Cloud (AmazonEC2) lanciata da Elastic Beanstalk per aiutarti a risolvere i problemi più comuni. Mentre l'automazione raccoglie i file di log associati, vengono apportate modifiche alla struttura del file system, tra cui la creazione di directory temporanee, la copia dei file di registro nelle directory temporanee e la compressione dei file di registro in un archivio. Questa attività può comportare un aumento `CPUUtilization` sull'EC2istanza Amazon. Per ulteriori informazioni`CPUUtilization`, consulta le metriche delle istanze nella Amazon CloudWatch User Guide.

Se specifichi un valore per il `S3BucketName` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dalla tua EC2 istanza Amazon, se lo stato della policy `isPublic` è impostato su o se l'access control list (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di `All Users` Amazon S3, i log non vengono caricati. `true` Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Se non specifichi un valore per il `S3BucketName` parametro, l'automazione carica il pacchetto di log nel bucket Elastic Beanstalk Amazon S3 predefinito nel punto in cui esegui l'automazione. Regione AWS La directory viene denominata in base alla seguente struttura,. `elasticbeanstalk-` *`region`* `-` *`accountID`* Il *`region`* e *`accountID`* i valori differiranno in base alla regione in Account AWS cui si esegue l'automazione. Il pacchetto di log verrà salvato nella `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* directory. Il *`environmentID`* e *`instanceID`* i valori differiranno in base al tuo ambiente Elastic Beanstalk e all'istanza Amazon da cui stai raccogliendo EC2 i log.

Per impostazione predefinita, il profilo di istanza AWS Identity and Access Management (IAM) collegato alle EC2 istanze Amazon dell'ambiente Elastic Beanstalk dispone delle autorizzazioni necessarie per caricare il pacchetto nel bucket Elastic Beanstalk Amazon S3 predefinito per

il tuo ambiente. Se specifichi un valore per il `S3BucketName` parametro, il profilo dell'istanza collegato all'EC2istanza Amazon deve consentire le `s3:PutObject` azioni`s3:GetBucketAcl`, `s3:GetBucketPolicys3:GetBucketPolicyStatus`, e per il bucket e il percorso Amazon S3 specificati.

> **Note**
>
> Questa automazione richiede almeno 500 MB di spazio su disco disponibile sul volume root Amazon Elastic Block Store (AmazonEBS) collegato alla tua EC2 istanza Amazon. Se lo spazio su disco disponibile sul volume principale non è sufficiente, l'automazione si interrompe.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EnvironmentId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk da cui desideri raccogliere il pacchetto di log.

- InstanceId

  Tipo: stringa

  (Obbligatorio) L'ID dell'EC2istanza Amazon nel tuo ambiente Elastic Beanstalk da cui desideri raccogliere il pacchetto di log.

- S3 BucketName

  Tipo: stringa

  (Facoltativo) Il bucket Amazon S3 in cui desideri caricare i log archiviati.

- S3 BucketPath

  Tipo: stringa

  (Facoltativo) Il percorso del bucket di Amazon S3 in cui desideri caricare il pacchetto di log. Questo parametro viene ignorato se non si specifica un valore per il parametro. `S3BucketName`

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che l'EC2istanza Amazon specificata nel `InstanceId` parametro è gestita da AWS Systems Manager.
- `aws:assertAwsResourceProperty`- Conferma che l'EC2istanza Amazon specificata nel `InstanceId` parametro è un'Windows Serveristanza.

- `aws:runCommand`- Verifica se l'istanza fa parte di un ambiente Elastic Beanstalk, se c'è spazio su disco sufficiente per raggruppare i log e se il bucket Amazon S3 in cui verranno caricati i log è pubblico.
- `aws:runCommand`- Raccoglie i file di log e carica l'archivio nel bucket Amazon S3 specificato nel parametro o nel bucket predefinito per `S3BucketName` l'ambiente Elastic Beanstalk se non viene specificato un valore.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Descrizione

Il `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` runbook consente la registrazione sull'ambiente AWS Elastic Beanstalk (Elastic Beanstalk) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- EnvironmentId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk a cui desideri abilitare l'accesso.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Fasi del documento

- `aws:executeAwsApi`- Abilita la registrazione sull'ambiente Elastic Beanstalk specificato nel parametro. `EnvironmentId`
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'ambiente cambi a. `Ready`
- `aws:executeScript`- Verifica che la registrazione sia stata abilitata nell'ambiente Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descrizione

Il `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook abilita le notifiche per l'ambiente AWS Elastic Beanstalk (Elastic Beanstalk) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- EnvironmentId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk per cui desideri abilitare le notifiche.
- TopicArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'argomento ARN di Amazon Simple Notification Service (AmazonSNS) a cui desideri inviare le notifiche.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Fasi del documento

- `aws:executeAwsApi`- Abilita le notifiche per l'ambiente Elastic Beanstalk specificato nel parametro. `EnvironmentId`
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'ambiente cambi a. `Ready`
- `aws:executeScript`- Verifica che le notifiche siano state abilitate per l'ambiente Elastic Beanstalk.

AWSSupport-TroubleshootElasticBeanstalk

Descrizione

Il `AWSSupport-TroubleshootElasticBeanstalk` runbook ti aiuta a risolvere i potenziali motivi per cui l'ambiente si trova in uno stato o. AWS Elastic Beanstalk `Degraded` `Severe` Questa automazione controlla le seguenti AWS risorse associate all'ambiente Elastic Beanstalk:

- Dettagli di configurazione per un sistema di bilanciamento del carico, uno AWS CloudFormation stack, un gruppo Amazon Auto EC2 Scaling, istanze Amazon Elastic Compute Cloud (EC2Amazon) e cloud privato virtuale (). VPC
- Problemi di configurazione della rete con le regole dei gruppi di sicurezza associati, le tabelle di routing e le liste di controllo dell'accesso alla rete (ACLs) associate alle sottoreti.
- Verifica la connettività agli endpoint Elastic Beanstalk e l'accesso pubblico a Internet.
- Verifica lo stato del load balancer.
- Verifica lo stato delle EC2 istanze Amazon.
- Recupera un pacchetto di log dall'ambiente Elastic Beanstalk e, facoltativamente, carica i file in. AWS Support

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ApplicationName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dell'applicazione Elastic Beanstalk.
- EnvironmentName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dell'ambiente Elastic Beanstalk.
- AWSS3UploaderLink

  Tipo: stringa

  Descrizione: (Facoltativo) URL Fornito all'utente AWS Support per caricare il pacchetto di log dall'ambiente Elastic Beanstalk su. Questa opzione è disponibile solo per i clienti che hanno acquistato un AWS Support piano e hanno aperto una richiesta di assistenza.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:Describe*`
- `cloudformation:Describe*`
- `cloudformation:Estimate*`

- cloudformation:Get*
- cloudformation:List*
- cloudformation:Validate*
- cloudwatch:Describe*
- cloudwatch:Get*
- cloudwatch:List*
- ec2:Describe*
- elasticbeanstalk:Check*
- elasticbeanstalk:Describe*
- elasticbeanstalk:List*
- elasticbeanstalk:RetrieveEnvironmentInfo*
- elasticbeanstalk:RequestEnvironmentInfo*
- elasticloadbalancing:Describe*
- rds:Describe*
- s3:Get*
- s3:List*
- sns:Get*
- sns:List*

Fasi del documento

- aws:executeScript- Verifica che il principale AWS Identity and Access Management (IAM) che ha avviato l'automazione disponga delle autorizzazioni necessarie per eseguire tutte le azioni definite nel runbook.
- aws:branch- Suddivide il flusso di lavoro in base ai risultati del passaggio precedente.
- aws:executeScript- Raccoglie informazioni sull'ambiente Elastic Beanstalk, tra cui il load balancer AWS CloudFormation , lo stack, il gruppo Auto Scaling, le istanze Amazon e la configurazione. EC2 VPC
- aws:executeScript- Verifica la presenza di problemi di connettività di rete con le tabelle di routing e i problemi associati alle sottoreti presenti nel tuo. ACLs VPC
- aws:executeScript- Verifica la presenza di problemi di connettività di rete con le regole del gruppo di sicurezza associate alle tue EC2 istanze Amazon.

- `aws:executeScript`- Verifica i controlli di stato per le EC2 istanze Amazon.
- `aws:executeScript`- Genera un link per un pacchetto di log del tuo ambiente Elastic Beanstalk.
- `aws:executeScript`- Carica il pacchetto di log su. AWS Support
- `aws:executeScript`- Genera un rapporto sulle azioni da intraprendere per aiutarti a risolvere i problemi che potrebbero influire sullo stato del tuo ambiente Elastic Beanstalk.

Sistema di bilanciamento del carico elastico

AWS Systems Manager L'automazione fornisce runbook predefiniti per Elastic Load Balancing. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWSConfigRemediation-DropInvalidHeadersForALB`

Descrizione

Il `AWSConfigRemediation-DropInvalidHeadersForALB` runbook consente all'application load balancer specificato di rimuovere le intestazioni con intestazioni non valide. HTTP

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- LoadBalancerArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) del sistema di bilanciamento del carico da cui desideri eliminare le intestazioni non valide.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita l'impostazione drop invalid header per il load balancer specificato nel parametro. `LoadBalancerArn`

- `aws:executeScript`- Verifica che l'impostazione drop invalid headers sia stata abilitata sul load balancer specificato nel parametro. `LoadBalancerArn`

AWS-EnableCLBAccessLogs

Descrizione

Il `AWS-EnableCLBAccessLogs` runbook abilita i log di accesso per un Classic Load Balancer.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EmitInterval

  Tipo: integer

  Valori validi: 5 | 60

  Impostazione predefinita: 60

  Descrizione: (Facoltativo) L'intervallo per la pubblicazione dei log di accesso in minuti.

- LoadBalancerNames

  Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole di Classic Load Balancer per cui si desidera abilitare i log di accesso.

- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui sono archiviati i log di accesso.

- S3 BucketPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) La gerarchia logica che hai creato per il tuo bucket Amazon S3, ad esempio. `my-bucket-prefix/prod` Se il prefisso non è fornito, il log viene posizionato al livello root del bucket.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita i log di accesso per i Classic Load Balancer specificati nel parametro. `LoadBalancerNames`

Output

E - Registri. nableCLBAccess SuccessesLoadBalancers - Elenco dei nomi dei sistemi di bilanciamento del carico in cui i log di accesso sono stati abilitati correttamente.

Registri E. nableCLBAccess FailedLoadBalancers - MapList dei nomi dei sistemi di bilanciamento del carico in cui l'attivazione dei log di accesso non è riuscita e il motivo dell'errore.

AWS-EnableCLBConnectionDraining

Descrizione

Il `AWS-EnableCLBConnectionDraining` runbook consente il drenaggio della connessione su un Classic Load Balancer CLB () fino al valore di timeout specificato. Il CLB drenaggio delle connessioni consente di completare le richieste in corso fatte alle istanze che stanno annullando la registrazione o che non sono funzionanti, con il timeout specificato che indica il momento in cui le connessioni vengono mantenute attive prima di segnalare l'annullamento della registrazione dell'istanza. Per ulteriori informazioni sull'esaurimento della connessione suCLBs, consulta Configurare il drenaggio della connessione per Classic Load Balancer nella Guida utente per Classic Load Balancer.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LoadBalancerName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del sistema di bilanciamento del carico su cui si desidera abilitare il drenaggio della connessione.

- ConnectionTimeout

  Tipo: integer

  Valori validi: 1-3600

  Impostazione predefinita: 300

  Descrizione: (Obbligatorio) Il valore di timeout della connessione per il sistema di bilanciamento del carico. Il valore di timeout può essere impostato tra 1 e 3600 secondi.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): Abilita il drenaggio della connessione e imposta il valore di timeout specificato per il load balancer specificato.
- VerifyLoadBalancerConnectionDrainingEnabled(aws: assertAwsResource Property): verifica che il drenaggio della connessione sia abilitato per il load balancer.
- VerifyLoadBalancerConnectionDrainingTimeout(aws: assertAwsResource Property): verifica che il valore di timeout della connessione per il sistema di bilanciamento del carico corrisponda al valore specificato.

`AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing`

Descrizione

Il `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` runbook abilita il bilanciamento del carico tra zone per il Classic Load Balancer CLB () specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- LoadBalancerName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del CLB dispositivo su cui desideri abilitare il bilanciamento del carico tra zone.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita il bilanciamento del carico tra zone per quanto CLB specificato nel parametro. `LoadBalancerName`
- `aws:assertAwsResourceProperty`- Verifica che il bilanciamento del carico tra zone sia stato abilitato su. CLB

`AWSConfigRemediation-EnableELBDeletionProtection`

Descrizione

Il `AWSConfigRemediation-EnableELBDeletionProtection` runbook abilita la protezione dall'eliminazione per l'elastic load balancer (ELB) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- LoadBalancerArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) su ELB cui desideri abilitare la protezione da eliminazione.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeScript`- Abilita la protezione dall'eliminazione sull'ELBintervallo specificato nel `LoadBalancerArn` parametro.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descrizione

Il `AWSConfigRemediation-EnableLoggingForALBAndCLB` runbook consente la registrazione per l' AWS Application Load Balancer o un Classic Load Balancer () specificato. CLB

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LoadBalancerId

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome Classic Load Balancer o l'Application Load Balancer. ARN

- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3.

- S3 BucketPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) La gerarchia logica che hai creato per il tuo bucket Amazon Simple Storage Service (Amazon S3), ad esempio. `my-bucket-prefix/prod` Se il prefisso non è fornito, il log viene posizionato al livello root del bucket.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeScript`- Abilita e verifica la registrazione per Classic Load Balancer o Application Load Balancer.

AWSSupport-TroubleshootCLBConnectivity

Descrizione

Il AWSSupport-TroubleshootCLBConnectivity runbook ti aiuta a risolvere i problemi di connettività tra istanze Classic Load Balancer (CLB) e Amazon Elastic Compute Cloud (Amazon). EC2 Inoltre, vengono esaminati i problemi di connettività tra un client e il. CLB Questo runbook esamina anche i controlli sanitari relativi aCLB, verifica che vengano seguite le migliori pratiche e crea una dashboard per la risoluzione dei problemi. Facoltativamente, puoi caricare l'output di automazione in un bucket Amazon Simple Storage Service (Amazon S3). Tuttavia, questo runbook non supporta il caricamento dell'output su bucket S3 accessibili al pubblico. Ti consigliamo di creare un bucket S3 temporaneo per questa automazione.

> **Important**
>
> L'utilizzo di questo runbook potrebbe comportare costi per la dashboard creata. Per ulteriori informazioni, consulta la pagina CloudWatchdei prezzi di Amazon

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InvestigationType

  Tipo: stringa

  Valori validi: Best practice | Problemi di connettività | Dashboard per la risoluzione dei problemi

  Descrizione: (Obbligatorio) Le operazioni che si desidera vengano eseguite dal runbook.

- LoadBalancerName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome di. CLB

- S3Location

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del bucket S3 a cui desideri inviare i risultati dell'automazione. I bucket accessibili pubblicamente non sono supportati. Se il bucket S3 utilizza la crittografia lato server, l'utente o il ruolo che esegue questa automazione deve disporre `kms:GenerateDataKey` delle autorizzazioni per la chiave. AWS KMS

- S3 LocationPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso chiave di Amazon S3 (sottocartella) in cui desideri caricare l'output dell'automazione. Il formato di output è memorizzato nel seguente formato: amzn-s3-demo-bucket/*S3LocationPrefix*/{{*InvestigationType*}} _ {{automazione:*EXECUTION_ID*}} .txt.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`

- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerPolicies
- elasticloadbalancing:DescribeInstanceHealth
- elasticloadbalancing:DescribeLoadBalancerAttributes
- iam:ListRoles
- cloudwatch:PutDashboard
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:SendCommand
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetPublicAccessBlock
- s3:PutObject

Fasi del documento

- aws:executeScript- Verifica che il valore CLB specificato nel LoadBalancerName parametro esista.

- `aws:branch`- Rami basati sul valore specificato per il `InvestigationType` parametro.
- `aws:executeScript`- Esegue controlli di connettività suCLB.
- `aws:executeScript`- Verifica che la CLB configurazione sia conforme alle best practice di Elastic Load Balancing.
- `aws:executeScript`- Crea una CloudWatch dashboard Amazon per il tuoCLB.
- `aws:executeScript`- Crea un file di testo con i risultati dell'automazione e lo carica nel bucket Amazon S3 specificato nel parametro. `S3Location`

Output

RunBestPractices.Riepilogo

RunConnectivityChecks.Riepilogo

CreateTroubleshootingDashboard.Uscita

UploadOutputToS3. Uscita

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing`

Descrizione

Il `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` runbook abilita il bilanciamento del carico tra zone per il network load balancer () specificato. NLB

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LoadBalancerArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) su NLB cui desideri abilitare il bilanciamento del carico tra zone.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita il bilanciamento del carico tra zone diverse per NLB quanto specificato nel `LoadBalancerArn` parametro.
- `aws:executeScript`- Verifica che il bilanciamento del carico tra zone sia stato abilitato su. NLB

AWS-UpdateALBDesyncMitigationMode

Descrizione

Il `AWS-UpdateALBDesyncMitigationMode` runbook aggiornerà la modalità di mitigazione desync su un Application Load Balancer ALB () alla modalità di mitigazione specificata. La modalità di mitigazione desync determina il modo in cui il load balancer gestisce le richieste che potrebbero rappresentare un rischio per la sicurezza dell'applicazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LoadBalancerArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) di ALB cui desideri modificare la modalità di mitigazione del desync.
- DesyncMitigationMode

  Tipo: stringa

  Valori validi: monitor | defensive | strictest

  Descrizione: (Obbligatoria) La modalità di mitigazione che desideri utilizzare. ALB Per informazioni sulle modalità di mitigazione della desincronizzazione, consulta la modalità di mitigazione di Desync nella Guida utente di Application Load Balancers.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- VerifyLoadBalancerType (aws: assertAwsResource Property): verifica che il valore specificato per il parametro di `LoadBalancerArn` input sia per un sistema di bilanciamento del carico delle applicazioni prima di procedere al passaggio successivo.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Aggiorna il ALB per utilizzare quanto specificato. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - Verifica che la modalità di mitigazione della desincronizzazione sia stata aggiornata per l'obiettivo. ALB

Output

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Caricamento del messaggio dello script che verifica la modifica apportata al tuo. ALB

AWS-UpdateCLBDesyncMitigationMode

Descrizione

Il `AWS-UpdateCLBDesyncMitigationMode` runbook aggiornerà la modalità di mitigazione della desincronizzazione su un Classic Load Balancer CLB () alla modalità di mitigazione specificata. La modalità di mitigazione desync determina il modo in cui il load balancer gestisce le richieste che potrebbero rappresentare un rischio per la sicurezza dell'applicazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LoadBalancerName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome di CLB cui si desidera modificare la modalità di mitigazione della desincronizzazione.
- DesyncMitigationMode

  Tipo: stringa

  Valori validi: monitor | defensive | strictest

  Descrizione: (Obbligatoria) La modalità di mitigazione che desideri utilizzare. CLB Per informazioni sulle modalità di mitigazione della desincronizzazione, consulta la modalità di mitigazione di Desync nella Guida utente di Application Load Balancers.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Aggiorna il file CLB per utilizzare quanto specificato`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - Verifica che la modalità di mitigazione della desincronizzazione sia stata aggiornata per l'obiettivo. CLB

Output

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Caricamento del messaggio dello script che verifica la modifica apportata al tuo. CLB

Amazon EMR

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. EMR Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

`AWSSupport-AnalyzeEMRLogs`

Descrizione

Questo runbook aiuta a identificare gli errori durante l'esecuzione di un job su un EMR cluster Amazon. Il runbook analizza un elenco di log definiti sul file system e cerca un elenco di parole chiave predefinite. Queste voci di registro vengono utilizzate per creare CloudWatch eventi Amazon Events in modo da poter intraprendere tutte le azioni necessarie in base agli eventi. Facoltativamente, il runbook pubblica le voci di registro nel gruppo di log Amazon CloudWatch Logs di tua scelta. Questo runbook attualmente cerca i seguenti errori e modelli nei file di registro:

- container_out_of_memory — Il YARN contenitore ha esaurito la memoria, l'esecuzione del processo potrebbe non riuscire.
- yarn_nodemanager_health: CORE o TASK node sta esaurendo lo spazio su disco e non sarà in grado di eseguire attività.
- node_state_change: o il nodo non è raggiungibile dal nodo. CORE TASK MASTER
- step_failure: Un passaggio non è riuscito. EMR
- no_core_nodes_running: Nessun nodo è attualmente in esecuzione, il cluster non è integro. CORE
- hdfs_missing_blocks: Ci sono blocchi mancanti che potrebbero portare alla perdita di dati. HDFS
- hdfs_high_util: HDFS L'utilizzo è elevato, il che può influire sui job e sullo stato del cluster.
- instance_controller_restart: il processo Instance-Controller è stato riavviato. Questo processo è essenziale per l'integrità del cluster.
- instance_controller_restart_legacy: il processo Instance-Controller è stato riavviato. Questo processo è essenziale per l'integrità del cluster.
- high_load: rilevata una media di carico elevata, può influire sulla segnalazione dello stato dei nodi o causare timeout o rallentamenti.
- yarn_node_blacklisted: oppure il nodo è stato inserito nella lista nera dall'esecuzione delle attività. CORE TASK YARN
- yarn_node_lost: o il nodo è stato contrassegnato come da, possibili problemi di connettività. CORE TASK LOST YARN

Le istanze associate a quanto specificato devono essere `ClusterID` gestite da. AWS Systems ManagerÈ possibile eseguire questa automazione una sola volta, pianificare l'automazione in modo che venga eseguita a un intervallo di tempo specifico o rimuovere una pianificazione creata in precedenza da un'automazione. Questo runbook supporta le EMR versioni di Amazon dalla 5.20 alla 6.30.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterID

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del cluster di cui si desidera analizzare i log dei nodi.
- Operazione

  Tipo: stringa

  Valori validi: Run Once | Schedule | Remove Schedule

  Descrizione: (Obbligatoria) L'operazione da eseguire sul cluster.
- IntervalTime

  Tipo: stringa

  Valori validi: 5 minuti | 10 minuti | 15 minuti

  Descrizione: (Facoltativo) L'intervallo di tempo che intercorre tra l'esecuzione dell'automazione. Questo parametro è applicabile solo se viene specificato `Schedule` per il `Operation` parametro.
- LogToCloudWatchLogs

  Tipo: stringa

  Valori validi: sì | no

  Descrizione: (Facoltativo) Se si specifica `yes` il valore di questo parametro, l'automazione crea un gruppo di log CloudWatch Logs con il nome specificato nel `CloudWatchLogGroup` parametro per memorizzare tutte le voci di registro corrispondenti.

- CloudWatchLogGroup

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del gruppo di log CloudWatch Logs in cui si desidera memorizzare tutte le voci di registro corrispondenti. Questo parametro è applicabile solo se viene specificato `yes` per il `LogToCloudWatchLogs` parametro.
- CreateLogInsightsDashboard

  Tipo: stringa

  Valori validi: sì | no

  Descrizione: (Facoltativo) Se si specifica`yes`, la CloudWatch dashboard viene creata se non esiste già. Questo parametro è applicabile solo se viene specificato `yes` per il `LogToCloudWatchLogs` parametro.
- CreateMetricFilters

  Tipo: stringa

  Valori validi: sì | no

  Descrizione: (Facoltativo) Specificate `yes` se desiderate creare filtri metrici per il gruppo di log CloudWatch Logs. Questo parametro è applicabile solo se si specifica `yes` per il `LogToCloudWatchLogs` parametro.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- iam:CreateRole
- iam:DeleteRole
- iam:GetRolePolicy
- iam:PutRolePolicy
- iam:DeleteRolePolicy
- iam:passrole
- cloudformation:DescribeStacks
- cloudformation:DeleteStack
- cloudformation:CreateStack
- events:DeleteRule
- events:RemoveTargets
- events:PutTargets
- events:PutRule
- events:DescribeRule
- logs:DescribeLogGroups
- logs:CreateLogGroup
- logs:PutMetricFilter
- cloudwatch:PutDashboard
- elasticmapreduce:ListInstances
- elasticmapreduce:DescribeCluster

Fasi del documento

- aws:executeAwsApi- Raccoglie informazioni sul EMR cluster Amazon specificato nel ClusterID parametro.
- aws:branch- Filiali basate sull'input.
  - Se l'operazione fornita è Run Once oSchedule:
    - aws:assertAwsResourceProperty- Verifica che il cluster sia disponibile.

- `aws:executeAwsApi`- Raccoglie tutte le istanze in esecuzione nel cluster. IDs
- `aws:assertAwsResourceProperty`- Verifica che l'SSMagente sia in esecuzione su tutte le istanze del cluster.
- `aws:branch`- Filiali a seconda che sia stata specificata l'esecuzione dell'automazione una sola volta o in base a una pianificazione.
  - Se l'operazione fornita è`Run Once`:
    - `aws:branch`- Rami basati sul valore specificato nel `LogToCloudWatchLogs` parametro.
      - Se `LogToCloudWatchLogs` il valore è`yes`:
        - `aws:executeScript`- Verifica se esiste `CloudWatchLogGroup` già un gruppo di log CloudWatch Logs con il nome specificato nel parametro. In caso contrario, il gruppo viene creato con il nome specificato.
        - `aws:branch`- Rami basati sul valore specificato nel `CreateMetricFilters` parametro.
          - Se `CreateMetricFilters` il valore è`yes`:
            - `aws:executeAwsApi`- Vengono eseguiti 12 passaggi per ogni filtro metrico
            - `aws:branch`- Rami basati sul valore specificato nel `CreateLogInsightsDashboard` parametro.
              - Se `CreateLogInsightsDashboard` il valore è`yes`:
                - `aws:executeAwsApi`- Crea una CloudWatch dashboard con lo stesso nome specificato nel `CloudWatchLogGroup` parametro, se non esiste già.
              - Se `CreateLogInsightsDashboard` il valore è`no`:
                - `aws:runCommand`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.
          - Se `CreateMetricFilters` il valore è`no`:
            - `aws:branch`- Rami basati sul valore specificato nel `CreateLogInsightsDashboard` parametro.
              - Se `CreateLogInsightsDashboard` il valore è`yes`:
                - `aws:executeAwsApi`- Crea una CloudWatch dashboard con lo stesso nome specificato nel `CloudWatchLogGroup` parametro, se non esiste già.
              - Se `CreateLogInsightsDashboard` il valore è`no`:
                - `aws:runCommand`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.

    - Se `LogToCloudWatchLogs` il valore èno:
      - `aws:executeAwsApi`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.
  - Se l'operazione fornita è`Schedule`:
    - `aws:createStack`- Crea un EventBridge evento Amazon destinato a questo runbook.
- Se l'operazione fornita è`Remove Schedule`:
  - `aws:executeAwsApi`- Verifica l'esistenza di una pianificazione per il cluster.
  - `aws:deleteStack`- Elimina la pianificazione.

Output

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstancesI. nstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.uscita

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Descrizione

Il `AWSSupport-DiagnoseEMRLogsWithAthena` runbook aiuta a diagnosticare EMR i log di Amazon utilizzando Amazon Athena in integrazione con Data Catalog. AWS Glue Amazon Athena viene utilizzato per interrogare i file di EMR log di Amazon per contenitori, log dei nodi o entrambi, con parametri opzionali per intervalli di date specifici o ricerche basate su parole chiave.

Il runbook può recuperare automaticamente la posizione del EMR log Amazon per un cluster esistente oppure puoi specificare la posizione del log di Amazon S3. Per analizzare i log, il runbook:

- Crea un AWS Glue database ed esegue query Amazon Athena Data Definition Language DDL () sulla posizione di log di Amazon EMR S3 per creare tabelle per i log del cluster e un elenco di problemi noti.

- Esegue query Data Manipulation Language (DML) per cercare modelli di problemi noti nei log di Amazon. EMR Le query restituiscono un elenco di problemi rilevati, il relativo numero di occorrenze e il numero di parole chiave corrispondenti in base al percorso del file Amazon S3.
- I risultati vengono caricati in un bucket Amazon S3 specificato sotto il prefisso. `saw_diagnose_EMR_known_issues`
- Il runbook restituisce i risultati delle query di Amazon Athena, evidenziando risultati, consigli e riferimenti agli articoli di Amazon Knowledge Center (KC) provenienti da un sottoinsieme predefinito.
- In caso di completamento o errore, il AWS Glue database e i file dei problemi noti caricati nel bucket Amazon S3 vengono eliminati.

Come funziona?

`AWSSupport-DiagnoseEMRLogsWithAthena`Eseguiamo l'analisi dei EMR log di Amazon utilizzando Amazon Athena per rilevare errori ed evidenziare risultati, consigli e articoli pertinenti del Knowledge Center.

Il runbook esegue i seguenti passaggi:

- Ottieni la posizione EMR del log del cluster Amazon utilizzando l'ID del cluster o inserisci la posizione Amazon S3 per recuperare la posizione e le dimensioni del log.
- Fornisci una stima dei costi di Athena in base alla dimensione della posizione del registro.
- Ottieni l'approvazione per procedere richiedendo l'approvazione ai IAM responsabili designati prima di eseguire le query su Athena e continuare con i passaggi successivi.
- Carica i problemi noti nel bucket Amazon S3 specificato, crea un AWS Glue database e tabelle.
- Esegui le query Athena sui dati dei log di AmazonEMR. Le query possono essere eseguite per intervallo di date, parole chiave, entrambi i criteri oppure essere eseguite senza filtri in base agli input forniti.
- Analizza i risultati per evidenziare i risultati, i consigli e gli articoli KC pertinenti.
- Link di output per i risultati delle DML query di Amazon Athena.
- Pulisci l'ambiente rimuovendo il database creato, le tabelle e i problemi noti caricati.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- atena: GetQueryExecution
- atena: StartQueryExecution
- atena: GetPreparedStatement
- atena: CreatePreparedStatement
- colla: GetDatabase
- colla: CreateDatabase
- colla: DeleteDatabase
- colla: CreateTable
- colla: GetTable
- colla: DeleteTable
- mappa elastica riduce: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- prezzi: GetProducts
- prezzi: GetAttributeValues
- prezzi: DescribeServices
- prezzi: ListPriceLists

Important

Per limitare l'accesso solo alle risorse necessarie a questa automazione, allega la seguente policy al IAM ruolo che attribuisce fiducia al SSM Servizio. Sostituisci Partition, Region e Account con i valori appropriati per la partizione, la regione e il numero di account in cui viene eseguito il runbook.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RestrictPutObjects",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
```

```
        "arn:{Partition}:s3:::*/*/results/*",
        "arn:{partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Sid": "RestrictDeleteAccess",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:{Partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:userDefinedFunction/
saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:CreateTable",
        "glue:GetTable",
        "glue:DeleteTable"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_known_issues",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_logs_table",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
j_*",
```

```
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    }
  ]
}
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Naviga AWSSupport-D iagnoseEMRLogs WithAthena nella AWS Systems Manager sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - ClusterId (obbligatorio):

     L'ID EMR del cluster Amazon.
   - S3 LogLocation (opzionale):

     La posizione del EMR log Amazon S3 di Amazon. Inserisci la posizione Amazon URL S3 in stile Path, ad esempio:. `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/` Fornisci questo parametro se il EMR cluster Amazon è stato chiuso per più di `30` giorni.
   - S3 BucketName (richiesto):

     Il nome del bucket Amazon S3 per caricare un elenco di problemi noti e l'output delle query Amazon Athena. Il bucket deve avere l'opzione Block Public Access abilitata e trovarsi nella stessa AWS regione e nello stesso account del EMR cluster Amazon.
   - Approvatori (obbligatori):

     L'elenco dei responsabili AWS autenticati che sono in grado di approvare o rifiutare l'azione. È possibile specificare i principali utilizzando uno dei seguenti formati: nome utente, utenteARN, IAM ruolo o ruolo di ruoloARN. IAM ARN Il numero massimo di approvatori è 10.

- FetchNodeLogsOnly (Facoltativo):

  Se impostato su`true`, l'automazione diagnostica i log dei contenitori delle EMR applicazioni Amazon. Il valore predefinito è `false`.

- FetchContainersLogsOnly(Facoltativo):

  Se impostato su`true`, l'automazione diagnostica i log dei EMR contenitori Amazon. Il valore predefinito è `false`.

- EndSearchDate (Facoltativo):

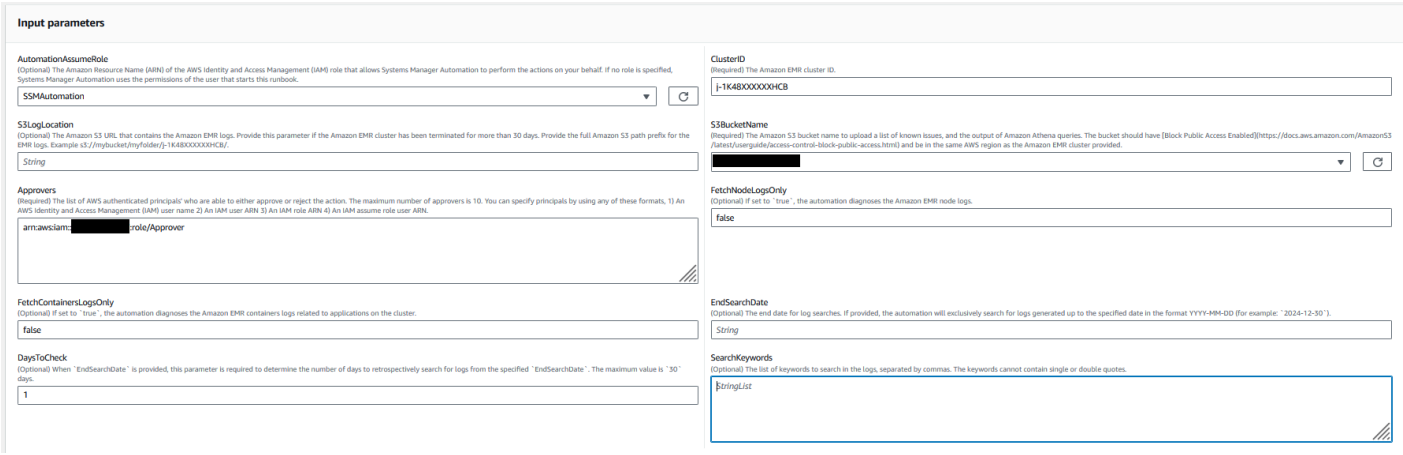
  La data di fine delle ricerche nei log. Se fornito, l'automazione cercherà esclusivamente i log generati fino alla data specificata nel formato YYYY -MM-DD (ad esempio:). `2024-12-30`

- DaysToCheck (Facoltativo):

  Quando `EndSearchDate` viene fornito, questo parametro è necessario per determinare il numero di giorni in cui cercare in modo retrospettivo i log tra quelli specificati. `EndSearchDate` Il valore massimo è in giorni. `30` Il valore predefinito è `1`.

- SearchKeywords (Facoltativo):

  L'elenco delle parole chiave da cercare nei log, separate da virgole. Le parole chiave non possono contenere virgolette singole o doppie.



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:

   - getLogLocation:

Recupera la posizione del log di Amazon S3 interrogando l'ID Amazon EMR Cluster specificato. Se l'automazione non è in grado di interrogare la posizione del registro dall'ID del EMR cluster Amazon, il runbook utilizza il parametro `S3LogLocation` di input.

- branchOnValidRegistro:

  Verifica la posizione dei EMR log di Amazon. Se la posizione è valida, procedi a stimare i costi potenziali di Amazon Athena durante l'esecuzione delle query sui log di Amazon. EMR

- estimateAthenaCosts:

  Determina la dimensione dei EMR log di Amazon e fornisce una stima dei costi per l'esecuzione delle scansioni Athena sul set di dati di log. Per le regioni non commerciali (non AWS partizioni), questo passaggio fornisce solo la dimensione del log senza stimare i costi. I costi possono essere calcolati utilizzando la documentazione sui prezzi di Athena nella regione specificata.

- approveAutomation:

  Attende l'approvazione dei IAM responsabili designati per procedere con le fasi successive dell'automazione. La notifica di approvazione contiene il costo stimato della scansione di Amazon Athena nei log di EMR Amazon e dettagli sulle risorse fornite dall'automazione.

- uploadKnownIssuesExecuteAthenaQueries:

  Carica i problemi noti predefiniti nel bucket Amazon S3 specificato nel parametro. `S3BucketName` Crea database e tabelle AWS Glue . Esegue le query di Amazon Athena nel database in base AWS Glue ai parametri di input.

- getQueryExecutionStato:

  Attende che l'esecuzione della query di Amazon Athena sia `SUCCEEDED` in corso. La DML query Amazon Athena cerca errori ed eccezioni nei log dei cluster AmazonEMR.

- analyzeAthenaResults:

  Analizza i risultati di Amazon Athena per fornire risultati, consigli e articoli del Knowledge Center (KC) provenienti da un set predefinito di mappature.

- getAnalyzeResultsQuery 1: ExecutionStatus

  Attende che l'esecuzione della query sia in corso. `SUCCEEDED` La query Amazon Athena analizza i risultati della DML query precedente. DML Questa query di analisi restituirà eccezioni corrispondenti con risoluzioni e articoli KC

- getAnalyzeResultsExecutionStatusQuery 2:

Attende che l'esecuzione della query sia in corso. `SUCCEEDED` La query Amazon Athena analizza i risultati della DML query precedente. DML Questa query di analisi restituirà un elenco di eccezioni/errori rilevati in ogni percorso di log di Amazon S3.

- printAthenaQueriesMessaggio:

  Stampa i link per i risultati delle DML query di Amazon Athena.

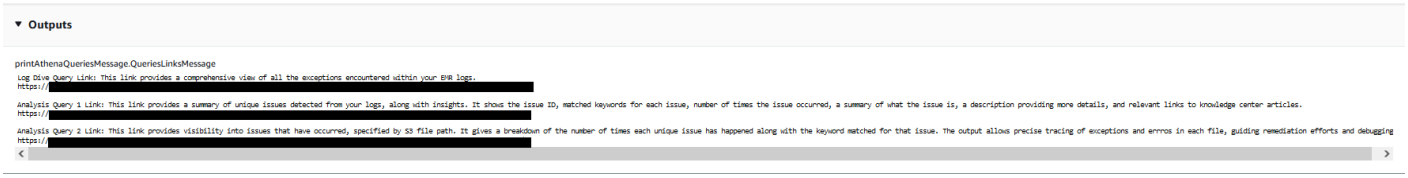
- cleanupResources:

  Pulisce le risorse eliminando il AWS Glue database creato ed eliminando i file con problemi noti creati nel bucket Amazon EMR logs.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

   L'output fornisce tre collegamenti per i risultati delle query Athena:

   - Elenco di tutti gli errori e le eccezioni ricorrenti presenti nei log del EMR cluster Amazon, insieme alle posizioni dei log corrispondenti (prefisso Amazon S3).
   - Riepilogo delle eccezioni note uniche riportate nei EMR log di Amazon, insieme alle risoluzioni consigliate e agli articoli KC per facilitare la risoluzione dei problemi.
   - Dettagli su dove compaiono errori ed eccezioni specifici nei percorsi di log di Amazon S3, per supportare ulteriori diagnosi.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Per ulteriori informazioni, consulta Troubleshooting Amazon EMR Clusters.

OpenSearch Servizio Amazon

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon OpenSearch Service. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

`AWSConfigRemediation-DeleteOpenSearchDomain`

Descrizione

Il `AWSConfigRemediation-DeleteOpenSearchDomain` runbook elimina il dominio Amazon OpenSearch Service specificato utilizzando. DeleteDomainAPI

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- DomainName

  Tipo: stringa

Valori consentiti: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri eliminare.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Fasi del documento

- `aws:executeScript`- Accetta il nome OpenSearch di dominio Amazon Service come input, lo elimina e verifica l'eliminazione.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descrizione

Il `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` runbook si abilita `EnforceHTTPS` su un determinato dominio Amazon OpenSearch Service utilizzando. UpdateDomainConfigAPI

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- DomainName

  Tipo: stringa

  Valori consentiti: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

  Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri utilizzare per l'applicazione. HTTPS
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Fasi del documento

- `aws:executeScript`- Abilita l'opzione `EnforceHTTPS` endpoint sul dominio Amazon OpenSearch Service specificato nel `DomainName` parametro.

`AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups`

Descrizione

Il `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` runbook aggiorna la configurazione del gruppo di sicurezza su un determinato dominio Amazon OpenSearch Service utilizzando il UpdateDomainConfigAPI.

> **Note**
>
> AWS I gruppi di sicurezza possono essere applicati solo ai domini Amazon OpenSearch Service configurati per Amazon Virtual Private Cloud (VPC) Access e non ai domini Amazon OpenSearch Service configurati per Public Access.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- DomainName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri utilizzare per aggiornare i gruppi di sicurezza.

- SecurityGroupList

  Tipo: StringList

  Descrizione: (Obbligatorio) Il gruppo di sicurezza IDs che desideri assegnare al dominio Amazon OpenSearch Service.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Fasi del documento

- `aws:executeScript`- Aggiorna la configurazione del gruppo di sicurezza sul dominio Amazon OpenSearch Service specificato nel `DomainName` parametro.

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`

Descrizione

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`il runbook di automazione viene utilizzato per identificare la causa dello stato di salute del cluster rosso o giallo e guidarti nella modifica del cluster in verde.

Come funziona?

Il runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` aiuta a risolvere la causa del cluster rosso o giallo e fornisce i passaggi successivi per risolvere questo problema analizzando la configurazione del cluster e l'utilizzo delle risorse.

Il runbook esegue i seguenti passaggi:

- Chiama il DescribeDomainAPIdominio di destinazione per ottenere la configurazione del cluster.
- Verifica se il dominio del OpenSearch servizio è basato su Internet (pubblico) o Amazon Virtual Private Cloud (VPC).
- Crea una AWS Lambda funzione pubblica o VPCbasata su Amazon a seconda della configurazione del cluster. Nota: la funzione Lambda contiene il codice di risoluzione dei problemi che esegue il OpenSearch servizio APIs sul cluster per determinare il motivo per cui il cluster è in rosso o giallo.
- Elimina la funzione Lambda.
- Visualizza i controlli eseguiti e i passaggi successivi consigliati per risolvere il problema del cluster rosso o giallo.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`

- cloudformation:DescribeStackEvents
- cloudformation:DeleteStack
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:InvokeFunction
- lambda:GetFunction
- es:DescribeDomain
- es:DescribeDomainConfig
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:DeleteNetworkInterface
- ec2:DescribeInstances
- ec2:AttachNetworkInterface
- cloudwatch:GetMetricData
- iam:PassRole

Il LambdaExecutionRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface

Panoramica della LambdaExecutionRole politica:

Di seguito è riportato un esempio del ruolo di esecuzione (AWS Identity and Access Management (IAM)) di una funzione Lambda che concede alla funzione il permesso di accedere ai AWS servizi

e alle risorse richiesti da questo runbook. Per ulteriori informazioni, consulta Ruolo di esecuzione Lambda.

> **Note**
>
> I `ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface`, e `ec2:DeleteNetworkInterface` sono necessari solo se il cluster di OpenSearch servizi è VPCbasato su Amazon per consentire alla funzione Lambda di creare e gestire le interfacce di VPC rete Amazon. Per ulteriori informazioni, consulta Connessione della rete in uscita alle risorse in un ruolo di esecuzione Amazon VPC e Lambda.

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": "es:ESHttpGet",
                    "Resource": [
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-
name>/",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/health",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/indices",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/allocation",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/allocation/explain"
                    ]
                },
                {
                    "Condition": {
                        "ArnLikeIfExists": {
                            "ec2:Vpc": "arn:<partition>:ec2:<region>:<account-id>:vpc/
<vpc_id>"
                        }
                    },
                    "Action": [
                        "ec2:DeleteNetworkInterface",
                        "ec2:CreateNetworkInterface",
```

```
                    "ec2:DescribeNetworkInterfaces",
                    "ec2:UnassignPrivateIpAddresses",
                    "ec2:AssignPrivateIpAddresses"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }

        ]
    }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

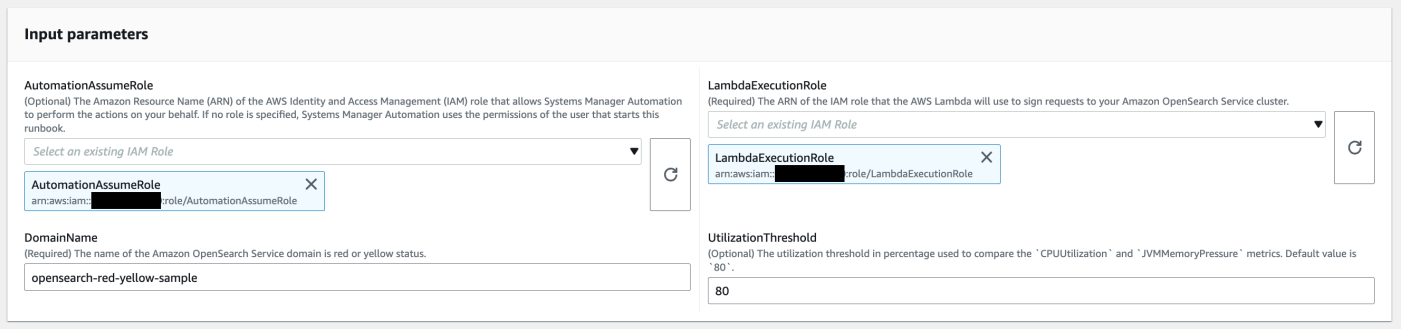
1. Passa a AWSSupport- TroubleshootOpenSearchRedYellowCluster nella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - LambdaExecutionRole (Obbligatorio):

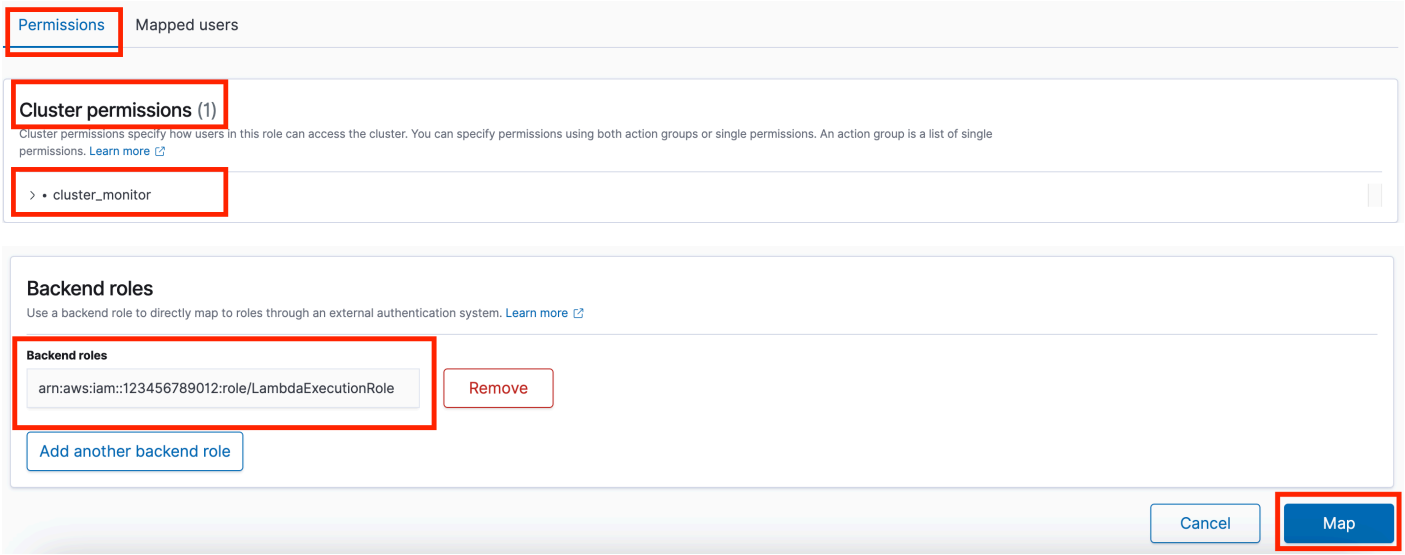
     Il ARN IAM ruolo che Lambda utilizzerà per firmare le richieste al tuo cluster Amazon OpenSearch Service.
   - DomainName (Obbligatorio):

     Il nome del dominio del OpenSearch servizio con lo stato di integrità del cluster rosso o giallo.
   - UtilizationThreshold (Facoltativo):

     La percentuale della soglia di utilizzo utilizzata per confrontare le JVMMemoryPressure metriche CPUUtilization e. Il valore predefinito è 80.



4. Se hai abilitato il controllo granulare degli accessi su un cluster di OpenSearch servizi, assicurati che il `LambdaExecutionRole` ruolo arn sia mappato a un ruolo con almeno l'autorizzazione. `cluster_monitor`



5. Seleziona Esegui.
6. L'automazione inizia.
7. Il runbook di automazione esegue i seguenti passaggi:
   - GetClusterConfiguration:

     Recupera la configurazione del cluster OpenSearch di servizio.
   - C: reateAWSLambda FunctionStack

     Crea una funzione Lambda temporanea nel tuo account utilizzando. AWS CloudFormation La funzione Lambda viene utilizzata per eseguire il OpenSearch servizio. APIs
   - WaitForAWSLambdaFunctionStack:

     Attende il completamento dello CloudFormation stack.

- GetClusterMetricsFromCloudWatch:

  Ottiene le metriche relative al cluster Amazon CloudWatch ClusterStatus e JVMMemoryPressure OpenSearch Service e la relativa data di creazione. CPUUtilization

- RunOpenSearchAPIs:

  Utilizza la funzione Lambda per chiamare il OpenSearch servizio APIs e analizzare i dati delle metriche del cluster per diagnosticare la causa dello stato rosso o giallo del cluster.

- D: eleteAWSLambda FunctionStack

  Elimina la funzione Lambda creata da questa automazione nel tuo account.

8. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

   - RootCause:

     Fornisce una panoramica della causa identificata dello stato di salute del cluster in rosso o giallo.

   - IssueDescription:

     Fornisce dettagli sul motivo per cui il cluster è in rosso o giallo e sui possibili passaggi per riportare il cluster allo stato verde.

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Per ulteriori informazioni, consulta la sezione Risoluzione dei problemi di Amazon OpenSearch Service

AWSSupport-TroubleshootOpenSearchHighCPU

Descrizione

Il AWSSupport-TroubleshootOpenSearchHighCPU runbook fornisce una soluzione automatizzata per raccogliere dati diagnostici da un dominio Amazon OpenSearch Service per risolvere problemi gravi. CPU

Come funziona?

Il AWSSupport-TroubleshootOpenSearchHighCPU runbook aiuta a risolvere i problemi di CPU utilizzo elevato nel dominio Amazon Service. OpenSearch

Il runbook esegue i seguenti passaggi:

- Esegue DescribeDomainAPIil dominio Amazon OpenSearch Service fornito per ottenere i metadati del cluster.
- Verifica se il dominio Amazon OpenSearch Service è pubblico o VPC basato su Amazon e, con l'aiuto di AWS CloudFormation, crea una AWS Lambda funzione pubblica o VPCbasata su Amazon.
- La funzione Lambda recupera i dati diagnostici dai domini di Amazon OpenSearch Service.
- Utilizza una macchina a AWS Step Functions stati per orchestrare più esecuzioni di funzioni Lambda per raccogliere dati più completi.
- Per impostazione predefinita, archivia i dati raccolti in un gruppo di CloudWatch log Amazon per 24 ore.
- Elimina le risorse create, ad eccezione del gruppo di CloudWatch log.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudformation:CreateStack`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DeleteStack`
- `lambda:CreateFunction`
- `lambda:DeleteFunction`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `lambda:TagResource`
- `es:DescribeDomain`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:AttachNetworkInterface`
- `ec2:DeleteNetworkInterface`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `states:CreateStateMachine`
- `states:DeleteStateMachine`
- `states:StartExecution`
- `states:TagResource`
- `states:DescribeStateMachine`

- states:DescribeExecution
- iam:PassRole
- iam:CreateRole
- iam:DeleteRole
- iam:GetRole
- iam:PutRolePolicy
- iam:DeleteRolePolicy
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

Il LambdaExecutionRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

Il ruolo di esecuzione Lambda concede alla funzione l'autorizzazione ad accedere ai AWS servizi e alle risorse richiesti da questo runbook. Per ulteriori informazioni, consulta Ruolo di esecuzione Lambda.

> **Note**
>
> I ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface, e ec2:DeleteNetworkInterface sono necessari solo se il cluster di OpenSearch servizi è VPCbasato su Amazon per consentire alla funzione Lambda di creare e gestire le interfacce di VPC rete Amazon. Per ulteriori informazioni, consulta Connessione della rete in uscita alle risorse in un ruolo di esecuzione Amazon VPC e Lambda.

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a AWSSupport- TroubleshootOpenSearchHigh CPU nella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole (Facoltativo):

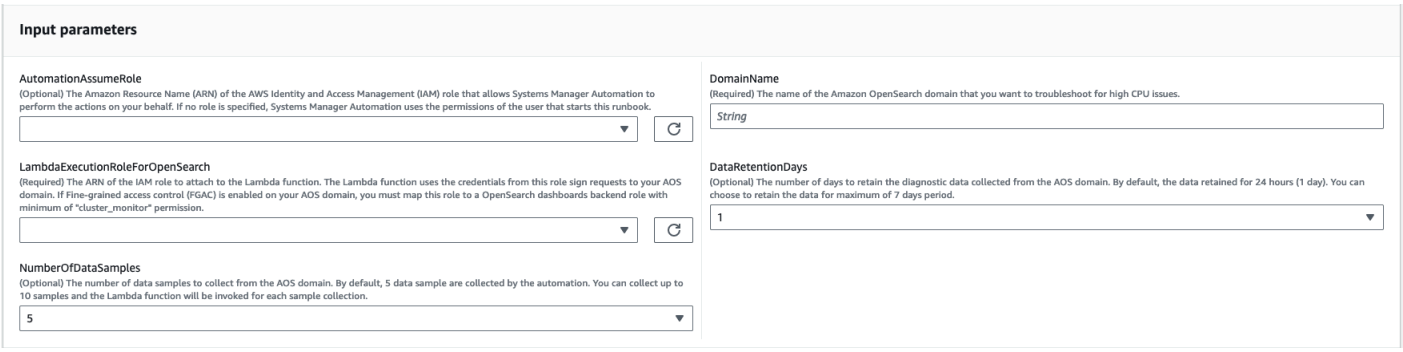
     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - DomainName (Obbligatorio):

     Il nome del dominio Amazon OpenSearch Service che desideri risolvere per problemi gravi. CPU
   - LambdaExecutionRoleForOpenSearch(Obbligatorio):

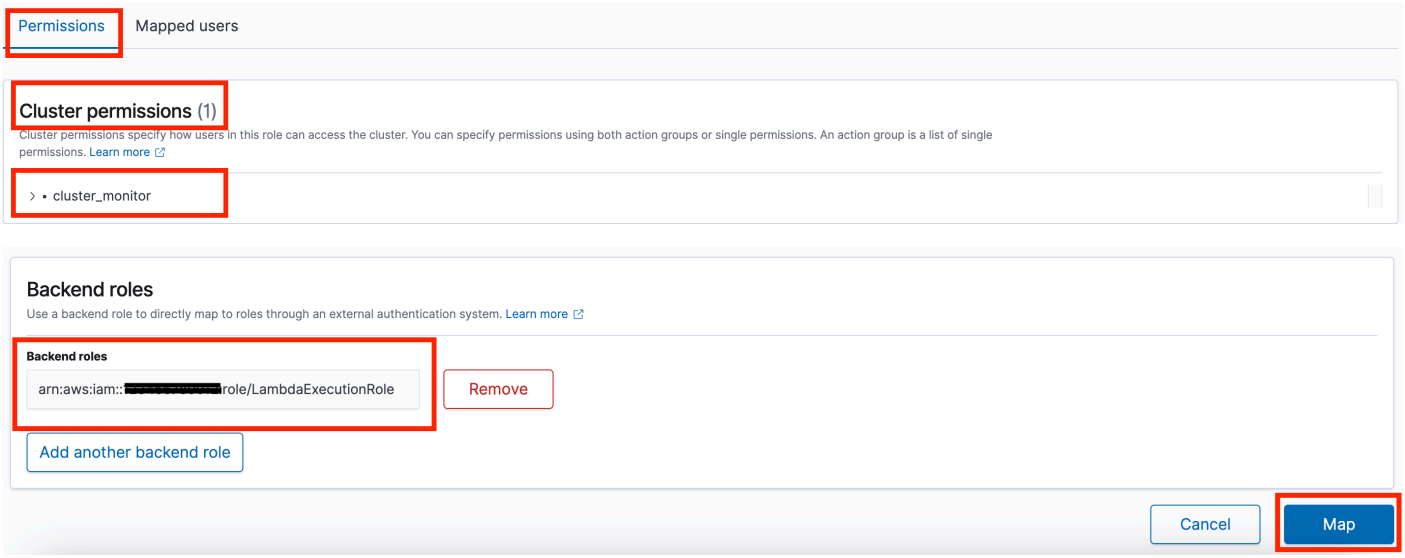
     Il ARN IAM ruolo da assegnare alla funzione Lambda. La funzione Lambda utilizza le credenziali di questo ruolo per firmare le richieste al dominio Amazon OpenSearch Service. Se il controllo granulare degli accessi è abilitato sul dominio Amazon OpenSearch Service, devi mappare questo ruolo a un ruolo di backend di OpenSearch Service Dashboards con un minimo di autorizzazione «cluster_monitor».
   - DataRetentionDays (Facoltativo):

     Il numero di giorni per conservare i dati diagnostici raccolti dal dominio Amazon OpenSearch Service. Per impostazione predefinita, i dati vengono conservati per 24 ore (un giorno). Puoi scegliere di conservare i dati per un massimo di 30 giorni.
   - NumberOfDataSamples (Facoltativo):

     Il numero di campioni di dati da raccogliere dal dominio Amazon OpenSearch Service. Per impostazione predefinita, vengono raccolti 5 campioni di dati. È possibile raccogliere fino a 10 campioni e la funzione Lambda verrà richiamata per ogni raccolta di campioni.



4. Se hai abilitato il controllo granulare degli accessi su un cluster di OpenSearch servizi, assicurati che il `LambdaExecutionRole` ruolo arn sia mappato a un ruolo con almeno l'autorizzazione. `cluster_monitor`



5. Seleziona Esegui.
6. L'automazione inizia.
7. Il runbook di automazione esegue i seguenti passaggi:
   - checkConcurrency:

     Assicura che esista una sola esecuzione di questo runbook destinata al dominio Amazon OpenSearch Service specificato. Se il runbook trova un'altra esecuzione indirizzata allo stesso nome di dominio, restituisce un errore e termina.
   - getDomainConfig:

     Ottiene i dettagli di configurazione per il dominio di OpenSearch servizio di destinazione.
   - provisionResources:

Fornisce le risorse per la raccolta dei dati utilizzando AWS CloudFormation.

- waitForStackCreazione:

  Attende il completamento dello AWS CloudFormation stack.

- describeStackResources:

  Descrive lo AWS CloudFormation stack e ottiene il valore ARN della macchina a stati.

- runStateMachine:

  Richiama la funzione Lambda del raccoglitore di dati una o più volte eseguendo una macchina a stati Step Functions.

- describeErrorsFromStackEvents:

  Descrive gli errori presenti nella pila per individuare eventuali errori. AWS CloudFormation

- unstageOpenSearchH: ighCPUAutomation

  Elimina lo `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation stack.

- describeErrorsFromStackDeletion:

  Descrive gli errori riscontrati durante l'eliminazione dello stack. AWS CloudFormation

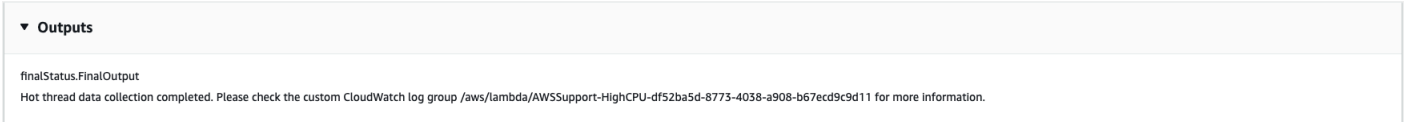
- finalStatus:

  Restituisce l'output finale del runbook. `AWSSupport-TroubleshootOpenSearchHighCPU`

8. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

   - finalStatus.FinalOutput:

     Fornisce il gruppo di CloudWatch log in cui sono archiviati i dati diagnostici.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione

- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Per ulteriori informazioni, consulta la sezione Risoluzione dei problemi di Amazon OpenSearch Service

EventBridge

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. EventBridge Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

Descrizione

Il `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook aggiunge una stringa di deduplicazione per tutti coloro che sono AWS Systems Manager OpsItems associati a una regola Amazon. EventBridge Il runbook non aggiunge una stringa di deduplicazione alla regola se ne è già stata applicata una. Per ulteriori informazioni sulle stringhe di deduplicazione e OpsItems, vedere Reducing duplicate nella Guida per l'utente. OpsItems AWS Systems Manager

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DedupString

  Tipo: stringa

  Descrizione: (Obbligatoria) La stringa di deduplicazione che si desidera aggiungere alla regola.
- RuleName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della regola a cui si desidera aggiungere la stringa di deduplicazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Fasi del documento

- `aws:executeScript`- Aggiunge una stringa di deduplicazione alla EventBridge regola specificata nel parametro. `RuleName`

AWS-DisableEventBridgeRule

Descrizione

Il *AWS-DisableEventBridgeRule* runbook disabilita la EventBridge regola Amazon specificata. Per ulteriori informazioni sulle regole EventBridge , consulta le regole di Amazon EventBridge nella Amazon User Guide. EventBridge

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EventBusName

  Tipo: stringa

  Impostazione predefinita: impostazione predefinita

  Descrizione: (Facoltativo) Il bus degli eventi associato alla regola che desideri disabilitare.
- RuleName

  Tipo: stringa

Descrizione: (Obbligatorio) Il nome della regola che desideri disabilitare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Fasi del documento

- `aws:executeAwsApi`- Disattiva la EventBridge regola specificata nel `RuleName` parametro.

Amazon FSx

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. FSx Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSSupport-ValidateFSxWindowsADConfig

`AWSSupport-ValidateFSxWindowsADConfig`

Descrizione

Il `AWSSupport-ValidateFSxWindowsADConfig` runbook viene utilizzato per convalidare la configurazione autogestita di Active Directory (AD) di un file server Amazon FSx per Windows

Come funziona?

Il runbook `AWSSupport-ValidateFSxWindowsADConfig` esegue lo script di FSx convalida di Amazon sull'istanza temporanea di Amazon Elastic Compute Cloud (AmazonEC2) Windows lanciata dal runbook nella sottorete Amazon. FSx Lo script esegue più controlli per convalidare la connettività di rete ai DNS server AD/ autogestiti e le autorizzazioni dell'account di servizio Amazon. FSx Il

runbook può convalidare un file server FSx Amazon for Windows fallito o configurato in modo errato o creare un nuovo FSx Amazon for Windows File Server con AD autogestito.

Per impostazione predefinita, il runbook crea l'istanza Amazon EC2 Windows, il gruppo di sicurezza per AWS Systems Manager (SSM) access, AWS Identity and Access Management (IAM) ruolo e policy utilizzando AWS CloudFormation nella FSx sottorete Amazon. Se desideri eseguire lo script su un'EC2istanza Amazon esistente, fornisci l'ID nel parametro`InstanceId`. In caso di esecuzione riuscita, elimina le CloudFormation risorse. Tuttavia, per conservare le risorse, impostate il `RetainCloudFormationStack` parametro su`true`.

Il CloudFormation modello crea un IAM ruolo per tuo conto con le autorizzazioni necessarie da collegare all'EC2istanza Amazon per eseguire lo script di FSx convalida di Amazon. Per specificare un profilo di IAM istanza esistente per l'istanza temporanea, utilizza il `InstanceProfileName` parametro. Il IAM ruolo associato deve contenere le seguenti autorizzazioni:

- `ec2:DescribeSubnets`e `ec2:DescribeVpcs` autorizzazioni e Amazon Managed Policy`AmazonSSMManagedInstanceCore`.
- Autorizzazioni per ottenere il nome utente e la password dell'account del FSx servizio Amazon da Systems Manager chiamando il `GetSecretValue`API.
- Autorizzazioni per inserire l'oggetto nel bucket Amazon Simple Storage Service (Amazon S3) per l'output dello script.

Prerequisiti

La sottorete in cui viene creata l'EC2istanza Amazon temporanea (o l'istanza esistente fornita nel `InstanceId` parametro) deve consentire l'accesso agli endpoint e Amazon S3 per eseguire `AmazonFSxADValidation` lo script SSM utilizzando Run Command. AWS Systems Manager AWS Secrets Manager

AWS Secrets Manager configurazione

Lo script di convalida si connette al dominio Microsoft AD recuperando il nome utente e la password dell'account del FSx servizio Amazon con una chiamata di runtime a Secrets Manager. Segui la procedura descritta in Creare un AWS Secrets Manager segreto per creare un nuovo segreto di Secrets Manager. Assicurati che il nome utente e la password siano archiviati utilizzando una coppia chiave/valore nel formato. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}"` Per informazioni sulla protezione dell'accesso ai segreti, consulta Autenticazione e controllo degli accessi. AWS Secrets Manager

Per ulteriori informazioni sullo strumento, consulta i `README.md` file `TROUBLESHOOTING.md` and nel mazonFSx ADValidation file A.

Esecuzione del runbook

Esegui il runbook con i parametri Amazon FSx ID o AD. Di seguito è riportato il flusso di lavoro del runbook:

- Ottiene i parametri dall'FSxID Amazon o utilizza i parametri AD di input.
- Crea l'istanza Amazon EC2 Windows di convalida temporanea sulla FSx sottorete Amazon, sul gruppo di sicurezza per SSM l'accesso, il IAM ruolo e la politica (utilizzo condizionale). CloudFormation Se il `InstanceId` parametro è specificato, viene utilizzato.
- Scarica ed esegue lo script di convalida sull'EC2istanza Amazon di destinazione nella sottorete FSx principale di Amazon.
- Fornisce il codice dei risultati della convalida AD nell'output dell'automazione. Inoltre, l'output completo dello script viene caricato nel bucket Amazon S3.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudformation:CreateStack`
- `cloudformation:DeleteStack`
- `cloudformation:DescribeStacks`

- cloudformation:DescribeStackResources
- cloudformation:DescribeStackEvents
- ec2:CreateTags
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateLaunchTemplate
- ec2:DeleteLaunchTemplate
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeLaunchTemplates
- ec2:DescribeLaunchTemplateVersions
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:RevokeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupEgress
- iam:CreateRole
- iam:CreateInstanceProfile
- iam:GetInstanceProfile
- iam:getRolePolicy
- iam:DeleteRole
- iam:DeleteInstanceProfile
- iam:AddRoleToInstanceProfile
- iam:RemoveRoleFromInstanceProfile
- iam:AttachRolePolicy
- iam:DetachRolePolicy
- iam:PutRolePolicy
- iam:DeleteRolePolicy
- iam:GetRole

- iam:PassRole
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:DescribeAutomationExecutions
- ssm:GetDocument
- ssm:GetAutomationExecution
- ssm:DescribeAutomationStepExecutions
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:ListCommands
- ssm:GetCommandInvocation
- fsx:DescribeFileSystems
- ds:DescribeDirectories
- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetAccountPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetBucketLocation

Esempio IAM di policy per l'Automation Assume Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribe",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
```

```
                                "ec2:DescribeInstances",
                                "ec2:DescribeLaunchTemplates",
                                "ec2:DescribeLaunchTemplateVersions",
                                "ssm:DescribeInstanceInformation",
                                "ssm:DescribeAutomationExecutions",
                                "ssm:DescribeAutomationStepExecutions",
                                "fsx:DescribeFileSystems",
                                "ds:DescribeDirectories"
                            ],
                            "Resource": "*"
                        },
                        {
                            "Sid": "CloudFormation",
                            "Effect": "Allow",
                            "Action": [
                                "cloudformation:DescribeStacks",
                                "cloudformation:DescribeStackResources",
                                "cloudformation:DescribeStackEvents",
                                "cloudformation:CreateStack",
                                "cloudformation:DeleteStack"
                            ],
                            "Resource": "arn:*:cloudformation:*:*:stack/AWSSupport-
ValidateFSxWindowsADConfig-*"
                        },
                        {
                            "Sid": "AllowCreateLaunchTemplate",
                            "Effect": "Allow",
                            "Action": [
                                "ec2:CreateLaunchTemplate",
                                "ec2:CreateTags"
                            ],
                            "Resource": [
                                "arn:aws:ec2:*:*:launch-template/*"
                            ]
                        },
                        {
                            "Sid": "AllowEC2RunInstances",
                            "Effect": "Allow",
                            "Action": [
                                "ec2:RunInstances",
                                "ec2:CreateTags"
                            ],
                            "Resource": [
                                "arn:aws:ec2:*::image/*",
```

```
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:launch-template/*"
            ]
        },
        {
            "Sid": "AllowEC2RunInstancesWithTags",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        {
            "Sid": "EC2SecurityGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:*:ec2:*:*:security-group/*",
                "arn:*:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "EC2Remove",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
```

```
                "arn:aws:ec2:*:*:launch-template/*",
                "arn:*:ec2:*:*:security-group/*"
            ]
        },
        {
            "Sid": "IAMInstanceProfile",
            "Effect": "Allow",
            "Action": [
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": "arn:*:iam::*:instance-profile/*"
        },
        {
            "Sid": "IAM",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:getRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:GetRole",
                "iam:TagRole"
            ],
            "Resource": "arn:*:iam::*:role/*"
        },
        {
            "Sid": "SSM",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution",
                "ssm:GetDocument",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:GetParameters",
                "ssm:ListCommands",
                "ssm:GetCommandInvocation"
            ],
```

```
                "Resource": "*"
            },
            {
                "Sid": "SSMSendCommand",
                "Effect": "Allow",
                "Action": [
                    "ssm:SendCommand"
                ],
                "Resource": "arn:aws:ssm:*:*:document/AWS-
RunPowerShellScript"
            },
            {
                "Sid": "SSMSendCommandOnlyFsxInstance",
                "Effect": "Allow",
                "Action": [
                    "ssm:SendCommand"
                ],
                "Resource": [
                    "arn:aws:ec2:*:*:instance/*"
                ],
                "Condition": {
                    "StringLike": {
                        "ssm:resourceTag/CreatedBy": [
                            "AWSSupport-ValidateFSxWindowsADConfig"
                        ]
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": [
                            "ec2.amazonaws.com"
                        ]
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "s3:GetEncryptionConfiguration",
```

```
                            "s3:GetBucketPublicAccessBlock",
                            "s3:GetAccountPublicAccessBlock",
                            "s3:GetBucketPolicyStatus",
                            "s3:GetBucketAcl",
                            "s3:GetBucketLocation"
                        ],
                        "Resource": "*"
                    }
                ]
            }
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-ValidateFSxWindowsADConfig](#)a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per convalidare AD autogestito con un FSx Amazon esistente fallito o configurato in modo errato, inserisci i seguenti parametri:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - FSxId(Condizionale):

     L'ID del file server Amazon FSx per Windows. Ciò è necessario per convalidare Amazon esistente con errori o configurazioni errate. FSx
   - SecretArn (Obbligatorio):

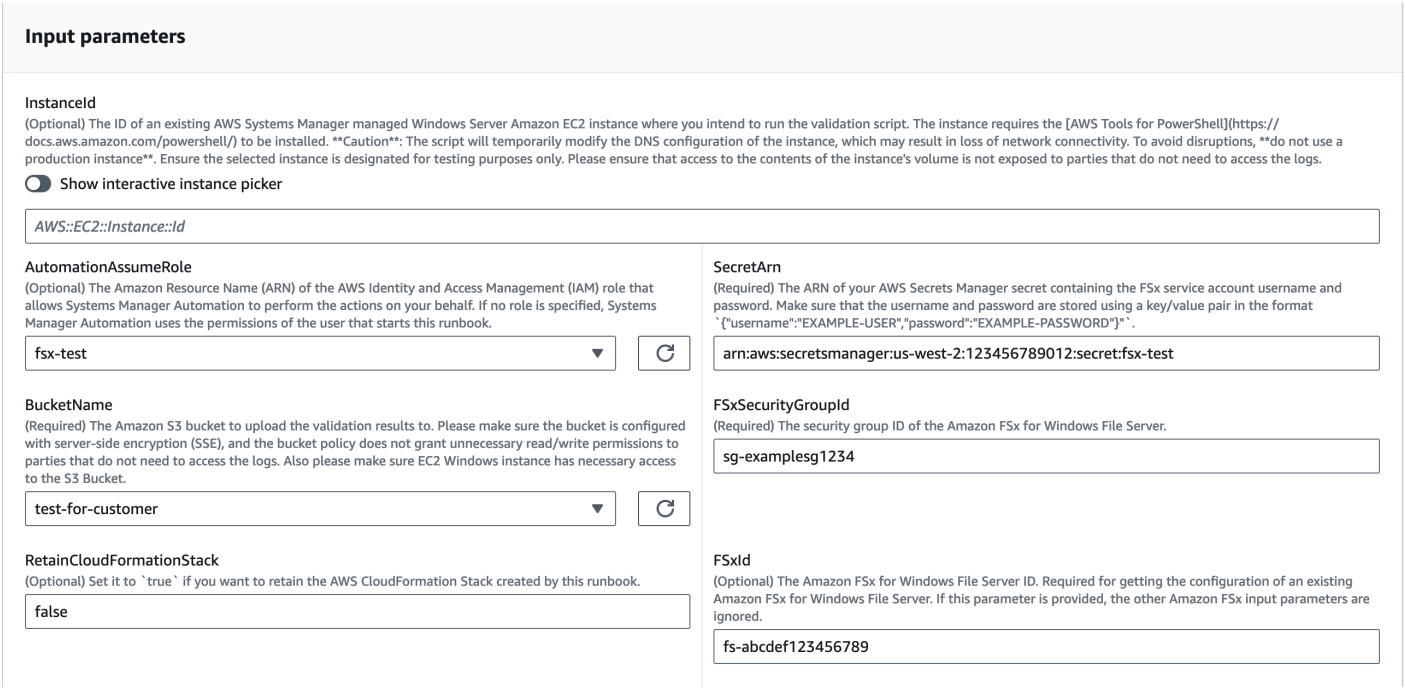
     Il segreto ARN del tuo Secrets Manager contenente il nome utente e la password dell'account del FSx servizio Amazon. Assicurati che il nome utente e la password siano memorizzati utilizzando una coppia chiave/valore nel formato. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}` Lo CloudFormation stack crea l'istanza di convalida con le autorizzazioni necessarie per eseguire questa operazione. `GetSecretValue` ARN

- FSxSecurityGroupId(Obbligatorio):

  L'ID del gruppo di sicurezza per Amazon FSx for Windows File Server.

- BucketName (Obbligatorio):

  Il bucket Amazon S3 su cui caricare i risultati della convalida. Assicurati che il bucket sia configurato con la crittografia lato server (SSE) e che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log. Assicurati inoltre che l'istanza Amazon EC2 Windows disponga dell'accesso necessario al bucket Amazon S3.



4. Per convalidare la configurazione AD autogestita per una nuova FSx creazione Amazon, inserisci i seguenti parametri:

   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

   - SecretArn (Obbligatorio):

     Il segreto ARN del tuo Secrets Manager contenente il nome utente e la password dell'account del FSx servizio Amazon. Assicurati che il nome utente e la password siano

memorizzati utilizzando una coppia chiave/valore nel formato. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}` Lo CloudFormation stack crea l'istanza di convalida con le autorizzazioni necessarie per eseguire questa operazione. `GetSecretValue` ARN

- FSxSecurityGroupId(Obbligatorio):

  L'ID del gruppo di sicurezza per Amazon FSx for Windows File Server.

- BucketName (Obbligatorio):

  Il bucket Amazon S3 su cui caricare i risultati della convalida. Assicurati che il bucket sia configurato con la crittografia lato server (SSE) e che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log. Assicurati inoltre che l'istanza Amazon EC2 Windows disponga dell'accesso necessario al bucket Amazon S3.

- FSxPreferredSubnetId(Condizionale):

  La sottorete preferita di Amazon FSx for Windows File Server.

- DomainName (Condizionale):

  Il nome di dominio completo del tuo dominio Microsoft AD autogestito.

- DnsIpAddresses (Condizionale):

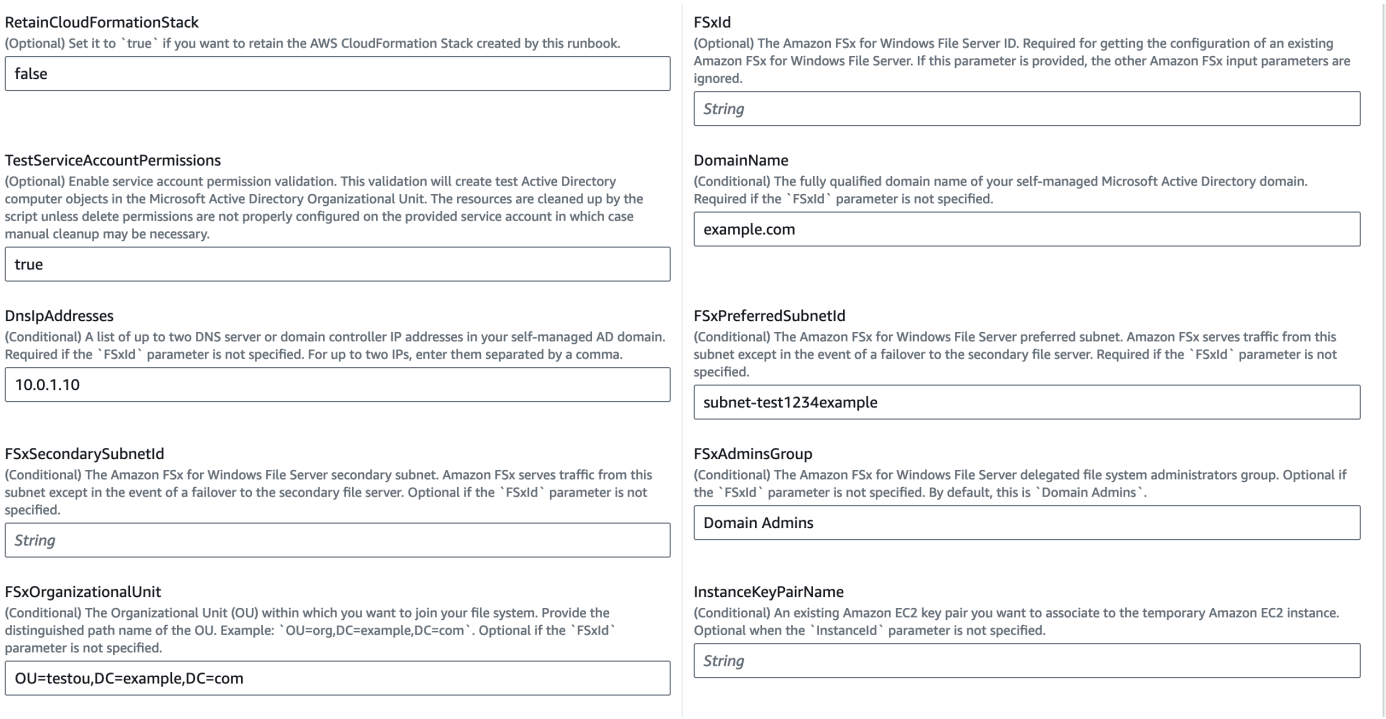
  Un elenco di un massimo di due indirizzi IP DNS del server o del controller di dominio nel dominio AD autogestito. Per un massimo di dueIPs, inseriscili separati da una virgola.

- FSxAdminsGroup(Condizionale):

  Il gruppo FSx di amministratori di file system delegati di Amazon for Windows File Server. Per impostazione predefinita, questo è `Domain Admins`.

- FSxOrganizationalUnit(Condizionale):

  L'unità organizzativa (OU) all'interno della quale si desidera inserire il file system. Fornire il nome del percorso distinto dell'unità organizzativa. Esempio: `OU=org,DC=example,DC=com`.



5. Seleziona Esegui.
6. L'automazione viene avviata.
7. Il documento esegue le seguenti operazioni:
   - CheckBucketPublicStatus(come:executeScript):

     Verifica se il bucket Amazon S3 di destinazione concede potenzialmente l'accesso pubblico in lettura e/o scrittura ai suoi oggetti.
   - BranchOnInputParameters(aws:branch):

     Filiali sui parametri di input forniti come Amazon FSx ID o FSx parametri Amazon.
   - AssertFileSystemTypeIsWindows(aws: assertAwsResource Proprietà):

     Se viene fornito un FSx ID Amazon, verifica che il tipo di file system sia Amazon FSx for Windows File Server.
   - GetValidationInputs(come:executeScript):

     Restituisce la configurazione Microsoft AD autogestita richiesta dal CloudFormation modello per creare l'EC2istanza Amazon.
   - BranchOnInstanceId (aws:branch):

Rami sull'ingresso fornito. `InstanceId` Se `InstanceId` fornito, lo script di convalida viene eseguito sull'EC2istanza Amazon di destinazione dall'automazione`step:RunValidationScript`.

- Crea EC2InstanceStack (aws:createStack):

  Crea l'EC2istanza Amazon nella sottorete preferita utilizzando AWS CloudFormation dove verrà `AmazonFSxADValidation` eseguito lo strumento

- DescribeStackResources(come:executeAwsApi):

  Descrive lo CloudFormation stack per ottenere l'ID temporaneo dell'EC2istanza Amazon.

- WaitForEC2InstanceToBeManaged(leggi: waitForAwsResourceProperty):

  Attende che l'EC2istanza Amazon sia gestita da Systems Manager per eseguire lo script di convalida utilizzando SSM Run Command.

- GetAmazonFSxADValidationAttachment(aws:): executeAwsApi

  Ottiene lo `AmazonFSxADValidation` strumento URL dagli allegati del runbook.

- RunValidationScript(come:): runCommand

  Esegue lo `AmazonFSxADValidation` strumento sull'EC2istanza Amazon temporanea e archivia il risultato nel bucket Amazon S3 specificato nel parametro. `BucketName`

- DescribeErrorsFromStackEvents(come:): executeScript

  Descrive gli eventi CloudFormation dello stack se i runbook non riescono a creare lo stack.

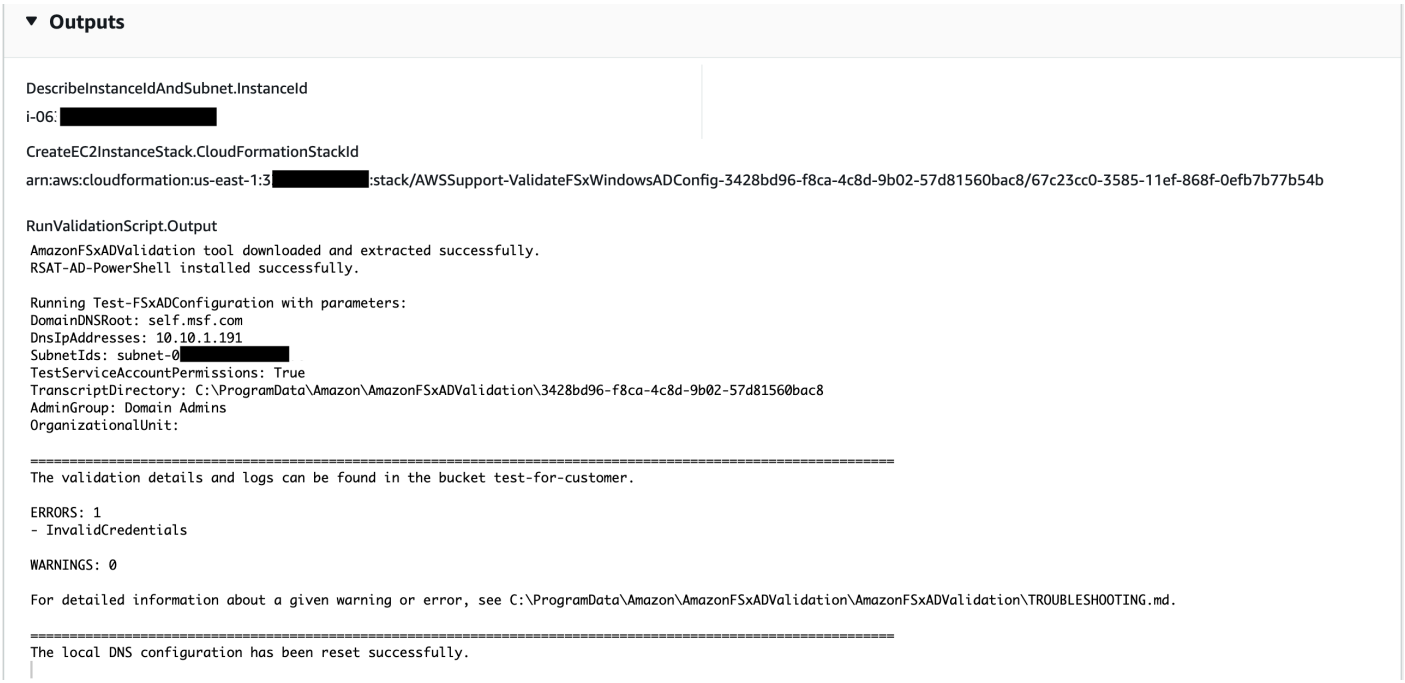
- BranchOnRetainCloudFormationStack(aws:branch):

  Rami `RetainCloudFormationStack` e `InstanceId` parametri per determinare se lo CloudFormation stack deve essere eliminato.

- DeleteCloudFormationStack(come:deleteStack):

  Elimina lo AWS CloudFormation stack.

8. Al termine, consulta la sezione Output per i risultati dell'esecuzione:



Il runbook caricherà i risultati dell'esecuzione dello script di convalida nel bucket Amazon S3.

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Cos'è Amazon FSx per Windows File Server?
- Convalida della configurazione AD autogestita FSx per Amazon for Windows File Server

GuardDuty

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. GuardDuty Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

AWSConfigRemediation-CreateGuardDutyDetector

Descrizione

Il `AWSConfigRemediation-CreateGuardDutyDetector` runbook crea un rilevatore Amazon GuardDuty (GuardDuty) nel luogo in Regione AWS cui esegui l'automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Fasi del documento

- `aws:executeAwsApi`- Crea un GuardDuty rilevatore.
- `aws:assertAwsResourceProperty`- Verifica lo stato `Status` del rilevatore. `ENABLED`

IAM

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Identity and Access Management Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-AttachIAMToInstance
- AWS-DeleteIAMInlinePolicy
- AWSConfigRemediation-DeleteIAMRole
- AWSConfigRemediation-DeleteIAMUser
- AWSConfigRemediation-DeleteUnusedIAMGroup
- AWSConfigRemediation-DeleteUnusedIAMPolicy
- AWSConfigRemediation-DetachIAMPolicy
- AWSConfigRemediation-EnableAccountAccessAnalyzer
- AWSSupport-GrantPermissionsToIAMUser
- AWSConfigRemediation-RemoveUserPolicies
- AWSConfigRemediation-ReplaceIAMInlinePolicy
- AWSConfigRemediation-RevokeUnusedIAMUserCredentials
- AWSConfigRemediation-SetIAMPasswordPolicy

`AWS-AttachIAMToInstance`

Descrizione

Associa un ruolo AWS Identity and Access Management (IAM) a un'istanza gestita.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ForceReplace

  Tipo: Booleano

  Descrizione: (Facoltativo) Contrassegno per specificare se sostituire o meno il IAM profilo esistente.

  Impostazione predefinita: true
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza a cui si desidera assegnare un IAM ruolo.
- RoleName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del IAM ruolo da aggiungere all'istanza gestita.

Fasi del documento

1. `aws:executeAwsApi`- DescribeInstanceProfile - Trova il profilo dell'IAMistanza collegato all'EC2istanza.
2. `aws:branch`- CheckInstanceProfileAssociations - Controllate il profilo dell'IAMistanza collegato all'EC2istanza.
   a. Se un profilo di IAM istanza è collegato ed `ForceReplace` è impostato su`true`:
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Dissocia il profilo dell'IAMistanza dall'EC2istanza.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Elenca i profili di istanza per il IAM ruolo fornito.
   c. `aws:branch`- CheckInstanceProfileCreated - Verifica se al IAM ruolo fornito è associato un profilo di istanza.
      i. Se al IAM ruolo è associato un profilo di istanza:
         A. `aws:executeAwsApi`- A ttachIAMProfile ToInstance - Associa il ruolo del profilo dell'IAMEC2istanza all'istanza.
      i. Se al IAM ruolo non è associato un profilo di istanza:
         A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Crea un ruolo del profilo di istanza per il IAM ruolo specificato.
         B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Associa il ruolo del profilo dell'istanza al IAM ruolo specificato.
         C. `aws:executeAwsApi`- GetInstanceProfile - Ottiene i dati del profilo dell'istanza per il IAM ruolo specificato.
         D. `aws:executeAwsApi`- A ttachIAMProfile ToInstanceWithRetry - Associa il ruolo del profilo dell'IAMEC2istanza all'istanza.

Output

ttachIAMProfileToInstanceWithRetryA. AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Un ttachIAMProfileToInstance. AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Descrizione

Il `AWS-DeleteIAMInlinePolicy` runbook elimina tutte le AWS Identity and Access Management (IAM) politiche in linea allegate alle identità specificate. IAM

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- IamArns

  Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole delle ARNs IAM identità da cui si desidera eliminare le politiche in linea. Questo elenco può includere IAM utenti, gruppi o ruoli.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Fasi del documento

- `aws:executeScript`- Elimina le politiche IAM in linea allegate alle identità di destinazione. IAM

AWSConfigRemediation-DeleteIAMRole

Descrizione

Il `AWSConfigRemediation-DeleteIAMRole` runbook elimina il ruolo AWS Identity and Access Management (IAM) specificato. Questa automazione non elimina i profili di istanza associati al IAM ruolo o i ruoli collegati al servizio.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMRoleID

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del IAM ruolo che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Fasi del documento

- `aws:executeScript`- Raccoglie il nome del IAM ruolo specificato nel `IAMRoleID` parametro.
- `aws:executeScript`- Raccoglie le politiche e i profili di istanza associati al IAM ruolo.
- `aws:executeScript`- Elimina le politiche allegate.
- `aws:executeScript`- Elimina il IAM ruolo e verifica che il ruolo sia stato eliminato.

AWSConfigRemediation-DeleteIAMUser

Descrizione

Il `AWSConfigRemediation-DeleteIAMUser` runbook elimina l'utente AWS Identity and Access Management (IAM) specificato. Questa automazione elimina o scollega le seguenti risorse associate all'utente: IAM

- Chiavi di accesso
- Politiche gestite allegate
- Credenziali Git
- IAMappartenenze a gruppi
- IAMpassword utente
- Policy inline
- dispositivi di autenticazione a più fattori (MFA)
- Certificati di firma
- SSHchiavi pubbliche

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMUserId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'IAMutente che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeactivateMFADevice`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:DeleteServiceSpecificCredential`
- `iam:DeleteSigningCertificate`
- `iam:DeleteSSHPublicKey`
- `iam:DeleteVirtualMFADevice`
- `iam:DeleteUser`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:GetUser`
- `iam:ListAttachedUserPolicies`
- `iam:ListAccessKeys`
- `iam:ListGroupsForUser`
- `iam:ListMFADevices`
- `iam:ListServiceSpecificCredentials`
- `iam:ListSigningCertificates`

- `iam:ListSSHPublicKeys`
- `iam:ListUserPolicies`
- `iam:ListUsers`
- `iam:RemoveUserFromGroup`

Fasi del documento

- `aws:executeScript`- Raccoglie il nome utente dell'IAMutente specificato nel `IAMUserId` parametro.
- `aws:executeScript`- Raccoglie chiavi di accesso, certificati, credenziali, MFA dispositivi e SSH chiavi associati all'utente. IAM
- `aws:executeScript`- Raccoglie le appartenenze ai gruppi e le politiche per l'utente. IAM
- `aws:executeScript`- Elimina chiavi di accesso, certificati, credenziali, MFA dispositivi e SSH chiavi associati all'utente. IAM
- `aws:executeScript`- Elimina le appartenenze ai gruppi e le politiche per l'utente. IAM
- `aws:executeScript`- Elimina l'IAMutente e verifica che sia stato eliminato.

`AWSConfigRemediation-DeleteUnusedIAMGroup`

Descrizione

Il `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook elimina un IAM gruppo che non contiene utenti.

Il `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook elimina un IAM gruppo che non contiene utenti.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- GroupName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del IAM gruppo che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Fasi del documento

- `aws:executeScript`- Rimuove IAM le politiche gestite e in linea associate al IAM gruppo target, quindi elimina il gruppo. IAM

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descrizione

Il `AWSConfigRemediation-DeleteUnusedIAMPolicy` runbook elimina una politica AWS Identity and Access Management (IAM) che non è associata a utenti, gruppi o ruoli.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- IAMResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa della IAM policy che desideri eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`

- `config:ListDiscoveredResources`
- `iam:DeletePolicy`
- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Fasi del documento

- `aws:executeScript`- Elimina la politica specificata nel `IAMResourceId` parametro e verifica che la politica sia stata eliminata.

`AWSConfigRemediation-DetachIAMPolicy`

Descrizione

Il `AWSConfigRemediation-DetachIAMPolicy` runbook rimuove la policy AWS Identity and Access Management (IAM) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della IAM policy che desideri scollegare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Fasi del documento

- `aws:executeScript`- Scollega la IAM politica da tutte le risorse.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descrizione

Il `AWSConfigRemediation-EnableAccountAccessAnalyzer` runbook crea un AWS Identity and Access Management (IAM) Access Analyzer nel tuo. Account AWSPer informazioni su Access Analyzer, vedere Uso di AWS IAM Access Analyzer nella Guida per l'utente. IAM

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AnalyzerName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dell'analizzatore da creare.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Fasi del documento

- `aws:executeAwsApi`- Crea un analizzatore di accesso per il tuo account.
- `aws:waitForAwsResourceProperty`- Attende che sia lo stato dell'analizzatore di accesso. `ACTIVE`
- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'analizzatore di accesso è. `ACTIVE`

AWSSupport-GrantPermissionsToIAMUser

Descrizione

Questo runbook concede le autorizzazioni specificate a un IAM gruppo (nuovo o esistente) e vi aggiunge l'utente esistenteIAM. Le policy valide disponibili sono: Billing (Fatturazione) o Support (Supporto). Per abilitare l'accesso alla fatturazione perIAM, ricordati di attivare anche l'accesso IAM utente e utente federato alle pagine Billing and Cost Management.

> **Important**
>
> Se fornisci un IAM gruppo esistente, tutti IAM gli utenti correnti del gruppo ricevono le nuove autorizzazioni.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- IAMGroupName

  Tipo: stringa

  Impostazione predefinita: ExampleSupportAndBillingGroup

  Descrizione: (obbligatorio) può essere un gruppo nuovo o esistente. Deve rispettare i limiti relativi ai nomi delle IAM entità.

- IAMUserName

  Tipo: stringa

  Impostazione predefinita: ExampleUser

  Descrizione: (obbligatorio) deve essere un utente esistente.

- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN ruolo assunto da lambda.

- Autorizzazioni

  Tipo: stringa

  Valori validi: SupportFullAccess | | BillingFullAccess SupportAndBillingFullAccess

  Predefinito: SupportAndBillingFullAccess

  Descrizione: (Obbligatorio) Scegli una delle seguenti opzioni: `SupportFullAccess` garantisce l'accesso completo al Support center. `BillingFullAccess`concede l'accesso completo alla dashboard di fatturazione. `SupportAndBillingFullAccess`garantisce l'accesso completo sia al Support center che alla dashboard di fatturazione. Ulteriori informazioni sulle policy sono disponibili nei dettagli del documento.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Le autorizzazioni richieste dipendono dalla modalità `AWSSupport-GrantPermissionsToIAMUser` di esecuzione.

In esecuzione come utente o ruolo attualmente connesso

Si consiglia di allegare la policy gestita di `AmazonSSMAutomationRole` Amazon e le seguenti autorizzazioni aggiuntive per poter creare la funzione Lambda e IAM il ruolo da passare a Lambda:

```
{
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Action": [
                                "lambda:InvokeFunction",
                                "lambda:CreateFunction",
                                "lambda:DeleteFunction",
                                "lambda:GetFunction"
                            ],
                            "Resource":
 "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
                            "Effect": "Allow"
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:CreateGroup",
                                "iam:AddUserToGroup",
                                "iam:ListAttachedGroupPolicies",
                                "iam:GetGroup",
                                "iam:GetUser"
                            ],
                            "Resource" : [
                                "arn:aws:iam::*:user/*",
                                "arn:aws:iam::*:group/*"
                            ]
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:AttachGroupPolicy"
```

```
                        ],
                        "Resource": "*",
                        "Condition": {
                            "ArnEquals": {
                                "iam:PolicyArn": [
                                    "arn:aws:iam::aws:policy/job-function/Billing",
                                    "arn:aws:iam::aws:policy/AWSSupportAccess"
                                ]
                            }
                        }
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:ListAccountAliases",
                            "iam:GetAccountSummary"
                        ],
                        "Resource" : "*"
                    }
                ]
            }
```

Usare e AutomationAssumeRole LambdaAssumeRole

L'utente deve disporre dei StartAutomationExecution permessi ssm: sul runbook e iam: PassRole sui IAM ruoli passati come and. AutomationAssumeRoleLambdaAssumeRole Ecco le autorizzazioni necessarie per ogni ruolo: IAM

```
AutomationAssumeRole

                {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Action": [
                                "lambda:InvokeFunction",
                                "lambda:CreateFunction",
                                "lambda:DeleteFunction",
                                "lambda:GetFunction"
                            ],
                            "Resource":
 "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
                            "Effect": "Allow"
```

```
                        }
                    ]
                }
```

LambdaAssumeRole

```
            {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:CreateGroup",
                            "iam:AddUserToGroup",
                            "iam:ListAttachedGroupPolicies",
                            "iam:GetGroup",
                            "iam:GetUser"
                        ],
                        "Resource" : [
                            "arn:aws:iam::*:user/*",
                            "arn:aws:iam::*:group/*"
                        ]
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:AttachGroupPolicy"
                        ],
                        "Resource": "*",
                        "Condition": {
                            "ArnEquals": {
                                "iam:PolicyArn": [
                                    "arn:aws:iam::aws:policy/job-function/Billing",
                                    "arn:aws:iam::aws:policy/AWSSupportAccess"
                                ]
                            }
                        }
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:ListAccountAliases",
```

```
                            "iam:GetAccountSummary"
                        ],
                        "Resource" : "*"
                    }
                ]
            }
```

Fasi del documento

1. `aws:createStack`- Esegui AWS CloudFormation Template per creare una funzione Lambda.
2. `aws:invokeLambdaFunction`- Esegui Lambda per impostare IAM le autorizzazioni.
3. `aws:deleteStack`- Elimina CloudFormation modello.

Output

configura IAM .Payload

`AWSConfigRemediation-RemoveUserPolicies`

Descrizione

Il `AWSConfigRemediation-RemoveUserPolicies` runbook elimina le policy in linea AWS Identity and Access Management (IAM) e rimuove tutte le policy gestite allegate all'utente specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMUserID

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'utente da cui desideri rimuovere le policy.

- PolicyType

  Tipo: stringa

  Valori validi: Tutti | In linea | Gestiti

  Predefinito: Tutti

  Descrizione: (Obbligatorio) Il tipo di IAM policy che desideri rimuovere dall'utente.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Fasi del documento

- `aws:executeScript`- Elimina e rimuove le IAM politiche dall'utente specificato nel parametro. `IAMUserID`

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descrizione

Il `AWSConfigRemediation-ReplaceIAMInlinePolicy` runbook sostituisce una policy inline AWS Identity and Access Management (IAM) con una policy gestita replicata. IAM Per una policy in linea associata a un utente, gruppo o ruolo, le autorizzazioni della policy in linea vengono clonate in una policy gestita. IAM La IAM policy gestita viene aggiunta alla risorsa e la policy in linea viene rimossa. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- InlinePolicyName

  Tipo: StringList

  Descrizione: (Obbligatorio) La IAM politica in linea che desideri sostituire.
- ResourceId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'IAMutente, del gruppo o del ruolo di cui desideri sostituire la politica in linea.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:AttachGroupPolicy`
- `iam:AttachRolePolicy`
- `iam:AttachUserPolicy`
- `iam:CreatePolicy`
- `iam:CreatePolicyVersion`
- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:GetGroupPolicy`
- `iam:GetRolePolicy`
- `iam:GetUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Fasi del documento

- `aws:executeScript`- Sostituisci la IAM politica in linea con una politica AWS replicata sulla risorsa specificata.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Descrizione

Il `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` runbook revoca le password () e le chiavi di accesso attive non utilizzate AWS Identity and Access Management . IAM Questo runbook disattiva anche le chiavi di accesso scadute ed elimina i profili di accesso scaduti. AWS Config deve essere abilitato nel luogo in cui si esegue questa automazione Regione AWS .

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- IAMResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della IAM risorsa da cui desideri revocare le credenziali non utilizzate.
- MaxCredentialUsageAge

  Tipo: stringa

  Impostazione predefinita: 90

  Descrizione: (Obbligatorio) Il numero di giorni entro i quali la credenziale deve essere stata utilizzata.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

Fasi del documento

- `aws:executeScript`- Revoca le IAM credenziali per l'utente specificato nel parametro. `IAMResourceId` Le chiavi di accesso scadute vengono disattivate e i profili di accesso scaduti vengono eliminati.

> **Note**
>
> Assicurati di configurare il `MaxCredentialUsageAge` parametro di questa azione di riparazione in modo che corrisponda al `maxAccessKeyAge` parametro della AWS Config regola utilizzata per attivare questa azione:. access-keys-rotated

`AWSConfigRemediation-SetIAMPasswordPolicy`

Descrizione

Il `AWSConfigRemediation-SetIAMPasswordPolicy` runbook imposta la politica della password utente AWS Identity and Access Management (IAM) per il tuo Account AWS.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- AllowUsersToChangePassword

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostato su`true`, tutti IAM gli utenti Account AWS possono utilizzarlo AWS Management Console per modificare le proprie password.
- HardExpiry

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostato su`true`, agli IAM utenti viene impedito di reimpostare le password dopo la scadenza della password.
- MaxPasswordAge

  Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero di giorni di validità della password di un IAM utente.

- MinimumPasswordLength

  Tipo: integer

  Valore predefinito: 6

  Descrizione: (Facoltativo) Il numero minimo di caratteri che può contenere la password di un IAM utente.

- PasswordReusePrevention

  Tipo: integer

  Impostazione predefinita: 0

  Descrizione: (Facoltativo) Il numero di password precedenti che un IAM utente non può riutilizzare.

- RequireLowercaseCharacters

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostata su`true`, la password di un IAM utente deve contenere un carattere minuscolo dell'alfabeto latino ISO di base (dalla a alla z).

- RequireNumbers

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostata su`true`, la password di un IAM utente deve contenere un carattere numerico (0-9).

- RequireSymbols

  Tipo: Booleano

  Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostata su`true`, la password di un IAM utente deve contenere un carattere non alfanumerico (! @ # $% ^ * () _ + - = [] {} | ').

- RequireUppercaseCharacters

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostata su`true`, la password di un IAM utente deve contenere un carattere maiuscolo dell'alfabeto latino ISO di base (dalla A alla Z).

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Fasi del documento

- `aws:executeScript`- Imposta la politica delle password IAM utente in base ai valori specificati per i parametri del runbook per il tuo. Account AWS

Flusso di dati Amazon Kinesis

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Kinesis Data Streams. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableKinesisStreamEncryption

AWS-EnableKinesisStreamEncryption

Descrizione

Il `AWS-EnableKinesisStreamEncryption` runbook abilita la crittografia su Amazon Kinesis Data Streams (Kinesis Data Streams). Le applicazioni Producer che scrivono su uno stream crittografato riscontreranno errori se non hanno accesso alla chiave (). AWS Key Management Service AWS KMS

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- KinesisStreamName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dello stream su cui si desidera abilitare la crittografia.
- KeyId

  Tipo: stringa

  Predefinito: alias/aws/kinesis

Descrizione: (Obbligatoria) La chiave gestita dal cliente che desideri utilizzare AWS KMS per la crittografia. Questo valore può essere un identificatore univoco globale, un ARN alias o una chiave oppure un nome alias preceduto da «alias/». È inoltre possibile utilizzare la chiave AWS gestita utilizzando il valore predefinito per il parametro.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Fasi del documento

- VerifyKinesisStreamStatus (`aws:waitforAwsResourceProperty`) - Verifica lo stato di Kinesis Data Streams.
- EnableKinesisStreamEncryption (`aws:executeAwsApi`) - Abilita la crittografia per Kinesis Data Streams.
- VerifyKinesisStreamUpdateComplete (`aws:waitForAwsResourceProperty`) - Attende che lo stato di Kinesis Data Streams ritorni a. `ACTIVE`
- VerifyKinesisStreamEncryption (`aws:assertAwsResourceProperty`) - Verifica che la crittografia sia abilitata per Kinesis Data Streams.

AWS KMS

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Key Management Service Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

AWSConfigRemediation-CancelKeyDeletion

Descrizione

Il `AWSConfigRemediation-CancelKeyDeletion` runbook annulla l'eliminazione della chiave gestita dal cliente AWS Key Management Service (AWS KMS) specificata dall'utente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- KeyId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente per la quale desideri annullare l'eliminazione.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Fasi del documento

- `aws:executeAwsApi`- Annulla l'eliminazione della chiave gestita dal cliente specificata nel `KeyId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che l'eliminazione della chiave è disabilitata nella chiave gestita dal cliente.

`AWSConfigRemediation-EnableKeyRotation`

Descrizione

Il `AWSConfigRemediation-EnableKeyRotation` runbook consente la rotazione automatica delle chiavi per la chiave simmetrica AWS Key Management Service (AWS KMS) gestita dal cliente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KeyId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente su cui desideri abilitare la rotazione automatica delle chiavi.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Fasi del documento

- `aws:executeAwsApi`- Abilita la rotazione automatica delle chiavi sulla chiave gestita dal cliente specificata nel `KeyId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la rotazione automatica delle chiavi è abilitata sulla chiave gestita dal cliente.

Lambda

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Lambda Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

Descrizione

Il `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` runbook abilita il AWS X-Ray live tracing sulla AWS Lambda funzione specificata nel parametro. `FunctionName`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- FunctionName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome o ARN la funzione Lambda su cui abilitare la traccia.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Abilita il tracciamento X-Ray sulla funzione Lambda specificata nel parametro. `FunctionName`
- `aws:assertAwsResourceProperty`- Verifica che il tracciamento X-Ray sia stato abilitato sulla funzione Lambda.

Output

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Risposta alla `UpdateFunctionConfiguration` API chiamata.

`AWSConfigRemediation-DeleteLambdaFunction`

Descrizione

Il `AWSConfigRemediation-DeleteLambdaFunction` runbook elimina la AWS Lambda funzione specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- LambdaFunctionName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della funzione Lambda che desideri eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Fasi del documento

- `aws:executeAwsApi`- Elimina la funzione Lambda specificata nel `LambdaFunctionName` parametro.
- `aws:executeScript`- Verifica che la funzione Lambda sia stata eliminata.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Descrizione

Il `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook crittografa, a riposo, le variabili di ambiente per la funzione (AWS Lambda Lambda) specificata utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente. Questo runbook deve essere usato solo come base per garantire che le variabili di ambiente della funzione Lambda siano crittografate secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più funzioni con diverse chiavi gestite dal cliente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- FunctionName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome o la funzione Lambda ARN di cui si desidera crittografare le variabili di ambiente.

- KMSKeyArn

  Tipo: stringa

  Descrizione: (Obbligatorio) La ARN chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare le variabili di ambiente della funzione Lambda.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Attende che la `LastUpdateStatus` proprietà sia. `Successful`
- `aws:executeAwsApi`- Crittografa le variabili di ambiente per la funzione Lambda specificata nel parametro utilizzando `FunctionName` AWS KMS la chiave gestita dal cliente specificata nel `KMSKeyArn` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la crittografia è abilitata sulle variabili di ambiente per la funzione Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descrizione

Il `AWSConfigRemediation-MoveLambdaToVPC` runbook sposta una funzione AWS Lambda (Lambda) su un Amazon Virtual Private Cloud (AmazonVPC).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- FunctionName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della funzione Lambda da trasferire su Amazon. VPC
- SecurityGroupIds

  Tipo: stringa

  Descrizione: (Obbligatorio) Il gruppo di sicurezza che IDs desideri assegnare alle interfacce di rete elastiche (ENIs) associate alla funzione Lambda.
- SubnetIds

  Tipo: stringa

  Descrizione: (Obbligatoria) La IDs sottorete in cui si desidera creare le interfacce di rete elastiche (ENIs) associate alla funzione Lambda.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Aggiorna la VPC configurazione Amazon per la funzione Lambda specificata nel `FunctionName` parametro.
- `aws:waitForAwsResourceProperty`- Attende che la `LastUpdateStatus` funzione Lambda sia attiva. `successful`
- `aws:executeScript`- Verifica che la configurazione VPC Amazon della funzione Lambda sia stata aggiornata correttamente.

`AWSSupport-RemediateLambdaS3Event`

Descrizione

Il `AWSSupport-TroubleshootLambdaS3Event` runbook fornisce una soluzione automatizzata per le procedure descritte negli articoli del AWS Knowledge Center Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda? e perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia funzione Lambda? Questo runbook ti aiuta a identificare e correggere il motivo per cui una notifica di evento di Amazon Simple Storage Service (Amazon S3) non è riuscita ad attivare la funzione specificata. AWS Lambda Se l'output del runbook suggerisce di convalidare e configurare la concorrenza della funzione Lambda, consulta Invocazione asincrona e scalabilità delle funzioni.AWS Lambda

> **Note**
>
> Gli errori «Impossibile convalidare le seguenti configurazioni di destinazione» possono verificarsi anche a causa di configurazioni errate degli eventi Amazon Simple Notification Service (AmazonSNS) e Amazon Simple Queue Service (Amazon) Amazon SQS S3. Questo runbook controlla solo le configurazioni delle funzioni Lambda. Se dopo aver usato il runbook continui a ricevere l'errore «Impossibile convalidare le seguenti configurazioni di

destinazione», esamina tutte le configurazioni di eventi Amazon e Amazon SNS Amazon S3 SQS esistenti.

[Esegui questa automazione (console)]

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LambdaFunctionArn

  Tipo: stringa

  Descrizione: (Obbligatorio) La ARN funzione Lambda.
- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 le cui notifiche di eventi attivano la funzione Lambda.
- Azione

Tipo: stringa

Valori validi: Risoluzione dei problemi | Rimedia

Descrizione: (Obbligatoria) L'azione che desideri venga eseguita dal runbook. L'`Troubleshoot`opzione consente di identificare eventuali problemi, ma non esegue alcuna azione mutante per risolverli. L'`Remediate`opzione consente di identificare e tentare di risolvere i problemi al posto tuo.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Fasi del documento

- `aws:branch`- Rami basati sull'input specificato per il `Action` parametro.

  Se il valore specificato è`Troubleshoot`:

  - `aws:executeAutomation`- Esegue il `AWSSupport-TroubleshootLambdaS3Event` runbook.
  - `aws:executeAwsApi`- Controlla l'output del `AWSSupport-TroubleshootLambdaS3Event` runbook eseguito nel passaggio precedente.

  Se il valore specificato è`Remediate`:

- `aws:executeScript`- Esegue uno script per risolvere i problemi descritti nella sezione Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda? e perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia funzione Lambda? Articoli del Knowledge Center.

Output

CheckOutput.Output

Risolvi Lambdas3Event.Output

AWSSupport-TroubleshootLambdaInternetAccess

Descrizione

Il `AWSSupport-TroubleshootLambdaInternetAccess` runbook ti aiuta a risolvere i problemi di accesso a Internet per una AWS Lambda funzione che è stata lanciata in Amazon Virtual Private Cloud (Amazon). VPC Risorse come i percorsi di sottorete, le regole dei gruppi di sicurezza e le regole della lista di controllo degli accessi alla rete (ACL) vengono esaminate per confermare che l'accesso a Internet in uscita è consentito.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- FunctionName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della funzione Lambda per la quale desideri risolvere i problemi di accesso a Internet.

- destinationIp

  Tipo: stringa

  Descrizione: (Obbligatorio) L'indirizzo IP di destinazione a cui desideri stabilire una connessione in uscita.

- destinationPort

  Tipo: stringa

  Impostazione predefinita: 443

  Descrizione: (Facoltativo) La porta di destinazione su cui si desidera stabilire una connessione in uscita.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Fasi del documento

- `aws:executeScript`- Verifica la configurazione di varie risorse nel luogo in VPC cui è stata lanciata la funzione Lambda.
- `aws:branch`- Rami in base al fatto che la funzione Lambda specificata sia VPC o meno in a.
- `aws:executeScript`- Esamina le route della tabella di routing per la sottorete in cui è stata lanciata la funzione Lambda e verifica che siano presenti le route verso un gateway di traduzione degli indirizzi di rete NAT () e un gateway Internet. Conferma che la funzione Lambda non si trova in una sottorete pubblica.
- `aws:executeScript`- Verifica che il gruppo di sicurezza associato alla funzione Lambda consenta l'accesso a Internet in uscita in base ai valori specificati per `destinationIp` i parametri and. `destinationPort`
- `aws:executeScript`- Verifica che le ACL regole associate alle sottoreti della funzione Lambda e il NAT gateway consenta l'accesso a Internet in uscita in base ai valori specificati per i parametri and. `destinationIp` `destinationPort`

Output

checkVpc.vpc - L'ID del VPC punto in cui è stata lanciata la funzione Lambda.

checkVpc.subnet - La IDs delle sottoreti in cui è stata lanciata la funzione Lambda.

checkVpc. securityGroups - Gruppi di sicurezza associati alla funzione Lambda.

controllareNACL. NACL- Messaggio di analisi con i nomi delle risorse. `LambdaIp`si riferisce all'indirizzo IP privato dell'interfaccia elastic network per la funzione Lambda. L'`LambdaIpRules`oggetto viene generato solo per le sottoreti che hanno un percorso verso un gateway. NAT Il seguente contenuto è un esempio dell'output.

```
{
   "subnet-1234567890":{
      "NACL":"acl-1234567890",
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule",
      "LambdaIpRules":{
         "{LambdaIp}":{
            "Egress":"notAllowed",
            "Ingress":"notAllowed",
```

```
            "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
 rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
 IP in your egress and ingress NACL rules"
         }
      }
   },
   "subnet-0987654321":{
      "NACL":"acl-0987654321",
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule"
   }
}
```

checkSecurityGroups.secgrps: analisi per il gruppo di sicurezza associato alla funzione Lambda. Il seguente contenuto è un esempio dell'output.

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets: analisi delle sottoreti VPC associate alla funzione Lambda. Il seguente contenuto è un esempio dell'output.

```
{
   "subnet-0c4ee6cdexample15":{
      "Route":{
         "DestinationCidrBlock":"8.8.8.0/26",
         "NatGatewayId":"nat-00f0example69fdec",
         "Origin":"CreateRoute",
         "State":"active"
      },
      "Analysis":"This Route Table has an active NAT gateway path. Also, The NAT
 gateway is launched in public subnet",
      "RouteTable":"rtb-0b1fexample16961b"
   }
}
```

AWSSupport-TroubleshootLambdaS3Event

Descrizione

Il `AWSSupport-TroubleshootLambdaS3Event` runbook fornisce una soluzione automatizzata per le procedure descritte negli articoli del AWS Knowledge Center Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda? e perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia funzione Lambda? Questo runbook ti aiuta a identificare il motivo per cui una notifica di evento di Amazon Simple Storage Service (Amazon S3) non è riuscita ad attivare la funzione specificata. AWS Lambda Se l'output del runbook suggerisce di convalidare e configurare la concorrenza della funzione Lambda, consulta Invocazione asincrona e scalabilità delle funzioni.AWS Lambda

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LambdaFunctionArn

  Tipo: stringa

Descrizione: (Obbligatoria) La ARN funzione Lambda attivata dalla notifica degli eventi di Amazon S3.

- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 le cui notifiche di eventi attivano la funzione Lambda.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Fasi del documento

- `aws:executeScript`- Esegue lo script per convalidare le impostazioni di configurazione per la notifica degli eventi di Amazon S3. Convalida la politica basata sulle risorse IAM per la funzione Lambda e genera un comando AWS Command Line Interface (AWS CLI) per aggiungere le autorizzazioni necessarie se le autorizzazioni richieste non sono presenti nella politica. Convalida le politiche delle risorse di altre funzioni Lambda che fanno parte delle notifiche degli eventi per lo stesso bucket S3 e genera AWS CLI un comando come output se mancano le autorizzazioni richieste.

Output

Lambdas3Event.OUTPUT

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Managed Workflows for Apache Airflow. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

AWSSupport-TroubleshootMWAAEnvironmentCreation

Descrizione

Il `AWSSupport-TroubleshootMWAAEnvironmentCreation` runbook fornisce informazioni per eseguire il debug dei problemi di creazione dell'ambiente Amazon Managed Workflows for Apache Airflow (AmazonMWAA) ed esegue controlli insieme ai motivi documentati con il massimo impegno per aiutare a identificare l'errore.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Recupera i dettagli dell'MWAAambiente Amazon.
- Verifica le autorizzazioni del ruolo di esecuzione.
- Verifica se l'ambiente dispone delle autorizzazioni per utilizzare la AWS KMS chiave fornita per la registrazione e se esiste il gruppo di log richiesto CloudWatch .
- Analizza i log nel gruppo di log fornito per individuare eventuali errori.
- Controlla la configurazione di rete per verificare se l'MWAAambiente Amazon ha accesso agli endpoint richiesti.
- Genera un rapporto con i risultati.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `airflow:GetEnvironment`
- `cloudtrail:LookupEvents`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRolePolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListRolePolicies`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`
- `kms:ListAliases`
- `logs:DescribeLogGroups`
- `logs:FilterLogEvents`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3control:GetPublicAccessBlock`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

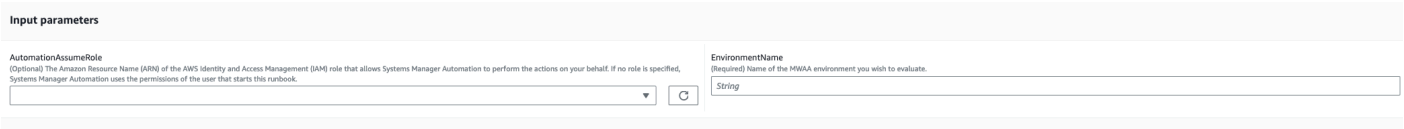
Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere AWSSupport-TroubleshootMWAAEnvironmentCreationa Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - EnvironmentName (Obbligatorio):

     Nome dell'MWAAambiente Amazon che desideri valutare.



4. Seleziona Esegui.
5. L'automazione si avvia.
6. Il documento esegue le seguenti operazioni:
   - **`GetMWAAEnvironmentDetails:`**

     Recupera i dettagli dell'MWAAambiente Amazon. Se questo passaggio fallisce, il processo di automazione si interromperà e verrà visualizzato come. `Failed`
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Verifica che il ruolo di esecuzione disponga delle autorizzazioni richieste per le risorse AmazonMWAA, Amazon S3 CloudWatch CloudWatch, Logs e Amazon. SQS Se rileva una chiave gestita dal cliente AWS Key Management Service (AWS KMS), l'automazione convalida le autorizzazioni richieste dalla chiave. Questo passaggio utilizza il `iam:SimulateCustomPolicy` API per accertare se il ruolo di esecuzione dell'automazione soddisfa tutte le autorizzazioni richieste.
   - **`CheckKMSPolicyOnKMSKey:`**

Verifica se la politica della AWS KMS chiave consente all'MWAAambiente Amazon di utilizzare la chiave per crittografare i CloudWatch log. Se la AWS KMS chiave è AWS gestita, l'automazione salta questo controllo.

- **CheckIfRequiredLogGroupsExists:**

  Verifica se esistono i gruppi di CloudWatch log richiesti per l'MWAAambiente Amazon. In caso contrario, l'automazione verifica CloudTrail eventuali `CreateLogGroup` `DeleteLogGroup` eventi. Questo passaggio verifica anche la presenza di `CreateLogGroup` eventi.

- **BranchOnLogGroupsFindings:**

  Filiali basate sull'esistenza di gruppi di CloudWatch log relativi all'MWAAambiente Amazon. Se esiste almeno un gruppo di log, l'automazione lo analizza per individuare gli errori. Se non sono presenti gruppi di log, l'automazione salta il passaggio successivo.

- **CheckForErrorsInLogGroups:**

  Analizza i gruppi di CloudWatch log per individuare gli errori.

- **GetRequiredEndPointsDetails:**

  Recupera gli endpoint di servizio utilizzati dall'ambiente Amazon. MWAA

- **CheckNetworkConfiguration:**

  Verifica che la configurazione di rete MWAA dell'ambiente Amazon soddisfi i requisiti, inclusi i controlli sui gruppi di sicurezza, la reteACLs, le sottoreti e le configurazioni delle tabelle di routing.

- **CheckEndpointsConnectivity:**

  Richiama l'automazione `AWSSupport-ConnectivityTroubleshooter` secondaria per convalidare la connettività MWAA di Amazon agli endpoint richiesti.

- **CheckS3BlockPublicAccess:**

  Verifica se il bucket Amazon S3 dell'MWAAambiente Amazon è `Block Public Access` abilitato ed esamina anche le impostazioni generali di Amazon S3 Block Public Access dell'account.

- **GenerateReport:**

  Raccoglie informazioni dall'automazione e stampa il risultato o l'output di ogni passaggio.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- Verifica delle autorizzazioni del ruolo di esecuzione MWAA dell'ambiente Amazon:

  Verifica se il ruolo di esecuzione dispone delle autorizzazioni richieste per le risorse AmazonMWAA, Amazon S3 CloudWatch CloudWatch, Logs e Amazon. SQS Se viene rilevata una AWS KMS chiave Customer Managed, l'automazione convalida le autorizzazioni richieste dalla chiave.

- Verifica della politica AWS KMS chiave MWAA dell'ambiente Amazon:

  Verifica se il ruolo di esecuzione possiede le autorizzazioni necessarie per le risorse Amazon, Amazon MWAA S3, CloudWatch Logs e Amazon. CloudWatch SQS Inoltre, se viene rilevata una AWS KMS chiave Customer Managed, l'automazione verifica le autorizzazioni richieste dalla chiave.

- Verifica dei gruppi di CloudWatch log MWAA dell'ambiente Amazon:

  Verifica se esistono i gruppi di CloudWatch log richiesti per l'MWAAambiente Amazon. In caso contrario, l'automazione verifica CloudTrail la localizzazione `CreateLogGroup` e `DeleteLogGroup` gli eventi.

- Verifica delle tabelle di MWAA routing dell'ambiente Amazon:

  Verifica se le tabelle di VPC routing Amazon nell'MWAAambiente Amazon sono configurate correttamente.

- Verifica dei gruppi di sicurezza MWAA dell'ambiente Amazon:

  Verifica se l'MWAAambiente Amazon I gruppi VPC di sicurezza Amazon sono configurati correttamente.

- Verifica dell'MWAAambiente Amazon NetworkACLs:

  Verifica se i gruppi VPC di sicurezza Amazon nell'MWAAambiente Amazon sono configurati correttamente.

- Verifica delle sottoreti MWAA dell'ambiente Amazon:

  Verifica se le sottoreti MWAA dell'ambiente Amazon sono private.

- Verifica della connettività degli endpoint richiesta MWAA dall'ambiente Amazon:

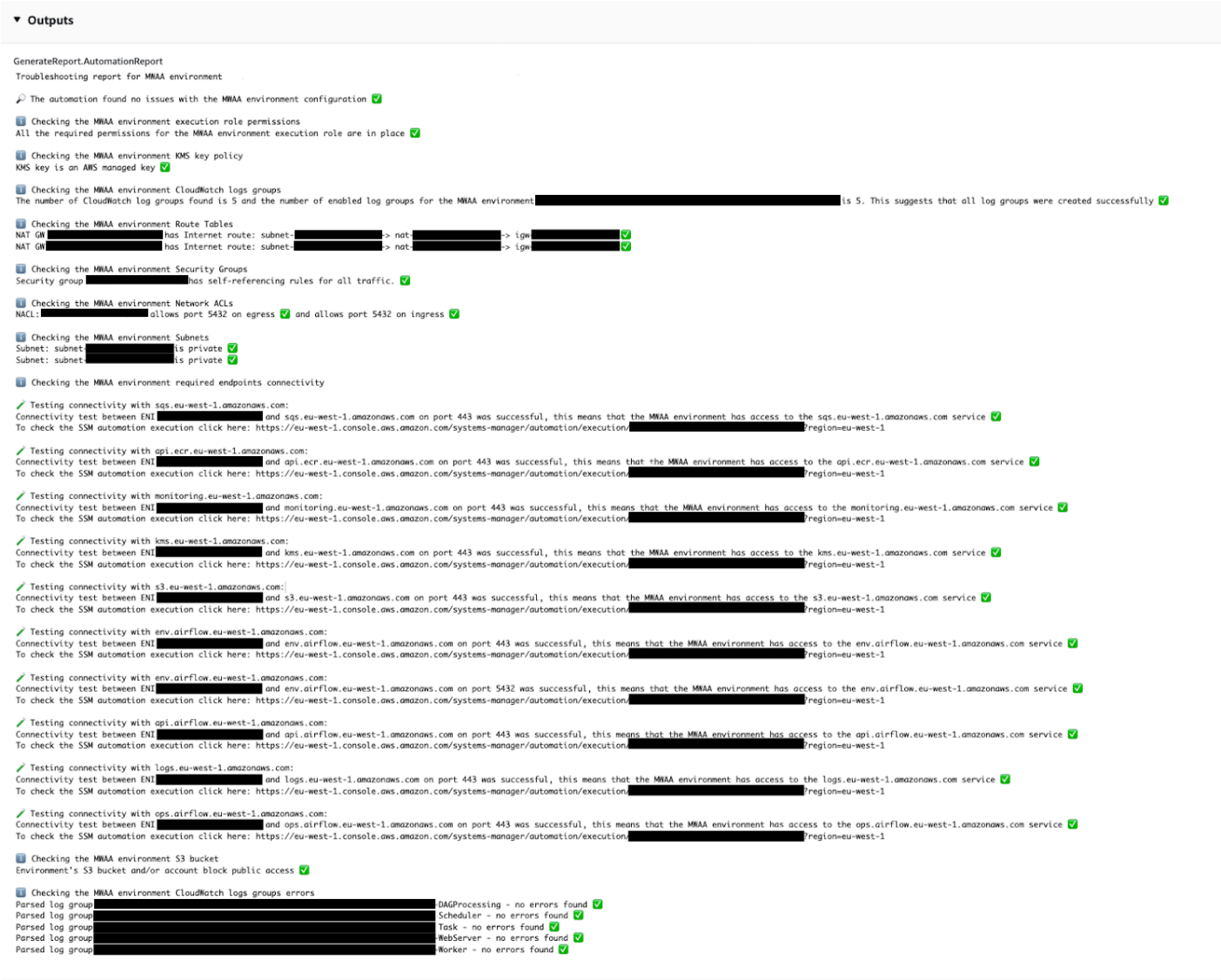
  Verifica se l'MWAAambiente Amazon può accedere agli endpoint richiesti. A tal fine, l'automazione richiama l'automazione. `AWSSupport-ConnectivityTroubleshooter`

- Verifica del bucket Amazon S3 in MWAA ambiente Amazon:

Verifica se il bucket Amazon S3 dell'MWAAambiente Amazon è `Block Public Access` abilitato ed esamina anche le impostazioni di Amazon S3 Block Public Access dell'account.

- La verifica dei CloudWatch log MWAA dell'ambiente Amazon raggruppa gli errori:

  Analizza i gruppi di CloudWatch log esistenti dell'MWAAambiente Amazon per individuare gli errori.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)

- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

Neptune

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Neptune. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableNeptuneDbAuditLogsToCloudWatch
- AWS-EnableNeptuneDbBackupRetentionPeriod
- AWS-EnableNeptuneClusterDeletionProtection

`AWS-EnableNeptuneDbAuditLogsToCloudWatch`

Descrizione

Il `AWS-EnableNeptuneDbAuditLogsToCloudWatch` runbook ti aiuta a inviare i log di controllo per un cluster Amazon Neptune DB ad Amazon Logs. CloudWatch

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DbClusterResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della risorsa del cluster Neptune DB per cui desideri abilitare i log di controllo.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Restituisce l'ID del cluster Neptune DB.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica che il tipo di motore Neptune DB sia. `neptune`
- EnableNeptuneDbAuditLogs (`aws:executeAwsApi`) - Consente l'invio dei log di controllo per il cluster Neptune DB. CloudWatch
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Verifica che lo stato del cluster Neptune DB sia. `available`

- VerifyNeptuneDbAuditLogs (`aws:executeScript`) - Verifica che i log di controllo siano stati configurati correttamente per l'invio a Logs. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

Descrizione

Il `AWS-EnableNeptuneDbBackupRetentionPeriod` runbook consente di abilitare backup automatici con un periodo di conservazione dei backup compreso tra 7 e 35 giorni per un cluster Amazon Neptune DB.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DbClusterResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della risorsa del cluster Neptune DB per cui desideri abilitare i backup.

- BackupRetentionPeriod

  Tipo: integer

  Valori validi: 7-35

  Descrizione: (Obbligatorio) Il numero di giorni di conservazione dei backup.
- PreferredBackupWindow

  Tipo: stringa

  Descrizione: (Facoltativo) Un periodo di tempo giornaliero di almeno 30 minuti per l'esecuzione dei backup. Il valore deve essere in Universal Time Coordinated (UTC) e utilizzare il formato:`hh24:mm-hh24:mm`. Il periodo di conservazione dei backup non può essere in conflitto con la finestra di manutenzione preferita.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Restituisce l'ID del cluster Neptune DB.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica che il tipo di motore Neptune DB sia. `neptune`
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Verifica che lo stato del cluster Neptune DB sia. `available`
- ModifyNeptuneDbRetentionPeriod (`aws:executeAwsApi`) - Imposta il periodo di conservazione per il cluster Neptune DB.

- VerifyNeptuneDbBackupsEnabled (`aws:executeScript`) - Verifica che il periodo di conservazione e la finestra di backup siano stati impostati correttamente.

AWS-EnableNeptuneClusterDeletionProtection

Descrizione

Il `AWS-EnableNeptuneClusterDeletionProtection` runbook abilita la protezione dall'eliminazione per il cluster Amazon Neptune specificato.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DbClusterResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del cluster Neptune su cui desideri abilitare la protezione dall'eliminazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Restituisce l'ID del cluster Neptune DB.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica che il tipo di motore del cluster DB specificato sia. `neptune`
- VerifyNeptuneStatus (`aws:waitForAwsResourceProperty`) - Verifica che lo stato del cluster sia. `available`
- EnableNeptuneDbDeletionProtection (`aws:executeAwsApi`) - Abilita la protezione dall'eliminazione sul cluster Neptune DB.
- VerifyNeptuneDbDeletionProtection (`aws:assertAwsResourceProperty`) - Verifica che la protezione da eliminazione sia abilitata sul cluster DB.

Output

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - L'output dell'APIoperazione.

Amazon RDS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Relational Database Service. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-CreateEncryptedRdsSnapshot

- AWS-CreateRdsSnapshot
- AWSConfigRemediation-DeleteRDSCluster
- AWSConfigRemediation-DeleteRDSClusterSnapshot
- AWSConfigRemediation-DeleteRDSInstance
- AWSConfigRemediation-DeleteRDSInstanceSnapshot
- AWSConfigRemediation-DisablePublicAccessToRDSInstance
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance
- AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance
- AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS
- AWSConfigRemediation-EnableMultiAZOnRDSInstance
- AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance
- AWSConfigRemediation-EnableRDSClusterDeletionProtection
- AWSConfigRemediation-EnableRDSInstanceBackup
- AWSConfigRemediation-EnableRDSInstanceDeletionProtection
- AWSConfigRemediation-ModifyRDSInstancePortNumber
- AWSSupport-ModifyRDSSnapshotPermission
- AWSPremiumSupport-PostgreSQLWorkloadReview
- AWS-RebootRdsInstance
- AWSSupport-ShareRDSSnapshot
- AWS-StartRdsInstance
- AWS-StartStopAuroraCluster
- AWS-StopRdsInstance
- AWSSupport-TroubleshootConnectivityToRDS
- AWSSupport-TroubleshootRDSIAMAuthentication
- AWSSupport-ValidateRdsNetworkConfiguration

AWS-CreateEncryptedRdsSnapshot

Descrizione

Il `AWS-CreateEncryptedRdsSnapshot` runbook crea uno snapshot crittografato da un'istanza Amazon Relational Database Service (Amazon) non crittografata. RDS

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DBInstanceIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'RDSistanza Amazon di cui desideri creare uno snapshot.
- DBSnapshotIdentifier

  Tipo: stringa

  Descrizione: (Facoltativo) Il modello di nome per lo RDS snapshot Amazon. Il modello di nome predefinito è *`DBInstanceIdentifier-yyyymmddhhmmss`*.
- ncryptedDBSnapshotIdentificatore E

  Tipo: stringa

Descrizione: (Facoltativo) Il nome dell'istantanea crittografata. Il nome predefinito è il valore specificato per il `DBSnapshotIdentifier` parametro aggiunto. `-encrypted`

- InstanceTags

  Tipo: stringa

  Descrizione: (Facoltativo) Tag da aggiungere all'istanza DB. (Esempio: Chiave= tagKey 1, Valore= tagValue 1; Chiave= tagKey 2, Valore= 2) 'tagValue

- KmsKeyId

  Tipo: stringa

  Impostazione predefinita: `alias/aws/rds`

  Descrizione: (Facoltativo) L'ID della chiaveARN, o l'alias chiave della chiave gestita dal cliente che desideri utilizzare per crittografare l'istantanea.

- SnapshotTags

  Tipo: stringa

  Descrizione: (Facoltativo) Tag da aggiungere all'istantanea. (Esempio: Chiave= tagKey 1, Valore= tagValue 1; Chiave= 2, Valore= tagKey 2) 'tagValue

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Fasi del documento

- `aws:executeScript`- Crea un'istantanea dell'istanza DB specificata nel `DBInstanceIdentifier` parametro.
- `aws:executeScript`- Verifica che l'istantanea creata nel passaggio precedente esista e sia. `available`
- `aws:executeScript`- Copia l'istantanea creata in precedenza in un'istantanea crittografata.
- `aws:executeScript`- Verifica l'esistenza dell'istantanea crittografata creata nel passaggio precedente.

Output

CopyRdsSnapshotToEncryptedRdsSnapshot. EncryptedSnapshotId - L'ID dello RDS snapshot Amazon crittografato.

AWS-CreateRdsSnapshot

Descrizione

Crea uno snapshot di Amazon Relational Database Service (RDSAmazon) per un'istanza AmazonRDS.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'DBInstanceIdID dell'RDSistanza da cui creare un'istantanea.

- DBSnapshotIdentifier

  Tipo: stringa

  Descrizione: (Facoltativo) L'DBSnapshotIdentifierID dell'RDSistantanea da creare.

- InstanceTags

  Tipo: stringa

  Descrizione: (Facoltativo) Tag da creare per esempio.

- SnapshotTags

  Tipo: stringa

  Descrizione: (Facoltativo) Tag da creare per l'istantanea.

Fasi del documento

createRDSSnapshot — Crea l'RDSistantanea e ne restituisce l'ID.

verifyRDSSnapshot — Verifica che l'istantanea creata nel passaggio precedente esista.

Output

createRDSSnapshot. SnapshotId — L'ID dell'istantanea creata.

AWSConfigRemediation-DeleteRDSCluster

Descrizione

Il `AWSConfigRemediation-DeleteRDSCluster` runbook elimina il cluster Amazon Relational Database Service (AmazonRDS) specificato. AWS Config deve essere abilitato nel luogo in Regione AWS cui esegui questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DBClusterId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`

- `rds:DescribeDBClusters`

Fasi del documento

- `aws:executeScript`- Elimina il cluster DB specificato nel `DBClusterId` parametro.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descrizione

Il `AWSConfigRemediation-DeleteRDSClusterSnapshot` runbook elimina lo snapshot del cluster Amazon Relational Database Service (AmazonRDS) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DBClusterSnapshotId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore dello snapshot del RDS cluster Amazon da eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Fasi del documento

- `aws:branch`- Verifica se l'istantanea del cluster è nello `available` stato. Se non è disponibile, il flusso termina.
- `aws:executeAwsApi`- Elimina lo snapshot del RDS cluster Amazon specificato utilizzando l'identificatore dello snapshot del cluster di database (DB).
- `aws:executeScript`- Verifica che lo snapshot del RDS cluster Amazon specificato sia stato eliminato.

`AWSConfigRemediation-DeleteRDSInstance`

Descrizione

Il `AWSConfigRemediation-DeleteRDSInstance` runbook elimina l'istanza di Amazon Relational Database Service (AmazonRDS) specificata. Quando elimini un'istanza di database (DB), tutti i backup automatici per quell'istanza vengono eliminati e non possono essere ripristinati. Le istantanee manuali del DB non vengono eliminate. Se l'istanza DB che si desidera eliminare si trova nello `incompatible-restore` stato `failedincompatible-network`, o,, è necessario impostare il `SkipFinalSnapshot` parametro su. `true`

> **Note**
>
> Se l'istanza DB che desideri eliminare si trova in un cluster Amazon Aurora DB, il runbook non eliminerà l'istanza DB se è una replica di lettura e l'unica istanza nel cluster DB.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB che desideri eliminare.
- SkipFinalSnapshot

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostato su`true`, non viene creata un'istantanea finale prima dell'eliminazione dell'istanza DB.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome dell'istanza DB dal valore specificato nel `DbiResourceId` parametro.
- `aws:branch`- Rami basati sul valore specificato nel `SkipFinalSnapshot` parametro.
- `aws:executeAwsApi`- Elimina l'istanza DB specificata nel `DbiResourceId` parametro.
- `aws:executeAwsApi`- Elimina l'istanza DB specificata nel `DbiResourceId` parametro dopo la creazione dello snapshot finale.
- `aws:assertAwsResourceProperty`- Verifica che l'istanza DB sia stata eliminata.

`AWSConfigRemediation-DeleteRDSInstanceSnapshot`

Descrizione

Il `AWSConfigRemediation-DeleteRDSInstanceSnapshot` runbook elimina lo snapshot dell'istanza Amazon Relational Database Service (AmazonRDS) specificato. Vengono eliminate solo le istantanee nello stato. `available` Questo runbook non supporta l'eliminazione di snapshot dalle istanze di database Amazon Aurora.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbSnapshotId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dello snapshot che desideri eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie lo stato dell'istantanea specificata nel parametro. `DbSnapshotId`
- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'istantanea è. `available`
- `aws:executeAwsApi`- Elimina l'istantanea specificata nel parametro. `DbSnapshotId`
- `aws:executeScript`- Verifica che l'istantanea sia stata eliminata.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descrizione

Il `AWSConfigRemediation-DisablePublicAccessToRDSInstance` runbook disabilita l'accessibilità pubblica per l'istanza di database (DB) di Amazon Relational Database Service (RDSAmazon) specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB per cui desideri disabilitare l'accessibilità pubblica.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Verifica che le istanze DB siano in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Disattiva l'accessibilità pubblica sull'istanza DB.
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB passi a uno stato. `MODIFYING`
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB passi a uno `AVAILABLE` stato.
- `aws:assertAwsResourceProperty`- Conferma che l'accessibilità pubblica è disabilitata sull'istanza DB.

`AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster`

Descrizione

Il `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` runbook abilita l'`CopyTagsToSnapshot`impostazione sul cluster Amazon Relational Database Service (RDSAmazon) specificato. L'attivazione di questa impostazione copia tutti i tag dal cluster DB nelle istantanee del cluster DB. L'impostazione predefinita prevede di non copiarli. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- ApplyImmediately

  Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per il `PreferredMaintenanceWindow` cluster DB.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbClusterResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui desideri abilitare l'`CopyTagsToSnapshot`impostazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore del cluster DB dall'identificatore di risorse del cluster DB.
- `aws:assertAwsResourceProperty`- Conferma che il cluster DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita l'`CopyTagsToSnapshot`impostazione sul cluster DB.

- `aws:assertAwsResourceProperty`- Conferma che l'`CopyTagsToSnapshot`impostazione è abilitata sul cluster DB.

`AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance`

Descrizione

Il `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` runbook abilita l'`CopyTagsToSnapshot`impostazione sull'istanza Amazon Relational Database Service (RDSAmazon) specificata. L'attivazione di questa impostazione copia tutti i tag dall'istanza DB negli snapshot dell'istanza DB. L'impostazione predefinita prevede di non copiarli. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- ApplyImmediately

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow`istanza DB.
- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare l'`CopyTagsToSnapshot`impostazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita l'`CopyTagsToSnapshot`impostazione sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che l'`CopyTagsToSnapshot`impostazione è abilitata sull'istanza DB.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Descrizione

Il `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` runbook abilita il monitoraggio avanzato sull'istanza di RDS database Amazon specificata. Per informazioni su Enhanced Monitoring, consulta Enhanced Monitoring nella Amazon RDS User Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- MonitoringInterval

  Tipo: integer

  Valori validi: 1 | 5 | 10 | 15 | 30 | 60

  Descrizione: (Obbligatorio) L'intervallo in secondi durante il quale le metriche di Enhanced Monitoring vengono raccolte dall'istanza DB.
- MonitoringRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) del IAM ruolo che consente RDS ad Amazon di inviare i parametri di Enhanced Monitoring ad Amazon CloudWatch Logs.

- ResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare Enhanced Monitoring.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita il monitoraggio avanzato sull'istanza DB.
- `aws:executeScript`- Conferma che il monitoraggio avanzato è abilitato sull'istanza DB.

`AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS`

Descrizione

Il `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` runbook abilita l'`AutoMinorVersionUpgrade`impostazione sull'istanza di RDS database Amazon specificata. L'abilitazione di questa impostazione significa che gli aggiornamenti delle versioni minori vengono applicati automaticamente all'istanza DB durante la finestra di manutenzione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri `AutoMinorVersionUpgrade` impostare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.

- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita l'`AutoMinorVersionUpgrade`impostazione sull'istanza DB.
- `aws:executeScript`- Conferma che l'`AutoMinorVersionUpgrade`impostazione è abilitata sull'istanza DB.

`AWSConfigRemediation-EnableMultiAZOnRDSInstance`

Descrizione

Il `AWSConfigRemediation-EnableMultiAZOnRDSInstance` runbook modifica l'istanza del database (DB) Amazon Relational Database Service (RDSAmazon) in una distribuzione Multi-AZ. La modifica di questa impostazione non comporta un'interruzione. La modifica viene applicata durante la finestra di manutenzione successiva, a meno che non si imposti il `ApplyImmediately` parametro su. `true`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- ApplyImmediately

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow`istanza DB.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore Regione AWS-unique e immutabile per l'istanza DB per abilitare l'impostazione. `MultiAZ`

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Recupera il nome dell'istanza DB utilizzando il valore fornito nel `DBInstanceId` parametro.
- `aws:executeAwsApi`- Verifica che sia. `DBInstanceStatus` `available`
- `aws:branch`- Verifica se `MultiAZ` è già impostato `true` su sull'istanza DB specificata nel `DbiResourceId` parametro.
- `aws:executeAwsApi`- Modifica l'`MultiAZ`impostazione `true` sull'istanza DB specificata nel `DbiResourceId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che `MultiAZ` sia impostato `true` sull'istanza DB specificata nel `DbiResourceId` parametro.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Descrizione

Il `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` runbook abilita Performance Insights sull'istanza Amazon RDS DB specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui si desidera abilitare Performance Insights.
- PerformanceInsightsKMSKeyId

  Tipo: stringa

  Impostazione predefinita: `alias/aws/rds`

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN), l'ID chiave o l'alias chiave della chiave gestita dal cliente AWS Key Management Service (AWS KMS) che desideri che Performance Insights utilizzi per crittografare tutti i dati potenzialmente sensibili. Se inserisci l'alias chiave per questo parametro, aggiungi al valore il prefisso. **`alias/`** Se non si specifica un valore per questo parametro, Chiave gestita da AWS viene utilizzato.

- PerformanceInsightsRetentionPeriod

  Tipo: integer

  Valori validi: 7.731

  Impostazione predefinita: 7

  Descrizione: (Facoltativo) Il numero di giorni in cui desideri conservare i dati di Performance Insights.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'istanza DB è. `available`
- `aws:executeAwsApi`- Raccoglie ARN la chiave gestita AWS KMS dal cliente specificata nel `PerformanceInsightsKMSKeyId` parametro.

- `aws:branch`- Verifica se un valore è già assegnato alla `PerformanceInsightsKMSKeyId` proprietà dell'istanza DB.
- `aws:executeAwsApi`- Abilita Performance Insights sull'istanza DB specificata nel `DbiResourceId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che il valore specificato per il `PerformanceInsightsKMSKeyId` parametro è stato utilizzato per abilitare la crittografia per Performance Insights sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che Performance Insights è abilitato sull'istanza DB.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descrizione

Il `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook abilita la protezione dall'eliminazione sul cluster Amazon Relational Database Service (RDSAmazon) specificato. AWS Config deve essere abilitato nel luogo in Regione AWS cui esegui questa automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ClusterId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome del cluster DB dall'identificatore di risorse del cluster DB.
- `aws:assertAwsResourceProperty`- Verifica che lo stato del cluster DB sia. `available`
- `aws:executeAwsApi`- Abilita la protezione dall'eliminazione sul cluster DB specificato nel `ClusterId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la protezione da eliminazione sia stata abilitata sul cluster DB.

AWSConfigRemediation-EnableRDSInstanceBackup

Descrizione

Il `AWSConfigRemediation-EnableRDSInstanceBackup` runbook abilita i backup per l'istanza di database Amazon Relational Database Service (AmazonRDS) specificata. Questo runbook non supporta l'abilitazione dei backup per le istanze di database Amazon Aurora.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- ApplyImmediately

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow`istanza DB.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BackupRetentionPeriod

  Tipo: integer

  Valori validi: 1-35

Descrizione: (Obbligatorio) Il numero di giorni di conservazione dei backup.

- DbiResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB per cui desideri abilitare i backup.

- PreferredBackupWindow

  Tipo: stringa

  Descrizione: (Facoltativo) L'intervallo di tempo giornaliero (inUTC) durante il quale vengono creati i backup.

  Vincoli:

  - Deve essere nel formato `hh24:mi-hh24:mi`
  - Deve essere in formato Coordinated Universal Time (UTC)
  - Il valore non deve essere in conflitto con la finestra di manutenzione preferita
  - Il valore deve essere almeno di 30 minuti

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeScript`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB. Abilita i backup per l'istanza DB. Conferma che i backup sono abilitati sull'istanza DB.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descrizione

Il AWSConfigRemediation-EnableRDSInstanceDeletionProtection runbook abilita la protezione dall'eliminazione sull'istanza di RDS database Amazon specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- ApplyImmediately

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow`istanza DB.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DbInstanceResourceId

  Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:executeAwsApi`- Abilita la protezione dall'eliminazione sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che la protezione da eliminazione è abilitata sull'istanza DB.

`AWSConfigRemediation-ModifyRDSInstancePortNumber`

Descrizione

Il `AWSConfigRemediation-ModifyRDSInstancePortNumber` runbook modifica il numero di porta su cui l'istanza Amazon Relational Database Service (AmazonRDS) accetta le connessioni. L'esecuzione di questa automazione riavvierà il database.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- PortNumber

  Tipo: stringa

  Descrizione: (Facoltativo) Il numero di porta su cui desideri che l'istanza DB accetti le connessioni.
- RDSDBInstanceResourceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB di cui desideri modificare il numero di porta in ingresso.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.

- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Modifica il numero di porta in entrata su cui l'istanza DB accetta le connessioni.
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB si trovi in uno stato. `MODIFYING`
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB si trovi in uno `AVAILABLE` stato.

AWSSupport-ModifyRDSSnapshotPermission

Descrizione

Il `AWSSupport-ModifyRDSSnapshotPermission` runbook ti aiuta a modificare le autorizzazioni per più snapshot di Amazon Relational Database Service (Amazon). RDS Usando questo runbook, puoi creare istantanee `Public` o `Private` condividerle con altri. Account AWS Le istantanee crittografate con una KMS chiave predefinita non possono essere condivise con altri account utilizzando questo runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AccountIds

  Tipo: StringList

  Impostazione predefinita: none

  Descrizione: (Facoltativo) Gli IDs account con cui vuoi condividere le istantanee. Questo parametro è obbligatorio se si immette `No` il valore del `Private` parametro.

- AccountPermissionOperation

  Tipo: stringa

  Valori validi: aggiungi | rimuovi

  Impostazione predefinita: none

  Descrizione: (Facoltativo) Il tipo di operazione da eseguire.

- Privata

  Tipo: stringa

  Valori validi: Sì | No

  Descrizione: (Obbligatorio) Inserisci `No` il valore se desideri condividere istantanee con account specifici.

- SnapshotIdentifiers

  Tipo: StringList

  Descrizione: (Obbligatorio) I nomi degli RDS snapshot Amazon di cui desideri modificare l'autorizzazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Fasi del documento

1. `aws:executeScript`- Verifica le IDs istantanee fornite nel parametro. `SnapshotIdentifiers` Dopo aver verificato ilIDs, lo script verifica la presenza di istantanee crittografate e genera un elenco, se ne vengono trovate.
2. `aws:branch`- Suddivide l'automazione in base al valore immesso per il parametro. `Private`
3. `aws:executeScript`- Modifica le autorizzazioni delle istantanee specificate per condividerle con gli account specificati.
4. `aws:executeScript`- Modifica le autorizzazioni delle istantanee per cambiarle da a. `Public` `Private`

Output

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Risultato

MakePrivate.Risultato

MakePrivate.Comandi

AWSPremiumSupport-PostgreSQLWorkloadReview

Descrizione

Il `AWSPremiumSupport-PostgreSQLWorkloadReview` runbook acquisisce più istantanee delle statistiche sull'utilizzo del database Amazon Relational Database Service (RDSAmazon) SQL Postgre. Le statistiche acquisite sono necessarie a un esperto di AWS Support Proactive Services per eseguire una revisione operativa. Le statistiche vengono raccolte utilizzando un set di script shell SQL e personalizzati. Questi script vengono scaricati in un'istanza temporanea di Amazon Elastic Compute Cloud EC2 (Amazon) creata da questo runbook. Account AWS Il runbook richiede di fornire le credenziali utilizzando un AWS Secrets Manager segreto contenente una coppia chiave-valore

nome utente e password. Il nome utente deve avere i permessi per interrogare le viste e le funzioni statistiche standard di SQL Postgre.

Questo runbook crea automaticamente le seguenti AWS risorse utilizzando uno stack. Account AWS AWS CloudFormation È possibile monitorare la creazione dello stack utilizzando la console. AWS CloudFormation

- Un cloud privato virtuale (VPC) e un'EC2istanza Amazon lanciati in una sottorete privata di VPC con connettività opzionale a Internet tramite un NAT gateway.
- Un ruolo AWS Identity and Access Management (IAM) collegato all'EC2istanza temporanea di Amazon con le autorizzazioni per recuperare il valore segreto di Secrets Manager. Il ruolo fornisce anche le autorizzazioni per caricare file su un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta e, facoltativamente, su un case. AWS Support
- Una connessione VPC peering per consentire la connettività tra l'istanza DB e l'EC2istanza Amazon temporanea.
- VPCEndpoint Systems Manager, Secrets Manager e Amazon S3 collegati al dispositivo temporaneo. VPC
- Una finestra di manutenzione con attività registrate che avviano e interrompono periodicamente l'EC2istanza Amazon temporanea, eseguono script di raccolta dati e caricano file in un bucket Amazon S3. Viene inoltre creato un IAM ruolo per la finestra di manutenzione che fornisce le autorizzazioni per eseguire le attività registrate.

Al termine del runbook, lo AWS CloudFormation stack utilizzato per creare AWS le risorse necessarie viene eliminato e il report viene caricato nel bucket Amazon S3 di tua scelta e, facoltativamente, in un case. AWS Support

> **Note**
>
> Per impostazione predefinita, viene preservato il EBS volume Amazon root dell'EC2istanza Amazon temporanea. Puoi ignorare questa opzione impostando il `EbsVolumeDeleteOnTermination` parametro su. `true`

Prerequisiti

- Abbonamento Enterprise Support Questo runbook e Proactive Services Workload Diagnostics and Reviews richiedono un abbonamento Enterprise Support. Prima di utilizzare questo runbook,

contattate il Technical Account Manager (TAM) o lo Specialista TAM () per istruzioni. STAM Per ulteriori informazioni, consulta AWS Support Proactive Services.

- Account e Regione AWS quote Assicurati di non aver raggiunto il numero massimo di EC2 istanze Amazon o di VPCs poterle creare nell'account e nella regione in cui utilizzi questo runbook. Se devi richiedere un aumento del limite, consulta il modulo Aumento del limite di servizio.
- Configurazione del database
  1. L'`pg_stat_statements`estensione deve essere configurata nel database specificato nel `DatabaseName` parametro. Se non è stata effettuata la configurazione `pg_stat_statements` in`shared_preload_libraries`, è necessario modificare il valore nel DB Parameter Group e applicare le modifiche. Le modifiche al parametro `shared_preload_libraries` richiedono il riavvio dell'istanza DB. Per ulteriori informazioni, consulta la sezione Uso di gruppi di parametri. L'aggiunta `pg_stat_statements` a `shared_preload_libraries` aggiungerà un sovraccarico prestazionale. Tuttavia, ciò è utile per tenere traccia delle prestazioni delle singole dichiarazioni. Per ulteriori informazioni sull'`pg_stat_statements`estensione, consulta la documentazione di Postgre. SQL Se non configurate l'`pg_stat_statements`estensione o se l'estensione non è presente nel database utilizzato per la raccolta delle statistiche, l'analisi a livello di dichiarazione non verrà presentata nella revisione operativa.
  2. Assicurati che `track_counts` i `track_activities` parametri non siano disattivati. Se questi parametri sono disattivati nel DB Parameter Group, non saranno disponibili statistiche significative. La modifica di questi parametri richiederà il riavvio dell'istanza DB. Per ulteriori informazioni, consulta Lavorare con i parametri sull'istanza SQL database Amazon RDS for Postgre.
  3. Se il `track_io_timing` parametro è disattivato, le statistiche a livello di I/O non verranno incluse nella revisione operativa. La modifica `track_io_timing` richiederà il riavvio dell'istanza DB e comporterà un sovraccarico di prestazioni aggiuntivo a seconda del carico di lavoro dell'istanza DB. Nonostante il sovraccarico di prestazioni per i carichi di lavoro critici, questo parametro fornisce informazioni utili relative al tempo di I/O per query.

Fatturazione e addebiti Ti Account AWS verranno addebitati i costi associati all'EC2istanza Amazon temporanea, al EBS volume Amazon associato, al NAT gateway e ai dati trasferiti durante l'esecuzione di questa automazione. Per impostazione predefinita, questo runbook crea un'istanza `t3.micro` Amazon Linux 2 per raccogliere le statistiche. Il runbook avvia e arresta l'istanza tra i passaggi per ridurre i costi.

Sicurezza e governance dei dati Questo runbook raccoglie statistiche interrogando le visualizzazioni e le funzioni statistiche di SQLPostgre. Assicurati che le credenziali fornite nel `SecretId` parametro

consentano solo autorizzazioni di sola lettura per le visualizzazioni e le funzioni delle statistiche. Come parte dell'automazione, gli script di raccolta vengono caricati nel bucket Amazon S3 e possono essere collocati in. `s3://amzn-s3-demo-bucket/automation execution id/queries/`

Questi script raccolgono dati che vengono utilizzati da uno AWS specialista per esaminare gli indicatori chiave di prestazione a livello di oggetto. Lo script raccoglie informazioni come il nome della tabella, il nome dello schema e il nome dell'indice. Se una di queste informazioni contiene informazioni sensibili come indicatori di fatturato, nome utente, indirizzo e-mail o qualsiasi altra informazione di identificazione personale, ti consigliamo di interrompere questa revisione del carico di lavoro. Contattateci AWS TAM per discutere di un approccio alternativo per la revisione del carico di lavoro.

Assicurati di avere l'approvazione e l'autorizzazione necessarie per condividere le statistiche e i metadati raccolti da questa automazione. AWS

Considerazioni sulla sicurezza Se imposti il `UpdateRdsSecurityGroup` parametro `suyes`, il runbook aggiorna il gruppo di sicurezza associato all'istanza DB per consentire il traffico in entrata dall'indirizzo IP privato dell'EC2istanza Amazon temporanea.

Se imposti il `UpdateRdsRouteTable` parametro `suyes`, il runbook aggiorna la tabella di routing associata alla sottorete in cui è in esecuzione l'istanza DB per consentire il traffico verso l'EC2istanza Amazon temporanea tramite la connessione VPC peering.

Creazione di utenti Per consentire allo script di raccolta di connettersi al tuo RDS database Amazon, devi configurare un utente con le autorizzazioni per leggere le visualizzazioni statistiche. Quindi è necessario memorizzare le credenziali in Secrets Manager. Ti consigliamo di creare un nuovo utente dedicato per questa automazione. La creazione di un utente separato consente di controllare e tenere traccia delle attività eseguite da questa automazione.

1. Crea un nuovo utente.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Assicurati che questo utente possa effettuare solo connessioni di sola lettura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Imposta limiti a livello utente.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET work_mem=4096;"

psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET statement_timeout=10000;"

psql -h <database_connection_endpoint> -p <database_port>
-U <admin_user> -c "ALTER USER <user_name> SET
idle_in_transaction_session_timeout=60000;"
```

4. Concedi `pg_monitor` le autorizzazioni al nuovo utente in modo che possa accedere alle statistiche del DB. (Il `pg_monitor` ruolo è membro di `pg_read_all_settingspg_read_all_stats`, e`pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Autorizzazioni aggiunte al profilo dell'EC2istanza Amazon temporanea da questa Systems Manager Automation Le seguenti autorizzazioni vengono aggiunte al IAM ruolo associato all'istanza Amazon EC2 temporanea. La policy `AmazonSSMManagedInstanceCore` gestita è anche associata al IAM ruolo per consentire la gestione dell'EC2istanza Amazon da parte di Systems Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeTags"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation execution id/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account id:secret:secret id",
            "Effect": "Allow"
        },
        {
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:DescribeCases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Autorizzazioni aggiunte alla finestra di manutenzione temporanea da questa automazione di Systems Manager Le seguenti autorizzazioni vengono aggiunte automaticamente al IAM ruolo associato alle attività di manutenzione di Windows. Le attività di manutenzione di Windows vengono avviate, interrotte e inviano comandi all'EC2istanza temporanea di Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
                "ssm:GetCommandInvocation",
                "ssm:GetCalendarState",
                "ssm:CancelCommand",
                "ec2:DescribeInstanceStatus"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ssm:SendCommand",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ec2:region:account id:instance/temporary instance id",
                "arn:aws:ssm:*:*:document/AWS-RunShellScript",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            },
            "Action": "iam:PassRole",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

[Esegui questa automazione (console)]

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza DB.

- DatabaseName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del database ospitato sull'istanza DB.

- SecretId

  Tipo: stringa

  Descrizione: (Obbligatorio) Il segreto ARN di Secrets Manager contenente la coppia chiave-valore nome utente e password. Lo AWS CloudFormation stack crea una IAM policy con le autorizzazioni necessarie per eseguire questa `GetSecretValue` operazione. ARN Le credenziali vengono utilizzate per consentire all'istanza temporanea di raccogliere le statistiche del database. Contattate il vostro TAM o STAM per discutere delle autorizzazioni minime richieste.

- Riconosci

  Tipo: stringa

  Descrizione: (Obbligatorio) Inserisci **`yes`** se riconosci che questo runbook creerà risorse temporanee nel tuo account per raccogliere statistiche dall'istanza DB. Ti consigliamo di contattare il tuo TAM o STAM prima di eseguire questa automazione.

- SupportCase

  Tipo: stringa

Descrizione: (Facoltativo) Il numero del AWS Support caso fornito dal tuo TAM oSTAM. Se fornito, il runbook aggiorna il caso e allega i dati raccolti. Questa opzione richiede che l'EC2istanza Amazon temporanea disponga di connettività Internet per accedere all' AWS Support APIendpoint. È necessario impostare il `AllowVpcInternetAccess` parametro su. `true` L'oggetto del caso deve contenere la frase`AWSPremiumSupport-PostgreSQLWorkloadReview`.

- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 nel tuo account in cui desideri caricare i dati raccolti dall'automazione. Verifica che la policy del bucket non conceda autorizzazioni di lettura o scrittura non necessarie ai principali che non hanno bisogno di accedere al contenuto del bucket. Ti consigliamo di creare un nuovo bucket Amazon S3 temporaneo ai fini di questa automazione. Il runbook fornisce le autorizzazioni per l'`s3:PutObject`APIoperazione sul IAM ruolo associato all'istanza Amazon EC2 temporanea. I file caricati verranno archiviati in. `s3://`*`bucket name`*`/`*`automation execution id`*`/`

- InstanceType

  Tipo: stringa

  Descrizione: (Facoltativo) Il tipo di EC2 istanza Amazon temporanea che eseguirà gli script personalizzati SQL e di shell.

  Valori validi: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Predefinito: t3.micro

- VpcCidr

  Tipo: stringa

  Descrizione: (Facoltativo) L'intervallo di indirizzi IP in CIDR notazione per il nuovo VPC (ad esempio,). `172.31.0.0/16` Assicurati di selezionarne uno CIDR che non si sovrapponga o corrisponda a quello esistente VPC con connettività alla tua istanza DB. La più piccola VPC che puoi creare utilizza una subnet mask /28, mentre la più grande VPC utilizza una subnet mask /16.

  Impostazione predefinita: 172.31.0.0/16

- StackResourcesNamePrefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso e il tag del nome delle risorse AWS CloudFormation dello stack. Il runbook crea le risorse dello AWS CloudFormation stack utilizzando questo prefisso come parte del nome e del tag applicati alle risorse. La struttura per la coppia chiave-valore del tag è. *StackResourcesNamePrefix*`:{{automation:EXECUTION_ID}}`

Predefinito: AWSPostgreSQLWorkloadReview

- Pianificazione

  Tipo: stringa

  Descrizione: (Facoltativo) La pianificazione della finestra di manutenzione. Specifica la frequenza con cui la finestra di manutenzione esegue le attività. Il valore predefinito è every`1 hour`.

  Valori validi: 15 minuti | 30 minuti | 1 ora | 2 ore | 4 ore | 6 ore | 12 ore | 1 giorno | 2 giorni | 4 giorni

  Impostazione predefinita: 1 ora

- Durata

  Tipo: integer

  Descrizione: (Facoltativo) La durata massima, in minuti, per cui si desidera consentire l'esecuzione dell'automazione. La durata massima supportata è di 8.640 minuti (6 giorni). Il valore predefinito è 4.320 minuti (3 giorni).

  Valori validi: 30-8640

  Valore predefinito: 4320

- UpdateRdsRouteTable

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, il runbook aggiorna la tabella di routing associata alla sottorete in cui viene eseguita l'istanza DB. Viene aggiunto un IPv4 percorso per indirizzare il traffico verso l'IPV4indirizzo privato temporaneo dell'EC2istanza Amazon tramite la connessione VPC peering appena creata.

  Valori validi: true | false

Impostazione predefinita: false

- AllowVpcInternetAccess

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, il runbook crea un NAT gateway per fornire connettività Internet all'EC2istanza Amazon temporanea per comunicare con l' AWS Support APIendpoint. Puoi lasciare questo parametro come `false` se desideri solo che il runbook carichi l'output nel tuo bucket Amazon S3.

  Valori validi: true | false

  Impostazione predefinita: false

- UpdateRdsSecurityGroup

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, il runbook aggiorna il gruppo di sicurezza associato all'istanza DB per consentire il traffico proveniente dall'indirizzo IP privato dell'istanza temporanea.

  Valori validi: false | true

  Impostazione predefinita: false

- EbsVolumeDeleteOnTermination

  Tipo: stringa

  Descrizione: (Facoltativo) Se impostato su`true`, il volume root dell'EC2istanza Amazon temporanea viene eliminato dopo il completamento del runbook e l'eliminazione dello stack. AWS CloudFormation

  Valori validi: false | true

  Impostazione predefinita: false

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudformation:CreateStack`
- `cloudformation:DeleteStack`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AcceptVpcPeeringConnection`
- `ec2:AllocateAddress`
- `ec2:AssociateRouteTable`
- `ec2:AssociateVpcCidrBlock`
- `ec2:AttachInternetGateway`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateEgressOnlyInternetGateway`
- `ec2:CreateInternetGateway`
- `ec2:CreateNatGateway`
- `ec2:CreateRoute`
- `ec2:CreateRouteTable`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:CreateTags`
- `ec2:CreateVpc`
- `ec2:CreateVpcEndpoint`
- `ec2:CreateVpcPeeringConnection`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DeleteInternetGateway`
- `ec2:DeleteNatGateway`

- ec2:DeleteRoute
- ec2:DeleteRouteTable
- ec2:DeleteSecurityGroup
- ec2:DeleteSubnet
- ec2:DeleteTags
- ec2:DeleteVpc
- ec2:DeleteVpcEndpoints
- ec2:DescribeAddresses
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInternetGateways
- ec2:DescribeNatGateways
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DetachInternetGateway
- ec2:DisassociateRouteTable
- ec2:DisassociateVpcCidrBlock
- ec2:ModifySubnetAttribute
- ec2:ModifyVpcAttribute
- ec2:RebootInstances
- ec2:ReleaseAddress
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

- ec2:StartInstances
- ec2:StopInstances
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:GetRolePolicy
- iam:PassRole
- iam:PutRolePolicy
- iam:RemoveRoleFromInstanceProfile
- iam:TagPolicy
- iam:TagRole
- rds:DescribeDBInstances
- s3:GetAccountPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:ListBucket
- ssm:AddTagsToResource
- ssm:CancelMaintenanceWindowExecution
- ssm:CreateDocument

- ssm:CreateMaintenanceWindow
- ssm:DeleteDocument
- ssm:DeleteMaintenanceWindow
- ssm:DeregisterTaskFromMaintenanceWindow
- ssm:DescribeAutomationExecutions
- ssm:DescribeDocument
- ssm:DescribeInstanceInformation
- ssm:DescribeMaintenanceWindowExecutions
- ssm:GetCalendarState
- ssm:GetDocument
- ssm:GetMaintenanceWindowExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListTagsForResource
- ssm:RegisterTaskWithMaintenanceWindow
- ssm:RemoveTagsFromResource
- ssm:SendCommand
- support:AddAttachmentsToSet
- support:AddCommunicationToCase
- support:DescribeCases

Fasi del documento

1. aws:assertAwsResourceProperty- Conferma che l'istanza DB è nello available stato.
2. aws:executeAwsApi- Raccoglie dettagli sull'istanza DB.
3. aws:executeScript- Verifica se il bucket Amazon S3 specificato in S3BucketName consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.
4. aws:executeScript- Ottiene il contenuto del AWS CloudFormation modello dall'allegato Automation Runbook utilizzato per creare le risorse temporanee AWS nel tuo. Account AWS

5. `aws:createStack`- Crea le risorse dello AWS CloudFormation stack.
6. `aws:waitForAwsResourceProperty`- Attende l'esecuzione dell'EC2istanza Amazon creata dal AWS CloudFormation modello.
7. `aws:executeAwsApi`- Ottiene IDs l'EC2istanza Amazon temporanea e la connessione VPC peering creata da AWS CloudFormation.
8. `aws:executeAwsApi`- Ottiene l'indirizzo IP per l'EC2istanza Amazon temporanea per configurare la connettività con l'istanza DB.
9. `aws:executeAwsApi`- Etichetta il EBS volume Amazon collegato all'EC2istanza Amazon temporanea.
10. `aws:waitForAwsResourceProperty`- Attende che l'EC2istanza Amazon temporanea superi i controlli di stato.
11. `aws:waitForAwsResourceProperty`- Attende che l'EC2istanza Amazon temporanea venga gestita da Systems Manager. Se questo passaggio scade o fallisce, il runbook riavvia l'istanza.
    a. `aws:executeAwsApi`- Riavvia l'EC2istanza Amazon temporanea se il passaggio precedente non è riuscito o è scaduto.
    b. `aws:waitForAwsResourceProperty`- Attende che l'EC2istanza Amazon temporanea venga gestita da Systems Manager dopo il riavvio.
12. `aws:runCommand`- Installa i requisiti dell'applicazione Metadata Collector sull'istanza Amazon temporanea. EC2
13. `aws:runCommand`- Configura l'accesso alla tua istanza DB creando un file di configurazione sull'EC2istanza Amazon temporanea.
14. `aws:executeAwsApi`- Crea una finestra di manutenzione per eseguire periodicamente l'applicazione di raccolta dei metadati utilizzando Run Command. La finestra di manutenzione avvia e interrompe l'istanza tra i comandi.
15. `aws:waitForAwsResourceProperty`- Attende che la finestra di manutenzione creata dal AWS CloudFormation modello sia pronta.
16. `aws:executeAwsApi`- Ottiene IDs la finestra di manutenzione e il calendario delle modifiche creato da AWS CloudFormation.
17. `aws:sleep`- Attende la data di fine della finestra di manutenzione.
18. `aws:executeAwsApi`- Disattiva la finestra di manutenzione.
19. `aws:executeScript`- Ottiene i risultati delle attività eseguite durante la finestra di manutenzione.
20. `aws:waitForAwsResourceProperty`- Attende che la finestra di manutenzione termini l'ultima operazione prima di continuare.

21. `aws:branch`- Suddivide il flusso di lavoro a seconda che sia stato fornito un valore per il `SupportCase` parametro.
    a. `aws:changeInstanceState`- Avvia l'EC2istanza Amazon temporanea e attende il completamento dei controlli di stato prima di caricare il report.
    b. `aws:waitForAwsResourceProperty`- Attende che l'EC2istanza Amazon temporanea venga gestita da Systems Manager. Se questo passaggio si interrompe o fallisce, il runbook riavvia l'istanza.
        i. `aws:executeAwsApi`- Riavvia l'EC2istanza Amazon temporanea se il passaggio precedente non è riuscito o è scaduto.
        ii. `aws:waitForAwsResourceProperty`- Attende che l'EC2istanza Amazon temporanea venga gestita da Systems Manager dopo il riavvio.
    c. `aws:runCommand`- Allega il rapporto sui metadati al AWS Support caso se hai fornito un valore per il parametro. `SupportCase` Lo script comprime e divide il rapporto in file da 5 MB. Il numero massimo di file che lo script allega a un AWS Support caso è 12.
22. `aws:changeInstanceState`- Interrompe l'EC2istanza Amazon temporanea nel caso in cui lo AWS CloudFormation stack non riesca a eliminare.
23. `aws:executeAwsApi`- Descrive gli eventi AWS CloudFormation dello stack se i runbook non riescono a creare o aggiornare lo stack. AWS CloudFormation
24. `aws:waitForAwsResourceProperty`- Attende che lo AWS CloudFormation stack raggiunga lo stato di terminale prima di eliminarlo.
25. `aws:executeAwsApi`- Elimina lo AWS CloudFormation stack escludendo la finestra di manutenzione. Il EBS volume principale Amazon associato all'EC2istanza Amazon temporanea viene preservato se il valore del `EbsVolumeDeleteOnTermination` parametro è stato impostato su`false`.

AWS-RebootRdsInstance

Descrizione

Il `AWS-RebootRdsInstance` runbook riavvia un'istanza DB di Amazon Relational Database Service (AmazonRDS) se non è già in fase di riavvio.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon RDS DB che desideri riavviare.

Fasi del documento

RebootInstance - Riavvia l'istanza DB se non è già in fase di riavvio.

WaitForAvailableState - Attende che l'istanza DB completi il processo di riavvio.

Output

Questa automazione non ha uscite.

AWSSupport-ShareRDSSnapshot

Descrizione

Il `AWSSupport-ShareRDSSnapshot` runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo del Knowledge Center Come posso condividere uno snapshot

crittografato di Amazon RDS DB con un altro account? Se lo snapshot di Amazon Relational Database Service (Amazon RDS) è stato crittografato utilizzando l' Chiave gestita da AWS impostazione predefinita, non è possibile condividere lo snapshot. In questo caso, devi copiare lo snapshot utilizzando una chiave gestita dal cliente e quindi condividerlo con l'account di destinazione. Questa automazione esegue questi passaggi utilizzando il valore specificato nel `SnapshotName` parametro o l'ultima istantanea trovata per l'istanza o il cluster di database Amazon RDS selezionato.

> **Note**
>
> Se non specifichi un valore per il `KMSKey` parametro, l'automazione crea una nuova chiave gestita AWS KMS dal cliente nell'account che viene utilizzata per crittografare lo snapshot.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AccountIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Elenco separato da virgole di ID account con cui condividere l'istantanea.
- AutomationAssumeRole

  -Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Database

  - Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dell'istanza o del cluster di Amazon RDS DB di cui desideri condividere lo snapshot. Questo parametro è facoltativo se si specifica un valore per il `SnapshotName` parametro.

- KMSKey

  - Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) completo della chiave gestita dal AWS KMS cliente utilizzata per crittografare lo snapshot.

- SnapshotName

  - Tipo: stringa

  Descrizione: (Facoltativo) L'ID del cluster DB o dello snapshot dell'istanza che desideri utilizzare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

Sono `AutomationAssumeRole` necessarie le seguenti azioni per avviare correttamente il runbook per un cluster DB.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`

- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

Il ruolo IAM utilizzato per eseguire l'automazione deve essere aggiunto come utente chiave per utilizzare la chiave KMS specificata nel ARNKmsKey parametro. Per informazioni sull'aggiunta di utenti chiave a una chiave KMS, consulta Changing a key policy nella AWS Key Management Service Developer Guide.

Sono AutomationAssumeRole necessarie le seguenti azioni aggiuntive per avviare correttamente il runbook se non si specifica un valore per il KMSKey parametro.

- kms:CreateKey
- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

Fasi del documento

1. aws:executeScript- Verifica se è stato fornito un valore per il KMSKey parametro e crea una chiave gestita AWS KMS dal cliente se non viene trovato alcun valore.
2. aws:branch- Verifica se è stato fornito un valore per il SnapshotName parametro e si ramifica di conseguenza.
3. aws:executeAwsApi- Verifica se l'istantanea fornita proviene da un'istanza DB.
4. aws:executeScript- Formatta il SnapshotName parametro sostituendo i due punti con un trattino.
5. aws:executeAwsApi- Copia l'istantanea utilizzando il codice specificato. KMSKey
6. aws:waitForAwsResourceProperty- Attende il completamento dell'operazione di copia dell'istantanea.
7. aws:executeAwsApi- Condivide la nuova istantanea con quella specificata. AccountIds
8. aws:executeAwsApi- Verifica se l'istantanea fornita proviene da un cluster DB.
9. aws:executeScript- Formatta il SnapshotName parametro sostituendo i due punti con un trattino.
10. aws:executeAwsApi- Copia l'istantanea utilizzando il codice specificato. KMSKey

11. `aws:waitForAwsResourceProperty`- Attende il completamento dell'operazione di copia dell'istantanea.
12. `aws:executeAwsApi`- Condivide la nuova istantanea con quella specificata. `AccountIds`
13. `aws:executeAwsApi`- Verifica se il valore fornito per il `Database` parametro è un'istanza DB.
14. `aws:executeAwsApi`- Verifica se il valore fornito per il `Database` parametro è un cluster DB.
15. `aws:executeAwsApi`- Recupera un elenco di istantanee per quanto specificato. `Database`
16. `aws:executeScript`- Determina l'ultima istantanea disponibile dall'elenco assemblato nel passaggio precedente.
17. `aws:executeAwsApi`- Copia lo snapshot dell'istanza DB utilizzando il codice specificato. `KMSKey`
18. `aws:waitForAwsResourceProperty`- Attende il completamento dell'operazione di copia dell'istantanea.
19. `aws:executeAwsApi`- Condivide la nuova istantanea con quella specificata. `AccountIds`
20. `aws:executeAwsApi`- Recupera un elenco di istantanee per quanto specificato. `Database`
21. `aws:executeScript`- Determina l'ultima istantanea disponibile dall'elenco assemblato nel passaggio precedente.
22. `aws:executeAwsApi`- Copia lo snapshot dell'istanza DB utilizzando il codice specificato. `KMSKey`
23. `aws:waitForAwsResourceProperty`- Attende il completamento dell'operazione di copia dell'istantanea.
24. `aws:executeAwsApi`- Condivide la nuova istantanea con quella specificata. `AccountIds`
25. `aws:executeScript`- Elimina la chiave gestita dal AWS KMS cliente creata dall'automazione se non è stato specificato un valore per il `KMSKey` parametro e l'automazione fallisce.

AWS-StartRdsInstance

Descrizione

Avvia un'istanza di Amazon Relational Database Service (RDSAmazon).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: stringa

  Descrizione: (obbligatorio) ID dell'RDSistanza Amazon da avviare.

`AWS-StartStopAuroraCluster`

Descrizione

Questo runbook avvia o arresta un cluster Amazon Aurora.

> **Note**
>
> Per avviare un cluster, è necessario che sia in uno `stopped` stato. Per arrestare un cluster, è necessario che sia in uno `available` stato. Questo runbook non può essere utilizzato per avviare o arrestare un cluster Aurora Serverless, un cluster Aurora multimaster, parte di un database globale Aurora o un cluster che utilizza la query parallela Aurora.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- ClusterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del cluster Aurora che desideri arrestare o avviare.
- Azione

  Tipo: stringa

  Valori validi: Start | Stop

  Predefinito: Start

  Descrizione: (Obbligatorio) Il nome del cluster Aurora che desideri arrestare o avviare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `rds:DescribeDBClusters`

- `rds:StartDBCluster`
- `rds:StopDBCluster`

Fasi del documento

- `aws:executeScript`- Avvia o arresta il cluster in base ai valori specificati per.

Output

StartStopAuroraCluster. ClusterName - Il nome del cluster Aurora

StartStopAuroraCluster. CurrentStatus - Lo stato attuale del cluster Aurora

StartStopAuroraCluster.Message - Dettagli dell'automazione

AWS-StopRdsInstance

Descrizione

Arresta un'istanza di Amazon Relational Database Service (RDSAmazon).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: stringa

  Descrizione: (obbligatorio) ID dell'RDSistanza Amazon da interrompere.

AWSSupport-TroubleshootConnectivityToRDS

Descrizione

Il `AWSSupport-TroubleshootConnectivityToRDS` runbook diagnostica i problemi di connettività tra un'EC2istanza e un'istanza di Amazon Relational Database Service. L'automazione garantisce la disponibilità dell'istanza DB, quindi verifica le regole dei gruppi di sicurezza associati, gli elenchi di controllo degli accessi alla rete (reteACLs) e le tabelle di routing per potenziali problemi di connettività.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentifier

  Tipo: stringa

  Descrizione: (obbligatorio) ID istanza DB su cui testare la connettività.

- SourceInstance

  Tipo: stringa

  Modello consentito: ^i-[a-z0-9] {8,17}$

  Descrizione: (Obbligatorio) L'ID dell'EC2istanza da cui testare la connettività.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'istanza DB è`available`.
- `aws:executeAwsApi`- Ottiene informazioni sull'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulla rete di istanze DBACLs.
- `aws:executeAwsApi`- Ottiene la sottorete CIDR dell'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sull'EC2istanza.

- `aws:executeAwsApi`- Ottiene informazioni sulla rete dell'EC2istanzaACLs.
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati all'EC2istanza.
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati all'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulle tabelle di routing associate all'EC2istanza.
- `aws:executeAwsApi`- Ottiene informazioni sulla tabella di routing principale associata ad Amazon VPC per l'EC2istanza.
- `aws:executeAwsApi`- Ottiene informazioni sulle tabelle di routing associate all'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulla tabella di routing principale associata ad Amazon VPC per l'istanza DB.
- `aws:executeScript`- Valuta le regole del gruppo di sicurezza.
- `aws:executeScript`- Valuta la rete. ACLs
- `aws:executeScript`- Valuta le tabelle dei percorsi.
- `aws:sleep`- Termina l'automazione.

Output

getRDSInstanceProprietà. DBInstanceIdentifier- L'istanza DB utilizzata nell'automazione.

getRDSInstanceProprietà. DBInstanceStatus- Lo stato attuale diDBInstance.

evalSecurityGroupRegole. SecurityGroupEvaluation - Risultati del confronto delle regole del gruppo `SourceInstance` di sicurezza con le regole del gruppo di sicurezza dell'istanza DB.

evalNetworkAclRegole. NetworkAclEvaluation - Risultati del confronto tra la `SourceInstance` rete e ACLs la rete di istanze DBACLs.

evalRouteTableVoci. RouteTableEvaluation - Risultati del confronto della tabella delle `SourceInstance` rotte con le rotte delle istanze DB.

AWSSupport-TroubleshootRDSIAMAuthentication

Descrizione

`AWSSupport-TroubleshootRDSIAMAuthentication`Aiuta a risolvere i problemi di autenticazione AWS Identity and Access Management (IAM) per le istanze Amazon RDS for PostgreSQL, Amazon for MySQL, RDS Amazon RDS for MariaDB, Amazon Aurora Postgre e Amazon Aurora SQL My. SQL Usa questo runbook per verificare la configurazione richiesta per

l'IAMautenticazione con un'RDSistanza Amazon o un cluster Aurora. Fornisce inoltre passaggi per correggere i problemi di connettività RDS ad Amazon Instance o Aurora Cluster.

> **Important**
>
> Questo runbook non supporta Amazon RDS per Oracle o Amazon RDS per Microsoft SQL Server.

> **Important**
>
> Se viene fornita un'EC2istanza Amazon di origine e il database di destinazione è AmazonRDS, `AWSSupport-TroubleshootConnectivityToRDS` viene richiamata un'automazione secondaria per risolvere i problemi di connettivitàTCP. L'output fornisce anche comandi che puoi eseguire sull'EC2istanza Amazon o sul computer di origine per connetterti alle RDS istanze Amazon utilizzando IAM l'autenticazione.

Come funziona?

Questo runbook è composto da sei passaggi:

- Fase 1validateInputs: Convalida gli input dell'automazione.
- Passaggio 2 branchOnSourceEC2Provided: verifica se nei parametri di input viene fornito un ID Amazon EC2 Instance di origine.
- Fase 3validateRDSConnectivity: convalida la RDS connettività Amazon dall'EC2istanza Amazon di origine, se fornita.
- Fase 4validateRDSIAMAuthentication: Verifica se la funzionalità di IAM autenticazione è abilitata.
- Fase 5validateIAMPolicies: Verifica se le IAM autorizzazioni richieste sono presenti nell'utente/ruolo fornito. IAM
- Fase 6generateReport: Genera un rapporto dei risultati dei passaggi eseguiti in precedenza.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- RDSType

  Tipo: stringa

  Descrizione: (obbligatorio): seleziona il tipo di database relazionale a cui stai tentando di connetterti e autenticarti.

  Valori consentiti: o `Amazon RDS` `Amazon Aurora Cluster.`
- DBInstanceIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore dell'istanza di RDS database Amazon o del cluster di database Aurora di destinazione.

  Modello consentito: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  Numero massimo di caratteri: 63
- SourceEc2 InstanceIdentifier

  Tipo: `AWS::EC2::Instance::Id`

  Descrizione: (Facoltativo) L'ID Amazon EC2 Instance se ti connetti all'istanza di RDS database Amazon da un'EC2istanza Amazon in esecuzione nello stesso account e nella stessa regione. Non

specificare questo parametro se l'origine non è un'EC2istanza Amazon o se il RDS tipo di Amazon di destinazione è un cluster di database Aurora.

Impostazione predefinita: ""

- DBIAMRoleName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del IAM ruolo utilizzato per l'autenticazione IAM basata. Fornisci solo se il parametro non `DBIAMUserName` viene fornito, altrimenti lascialo vuoto. `DBIAMRoleName`O `DBIAMUserName` deve essere fornito.

  Modello consentito: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Numero massimo di caratteri: 64

  Impostazione predefinita: ""

- DBIAMUserName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome IAM utente utilizzato per l'autenticazione IAM basata. Fornisci solo se il `DBIAMRoleName` parametro non viene fornito, altrimenti lascialo vuoto. `DBIAMRoleName`O `DBIAMUserName` deve essere fornito.

  Modello consentito: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Numero massimo di caratteri: 64

  Impostazione predefinita: ""

- DBUserName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome utente del database mappato a un IAM ruolo/utente per l'autenticazione IAM basata all'interno del database. L'opzione predefinita `*` valuta se l'`rds-db:connect`autorizzazione è consentita a tutti gli utenti del database.

  Modello consentito: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Numero massimo di caratteri: 64

Impostazione predefinita: *

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `iam:GetPolicy`
- `iam:GetRole`
- `iam:GetUser`
- `iam:ListAttachedRolePolicies`
- `iam:ListAttachedUserPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`
- `iam:SimulatePrincipalPolicy`
- `rds:DescribeDBClusters`
- `rds:DescribeDBInstances`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

Istruzioni

1. Passa a AWSSupport-T roubleshootRDSIAMAuthentication nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole(Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- RDSType(Obbligatorio):

  Seleziona il tipo di Amazon RDS a cui stai tentando di connetterti e autenticarti. Scegli tra i due valori consentiti: oppure `Amazon RDS` `Amazon Aurora Cluster.`

- DBInstanceIdentifier(Obbligatorio):

  Inserisci l'identificatore dell'istanza di RDS database Amazon di destinazione o del cluster Aurora a cui stai tentando di connetterti e IAM utilizza le credenziali per l'autenticazione.

- SourceEc2 InstanceIdentifier (Opzionale):

  Fornisci l'ID Amazon EC2 Instance se ti connetti all'istanza di RDS database Amazon da un'EC2istanza Amazon presente nello stesso account e nella stessa regione. Lascia vuoto se l'origine non è Amazon EC2 o se il RDS tipo di Amazon di destinazione è un cluster Aurora.

- DBIAMRoleName(Facoltativo):

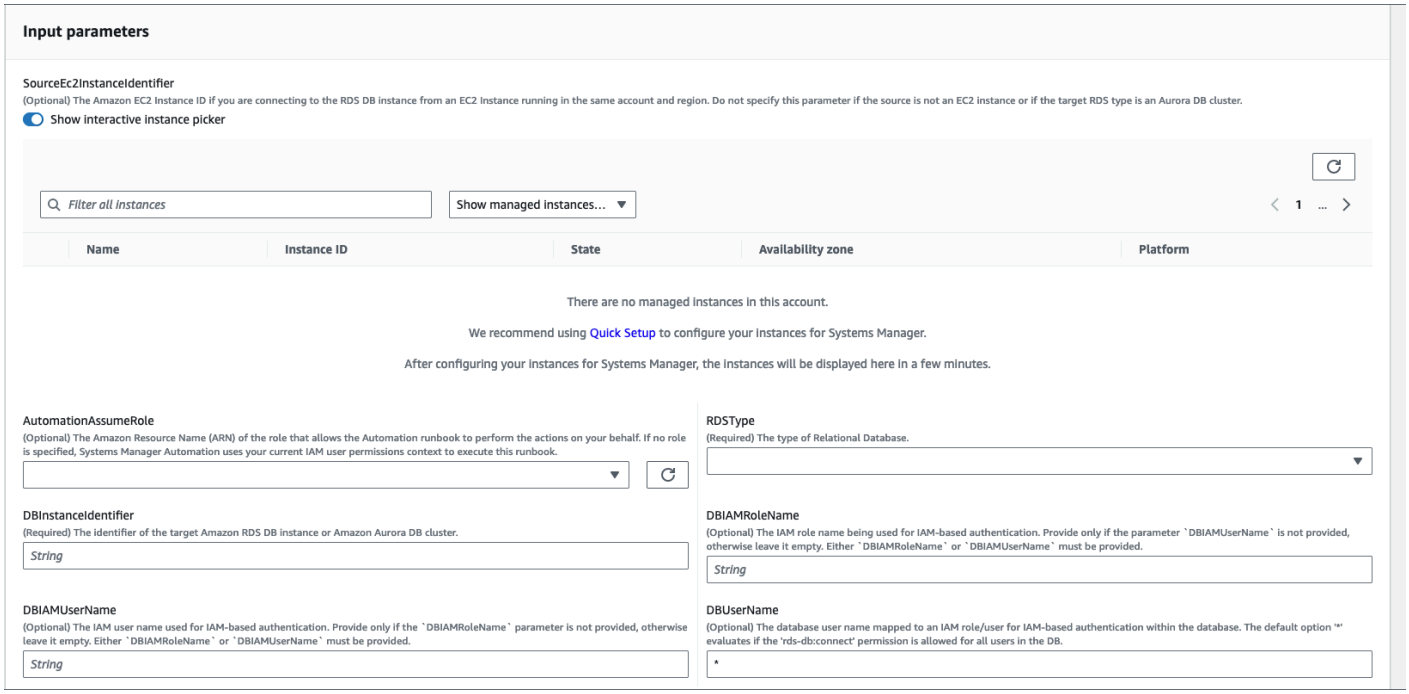
  Immettere il nome del IAM ruolo utilizzato per l'autenticazione IAM basata. Fornisci solo se non `DBIAMUserName` viene fornito; in caso contrario, lascia vuoto il campo. Fornito `DBIAMRoleName` o `DBIAMUserName` deve essere fornito.

- DBIAMUserName(Facoltativo):

  Immettere l'IAMutente utilizzato per l'autenticazione IAM basata. Fornire solo se non `DBIAMRoleName` viene fornito, altrimenti lasciare vuoto. Fornito `DBIAMRoleName` o `DBIAMUserName` deve essere fornito.

- DBUserName(Facoltativo):

  Immettere l'utente del database mappato a un IAM ruolo/utente per l'autenticazione IAM basata sul database. L'opzione predefinita `*` viene utilizzata per la valutazione; non viene fornito nulla in questo campo.



4. Seleziona Esegui.
5. Notate che l'automazione si avvia.
6. Il documento esegue le seguenti operazioni:
   - Fase 1validateInputs:

     Convalida gli input dell'automazione - `SourceEC2InstanceIdentifier` (opzionale), `DBInstanceIdentifier` or`ClusterID`, and `DBIAMRoleName` or. `DBIAMUserName` Verifica se i parametri di input inseriti sono presenti nel tuo account e nella tua regione. Verifica inoltre se l'utente ha inserito uno dei IAM parametri (ad esempio, `DBIAMRoleName` o`DBIAMUserName`). Inoltre, esegue altre verifiche, ad esempio se il database menzionato è nello stato Disponibile.
   - Fase 2: branchOnSource EC2Provided

     Verifica se nei parametri di input EC2 viene fornito Source Amazon e se il database è AmazonRDS. In caso affermativo, si procede alla fase 3. In caso contrario, salta il passaggio 3, che è la convalida di Amazon EC2 -Amazon RDS Connectivity, e procede al passaggio 4.
   - Fase 3: validateRDSConnectivity

     Se l'Amazon di origine EC2 viene fornito nei parametri di input e il database è AmazonRDS, la fase 2 avvia la fase 3. In questa fase, `AWSSupport-TroubleshootConnectivityToRDS` viene richiamata l'automazione secondaria per convalidare la RDS connettività Amazon dall'origine Amazon. EC2 Il runbook di automazione secondario `AWSSupport-`

`TroubleshootConnectivityToRDS` verifica se le configurazioni di rete richieste (Amazon Virtual Private Cloud [AmazonVPC], Security Groups, Network Access Control List []NACL, Amazon RDS availability) sono presenti in modo da consentirti di connetterti dall'EC2istanza Amazon all'istanza Amazon. RDS

- Fase 4: validateRDSIAMAuthentication

  Verifica se la funzionalità di IAM autenticazione è abilitata sull'RDSistanza Amazon o sul cluster Aurora.

- Fase 5: validateIAMPolicies

  Verifica se le IAM autorizzazioni richieste sono presenti nell'IAMutente/ruolo passato per consentire alle IAM credenziali di autenticarsi nell'RDSistanza Amazon per l'utente del database specificato (se presente).

- Fase 6: generateReport

  Ottiene tutte le informazioni dei passaggi precedenti e stampa il risultato o l'output di ogni passaggio. Elenca inoltre i passaggi a cui fare riferimento ed eseguire per connettersi all'RDSistanza Amazon utilizzando le IAM credenziali.

7. Una volta completata l'automazione, consulta la sezione Output per i risultati dettagliati:
   - Verifica dell'autorizzazione dell'IAMutente/ruolo per la connessione al database:

     Verifica se le IAM autorizzazioni richieste sono presenti nell'IAMutente/ruolo passato per consentire alle IAM credenziali di autenticarsi nell'RDSistanza Amazon per l'utente del database specificato (se presente).

   - Verifica dell'attributo di autenticazione IAM basato sul database:

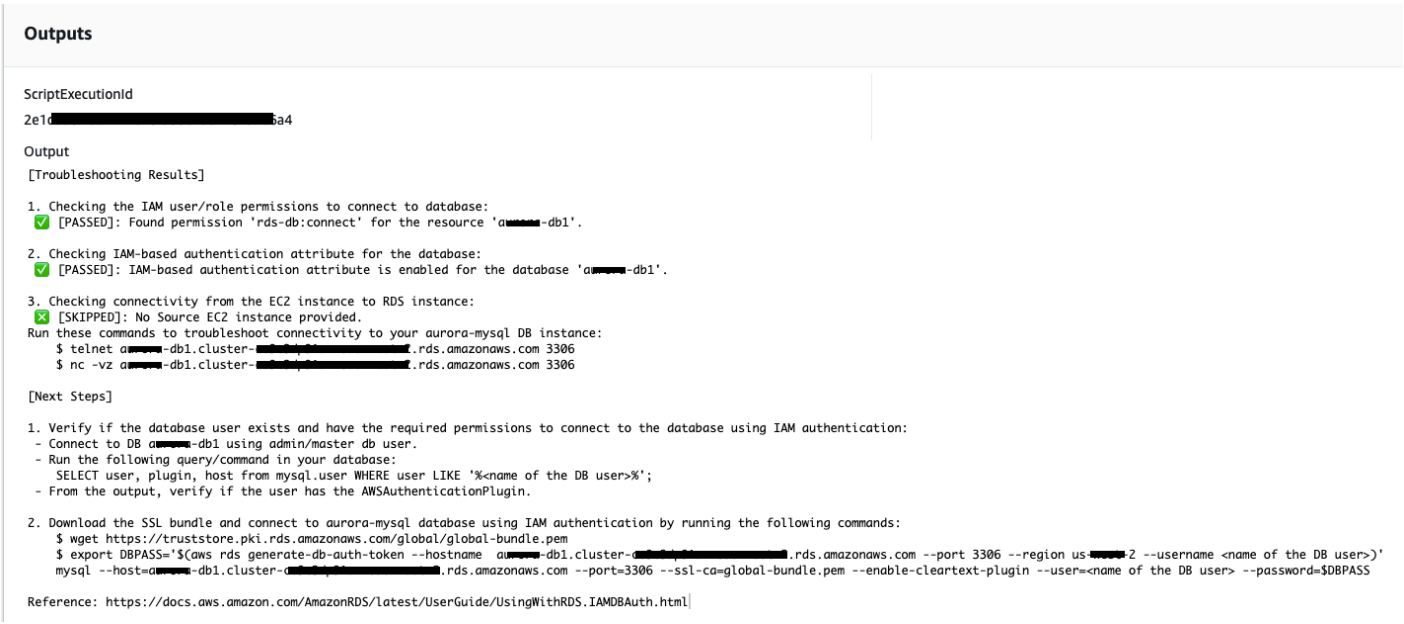
     Verifica se la funzionalità di IAM autenticazione è abilitata per il cluster Amazon RDS Database/ Aurora specificato.

   - Verifica della connettività da Amazon EC2 Instance ad Amazon RDS Instance:

     Verifica se le configurazioni di rete richieste (AmazonVPC, Security Groups, NACL Amazon RDS availability) sono presenti in modo da poterti connettere dall'EC2istanza Amazon all'istanza AmazonRDS.

   - Fasi successive:

     Elenca i comandi e i passaggi a cui fare riferimento ed eseguire per connettersi all'RDSistanza Amazon utilizzando le IAM credenziali.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWSSupport-ValidateRdsNetworkConfiguration

Descrizione

`AWSSupport-ValidateRdsNetworkConfiguration`l'automazione aiuta a evitare lo stato di incompatibilità della rete per l'istanza esistente di Amazon Relational Database Service (AmazonRDS) /Amazon Aurora/Amazon DocumentDB prima dell'esecuzione o dell'operazione. `ModifyDBInstance` `StartDBInstance` Se l'istanza è già in uno stato di rete incompatibile, il runbook ne fornirà il motivo.

Come funziona?

Questo runbook determina se l'istanza del RDS database Amazon entrerà in uno stato di rete incompatibile o, in caso affermativo, determina il motivo per cui si trova in uno stato di rete incompatibile.

Il runbook esegue i seguenti controlli sulla tua istanza di RDS database Amazon:

- Quota Amazon Elastic Network Interface (ENI) per regione.
- Esistono tutte le sottoreti del database Subnet Group.
- Sono disponibili un numero sufficiente di indirizzi IP gratuiti per le sottoreti.
- (Per le RDS istanze Amazon accessibili pubblicamente) Impostazioni degli VPC attributi (`enableDnsSupporteenableDnsHostnames`).

> **Important**
>
> Quando utilizzi questo documento su cluster Amazon Aurora/Amazon DocumentDB, assicurati di utilizzare invece di. `DBInstanceIdentifier` `ClusterIdentifier` In caso contrario, il documento fallirà nel primo passaggio.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`

- `ec2:DescribeSubnets`

Politica di esempio:

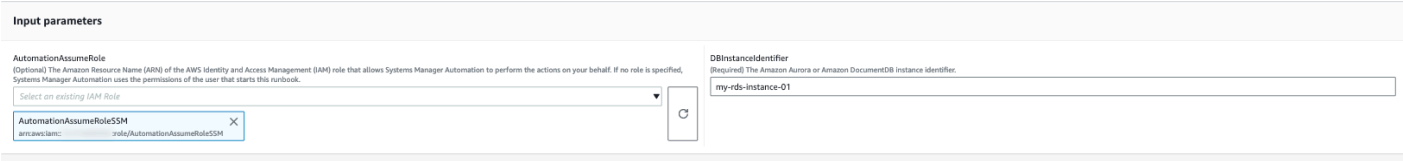
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateRdsNetwork",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "servicequotas:GetServiceQuota",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
            ]
        }
    ]
}
```

Istruzioni

1. Accedere al AWSSupportpulsante - ValidateRdsNetworkConfiguration nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole(Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - DBInstanceIdentifier(Obbligatorio):

Inserisci l'identificatore dell'istanza di Amazon Relational Database Service.



4. Seleziona Esegui.
5. Nota che l'automazione si avvia.
6. Il documento esegue le seguenti operazioni:
   - Fase 1 assertRdsState:

     Verifica se l'identificatore di istanza fornito esiste e presenta uno dei seguenti stati: `availablestopped`, `oincompatible-network`.
   - Fase 2: gatherRdsInformation

     Raccoglie le informazioni necessarie sull'RDSistanza Amazon da utilizzare successivamente nell'automazione.
   - Fase 3: checkEniQuota

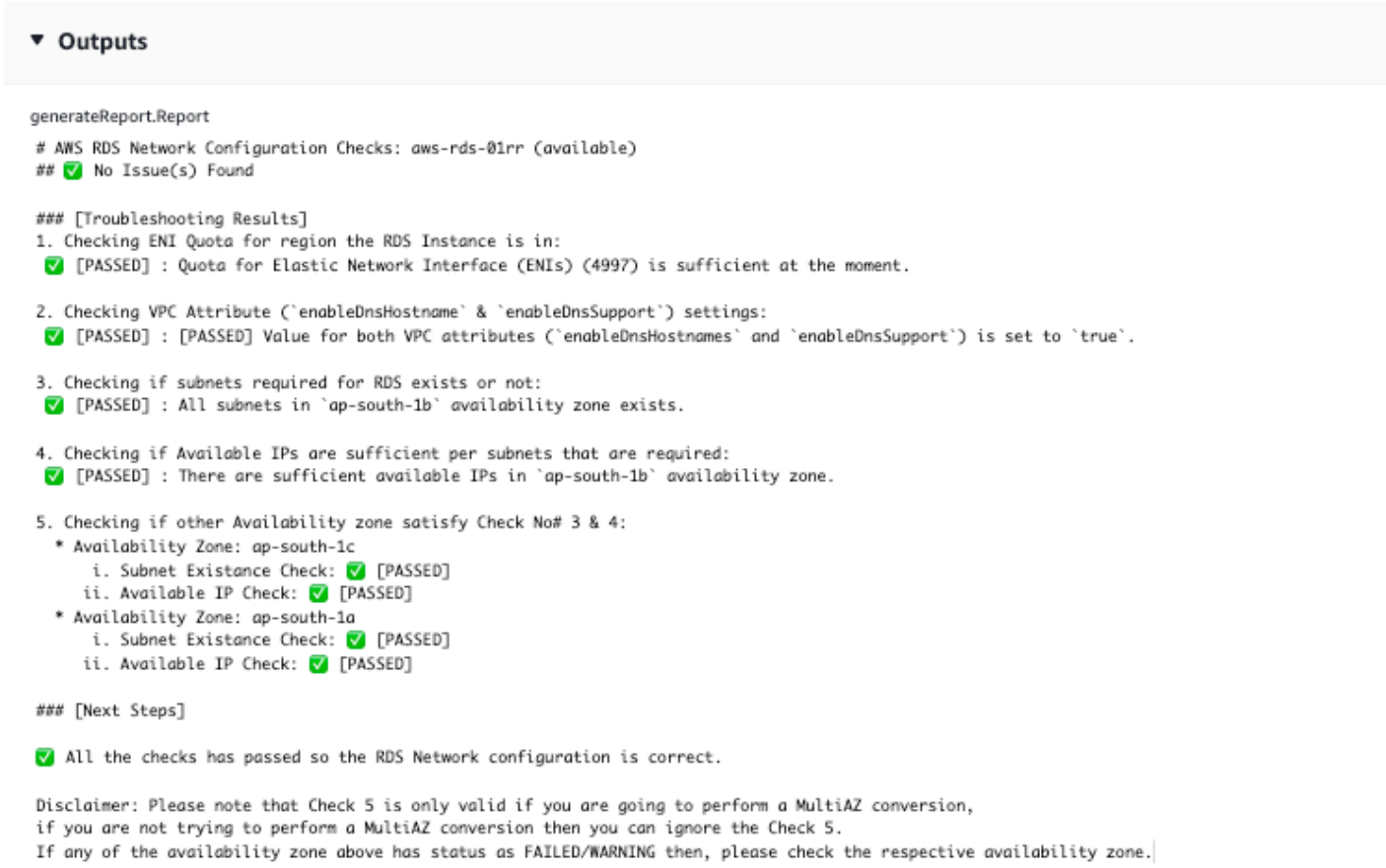
     Verifica la quota attualmente disponibile di Amazon ENI per la regione.
   - Fase 4 validateVpcAttributes:

     Verifica che i DNS parametri (`enableDnsSupporteenableDnsHostnames`) di Amazon VPC siano impostati su true (o meno se l'RDSistanza Amazon lo è`PubliclyAccessible`).
   - Fase 5: validateSubnetAttributes

     Convalida l'esistenza di sottoreti in `DBSubnetGroup` e verifica se sono disponibili IPs per ogni sottorete.
   - Fase 6: generateReport

     Ottiene tutte le informazioni dei passaggi precedenti e stampa il risultato o l'output di ogni passaggio. Elenca inoltre i passaggi a cui fare riferimento ed eseguire per connettersi all'RDSistanza Amazon utilizzando le IAM credenziali.
7. Una volta completata l'automazione, consulta la sezione Output per i risultati dettagliati:

RDSIstanza Amazon con configurazione di rete valida:



RDSIstanza Amazon con configurazione di rete errata (VPCl'attributo enableDnsHostnames è impostato su false):

Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Come posso risolvere i problemi con un RDS database Amazon che si trova in uno stato di rete incompatibile?
- Come posso risolvere i problemi con un'istanza di Amazon DocumentDB che si trova in uno stato di rete incompatibile?

Amazon Redshift

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Redshift. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWSConfigRemediation-DeleteRedshiftCluster`

Descrizione

Il `AWSConfigRemediation-DeleteRedshiftCluster` runbook elimina il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del cluster Amazon Redshift che desideri eliminare.
- SkipFinalClusterSnapshot

  Tipo: Booleano

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se impostata su`false`, l'automazione crea uno snapshot prima di eliminare il cluster Amazon Redshift. Se impostato su`true`, non viene creata una snapshot finale del cluster.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Fasi del documento

- `aws:branch`- Rami basati sul valore specificato per il `SkipFinalClusterSnapshot` parametro.
- `aws:executeAwsApi`- Elimina il cluster Amazon Redshift specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Verifica che il cluster Amazon Redshift sia stato eliminato.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descrizione

Il `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` runbook disabilita l'accessibilità pubblica per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster per cui desideri disabilitare l'accessibilità pubblica.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Disattiva l'accessibilità pubblica per il cluster specificato nel parametro. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cluster cambi a. `available`
- `aws:assertAwsResourceProperty`- Conferma che l'impostazione di accessibilità pubblica è disabilitata nel cluster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` runbook consente la registrazione di audit per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui desideri caricare i log.

- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare la registrazione di controllo.

- S3 KeyPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso chiave di Amazon S3 (sottocartella) in cui desideri caricare i log.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Fasi del documento

- `aws:branch`- Rami in base al fatto che sia stato specificato un valore per il `S3KeyPrefix` parametro.
- `aws:executeAwsApi`- Abilita la registrazione di controllo sul cluster specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la registrazione di controllo sia stata abilitata sul cluster.

`AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot`

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` runbook abilita istantanee automatizzate per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- AutomatedSnapshotRetentionPeriod

Tipo: integer

Valori validi: 1-35

Descrizione: (Obbligatorio) Il numero di giorni in cui vengono conservate le istantanee automatiche.

- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui si desidera abilitare le istantanee automatiche.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Abilita le istantanee di automazione sul cluster specificato nel `ClusterIdentifier` parametro.
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cluster cambi in. `available`
- `aws:executeScript`- Conferma che le istantanee automatiche sono state abilitate nel cluster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook abilita la crittografia sul cluster Amazon Redshift specificato utilizzando AWS Key Management Service una chiave AWS KMS() gestita dal cliente. Questo runbook deve essere usato solo come base per garantire

che i cluster Amazon Redshift siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più cluster con diverse chiavi gestite dal cliente. Questo runbook non può modificare la chiave gestita AWS KMS dal cliente utilizzata su un cluster già crittografato. Per modificare la chiave gestita AWS KMS dal cliente utilizzata per crittografare un cluster, è necessario innanzitutto disabilitare la crittografia sul cluster.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare la crittografia.
- KMSKeyARN

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare i dati del cluster.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia sul cluster Amazon Redshift specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata sul cluster.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` runbook consente il routing avanzato del cloud privato virtuale (VPC) per il cluster Amazon Redshift specificato. Per informazioni sul VPC routing avanzato, consulta Amazon Redshift VPC Enhanced Routing nella Amazon Redshift Management Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare il VPC routing avanzato.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Abilita il VPC routing avanzato sul cluster specificato nel `ClusterIdentifier` parametro.
- `assertAwsResourceProperty`- Conferma che il VPC routing avanzato è stato abilitato sul cluster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descrizione

Il `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` runbook richiede connessioni in entrata da utilizzare SSL per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare il VPC routing avanzato.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli dei parametri dal cluster specificato nel `ClusterIdentifier` parametro.
- `aws:executeAwsApi`- Abilita l'`require_ssl`impostazione sul cluster specificata nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Conferma che l'`require_ssl`impostazione è stata abilitata sul cluster.
- `aws:executeScript`- Verifica l'`require_ssl`impostazione per il cluster.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Descrizione

Il `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` runbook modifica le impostazioni di manutenzione per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AllowVersionUpgrade

  Tipo: Booleano

  Descrizione: (Obbligatorio) Se impostato su`true`, gli aggiornamenti delle versioni principali vengono applicati automaticamente al cluster durante la finestra di manutenzione.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- AutomatedSnapshotRetentionPeriod

  Tipo: integer

  Valori validi: 1-35

  Descrizione: (Obbligatorio) Il numero di giorni in cui vengono conservate le istantanee automatiche.
- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui si desidera abilitare il routing avanzatoVPC.
- PreferredMaintenanceWindow

  Tipo: stringa

  Descrizione: (Obbligatorio) L'intervallo di tempo settimanale (inUTC) durante il quale può essere effettuata la manutenzione del sistema.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Modifica le impostazioni di manutenzione per il cluster specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Conferma che le impostazioni di manutenzione modificate sono state configurate per il cluster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descrizione

Il `AWSConfigRemediation-ModifyRedshiftClusterNodeType` runbook modifica il tipo di nodo e il numero di nodi per il cluster Amazon Redshift specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Classic

  Tipo: Booleano

  Descrizione: (Facoltativo) Se impostato `sutrue`, l'operazione di ridimensionamento utilizza il processo di ridimensionamento classico.

- ClusterIdentifier

  Tipo: stringa

  Descrizione: (Obbligatorio) L'identificatore univoco del cluster di cui si desidera modificare il tipo di nodo.

- ClusterType

  Tipo: stringa

  Valori validi: nodo singolo | nodo multiplo

  Descrizione: (Obbligatorio) Il tipo di cluster che desideri assegnare al cluster.

- NodeType

  Tipo: stringa

  Valori validi: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  Descrizione: (Obbligatorio) Il tipo di nodo che desideri assegnare al cluster.

- NumberOfNodes

  Tipo: integer

  Valori validi: 2-100

  Descrizione: (Facoltativo) Il numero di nodi che desideri assegnare al cluster. Se il cluster è `single-node` di un tipo, non specificare un valore per questo parametro.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Fasi del documento

- `aws:executeScript`- Modifica il tipo di nodo e il numero di nodi per il cluster specificato nel `ClusterIdentifier` parametro.

Amazon S3

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Storage Service. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWS-ArchiveS3BucketToIntelligentTiering`

Descrizione

Il `AWS-ArchiveS3BucketToIntelligentTiering` runbook crea o sostituisce una configurazione di tiering intelligente per il bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 per cui desideri creare una configurazione di tiering intelligente.
- ConfigurationId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID per la configurazione di tiering intelligente. Può essere un nuovo ID di configurazione o l'ID di una configurazione esistente.
- NumberOfDaysToArchive

Tipo: stringa

Valori validi: 90-730

Descrizione: (Obbligatorio) Il numero di giorni consecutivi dopo che un oggetto nel bucket è idoneo alla transizione al livello Archive Access.

- NumberOfDaysToDeepArchive

  Tipo: stringa

  Valori validi: 180-730

  Descrizione: (Obbligatorio) Il numero di giorni consecutivi dopo che un oggetto nel bucket è idoneo alla transizione al livello Deep Archive Access.

- S3Prefix

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti a cui si desidera applicare la configurazione.

- Tag

  Tipo: MapList

  Descrizione: (Facoltativo) Metadati assegnati agli oggetti a cui si desidera applicare la configurazione. I tag sono costituiti da una chiave e da un valore definiti dall'utente.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Fasi del documento

- PutsBucketIntelligentTieringConfiguration (aws:executeScript) - Crea o aggiorna una configurazione Amazon S3 Intelligent-Tiering per il bucket specificato.
- VerifyBucketIntelligentTieringConfiguration(aws: assertAwsResource Property) - Verifica che la configurazione intelligente di S3 Bucket sia stata applicata al bucket specificato.

AWS-ConfigureS3BucketLogging

Descrizione

Abilita la registrazione su un bucket Amazon Simple Storage Service (Amazon S3).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 per il quale desideri configurare la registrazione.
- GrantedPermission

Tipo: stringa

Valori validi: _ | | FULL CONTROL READ WRITE

Descrizione: (obbligatorio) autorizzazioni di registrazione assegnate all'assegnatario per il bucket.

- GranteeEmailAddress

  Tipo: stringa

  (Facoltativo) Indirizzo e-mail dell'assegnatario.

- GranteeId

  Tipo: stringa

  Descrizione: (facoltativo) ID utente canonico ID dell'assegnatario.

- GranteeType

  Tipo: stringa

  Valori validi: CanonicalUser | AmazonCustomerByEmail | Gruppo

  Descrizione: (obbligatorio) Tipo di assegnatario.

- GranteeUri

  Tipo: stringa

  Descrizione: (Facoltativa) URI del gruppo beneficiario.

- TargetBucket

  Tipo: stringa

  Descrizione: (Obbligatorio) specifica il bucket in cui desideri che Amazon S3 memorizzi i log di accesso al server. È possibile impostare la distribuzione dei log a qualsiasi bucket di proprietà dell'utente. È anche possibile configurare più bucket in modo che distribuiscano i propri log allo stesso bucket di destinazione. In questo caso è necessario sceglierne uno diverso TargetPrefix per ogni bucket di origine in modo che i file di log forniti possano essere distinti per chiave.

- TargetPrefix

  Tipo: stringa

Impostazione predefinita: /

Descrizione: (facoltativo) specifica un prefisso per le chiavi in base alle quali i file di log verranno archiviati.

AWS-ConfigureS3BucketVersioning

Descrizione

Configura il controllo delle versioni per un bucket Amazon Simple Storage Service (Amazon S3).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 per cui desideri configurare il controllo delle versioni.

- VersioningState

  Tipo: stringa

  Valori validi: Abilitato | Sospeso

  Impostazione predefinita: Enabled

  Descrizione: (Facoltativo) Applicato all' VersioningConfiguration.Status. Se impostato su "Enabled", questo processo abilita la funzione Versioni multiple per gli oggetti nel bucket; a tutti gli oggetti aggiunti al bucket viene assegnato un ID versione univoco. Se impostato su`Suspended`, questo processo disabilita il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID della versione. `null`

`AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock`

Descrizione

Il `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` runbook configura le impostazioni dei blocchi di accesso pubblico di Amazon Simple Storage Service (Amazon S3) per un bucket Amazon S3 in base ai valori specificati nei parametri del runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BlockPublicAcls

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 blocca gli elenchi di controllo degli accessi pubblici (ACLs) per il bucket S3 e gli oggetti archiviati nel bucket S3 specificato nel parametro. `BucketName`

- BlockPublicPolicy

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 blocca le policy dei bucket pubblici per il bucket S3 specificato nel parametro. `BucketName`

- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 che desideri configurare.

- IgnorePublicAcls

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 ignora tutto il pubblico ACLs per il bucket S3 specificato nel parametro. `BucketName`

- RestrictPublicBuckets

  Tipo: Booleano

  Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 limita le politiche dei bucket pubblici per il bucket S3 specificato nel parametro. `BucketName`

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Fasi del documento

- `aws:executeAwsApi`- Crea o modifica la `PublicAccessBlock` configurazione per il bucket S3 specificato nel parametro. `BucketName`
- `aws:executeScript`- Restituisce la `PublicAccessBlock` configurazione per il bucket S3 specificato nel `BucketName` parametro e verifica che le modifiche siano state apportate correttamente in base ai valori specificati nei parametri del runbook.

AWSConfigRemediation-ConfigureS3PublicAccessBlock

Descrizione

Il `AWSConfigRemediation-ConfigureS3PublicAccessBlock` runbook configura le impostazioni dei blocchi di accesso pubblico Account AWS Amazon Simple Storage Service (Amazon S3) di accesso pubblico in base ai valori specificati nei parametri del runbook.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AccountId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del proprietario del bucket S3 Account AWS che stai configurando.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BlockPublicAcls

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 blocca gli elenchi di controllo degli accessi pubblici (ACLs) per i bucket S3 di proprietà dell' Account AWS utente specificato nel parametro. `AccountId`
- BlockPublicPolicy

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 blocca le policy dei bucket pubblici per i bucket S3 di proprietà del destinatario Account AWS specificato nel parametro. `AccountId`
- IgnorePublicAcls

  Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 ignora tutti i bucket S3 pubblici ACLs di proprietà del tipo Account AWS specificato nel parametro. `AccountId`

- RestrictPublicBuckets

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Se impostato su`true`, Amazon S3 limita le politiche dei bucket pubblici per i bucket S3 di proprietà del destinatario specificato nel Account AWS parametro. `AccountId`

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Fasi del documento

- `aws:executeAwsApi`- Crea o modifica la `PublicAccessBlock` configurazione per Account AWS quanto specificato nel `AccountId` parametro.
- `aws:executeScript`- Restituisce la `PublicAccessBlock` configurazione per il valore Account AWS specificato nel `AccountId` parametro e verifica che le modifiche siano state apportate correttamente in base ai valori specificati nei parametri del runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descrizione

Il `AWS-CreateS3PolicyToExpireMultipartUploads` runbook crea una politica del ciclo di vita per un bucket specifico che fa scadere i caricamenti incompleti in più parti in corso dopo un

determinato numero di giorni. Questo runbook unisce la nuova politica del ciclo di vita a tutte le policy relative ai bucket del ciclo di vita esistenti già esistenti.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 che desideri configurare.
- DaysUntilExpire

  Tipo: integer

  Descrizione: (Obbligatorio) Il numero di giorni di attesa di Amazon S3 prima di rimuovere definitivamente tutte le parti del caricamento.
- RuleId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID utilizzato per identificare la regola del bucket del ciclo di vita. Questo deve essere un valore univoco.

- S3Prefix

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti a cui si desidera applicare la configurazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Fasi del documento

- ConfigureExpireMultipartUploads (aws:executeScript) - Configura la politica del ciclo di vita per il bucket.
- VerifyExpireMultipartUploads (aws:executeScript) - Verifica che la politica del ciclo di vita sia stata configurata per il bucket.

Output

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

Descrizione

Usa Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon `Block Public Access` S3) per disabilitare l'accesso in lettura e scrittura per un bucket S3 pubblico. Per ulteriori informazioni, consulta Using Amazon S3 Block Public Access nella Guida per l'utente di Amazon Simple Storage Service.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- S3 BucketName

  Tipo: stringa

  Descrizione: (obbligatoria) bucket S3 in cui si desidera limitare l'accesso.

AWS-EnableS3BucketEncryption

Descrizione

Configura la crittografia predefinita per un bucket Amazon Simple Storage Service (Amazon S3).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (obbligatoria) nome del bucket S3 in cui si desidera crittografare i contenuti.
- SSEAlgorithm

  Tipo: stringa

  Impostazione predefinita: AES256

  Descrizione: (facoltativo) algoritmo di crittografia lato server da utilizzare per la crittografia predefinita.

AWS-EnableS3BucketKeys

Descrizione

Il `AWS-EnableS3BucketKeys` runbook abilita Bucket Keys sul bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Questa chiave a livello di bucket crea chiavi dati per

nuovi oggetti durante il suo ciclo di vita. Se non specifichi un valore per il `KmsKeyId` parametro, la crittografia lato server con chiavi gestite di Amazon S3 SSE (-S3) viene utilizzata per la configurazione di crittografia predefinita.

> **Note**
>
> Le chiavi Bucket di Amazon S3 non sono supportate per la crittografia lato server a doppio livello con AWS Key Management Service () chiavi (-).AWS KMS DSSE KMS

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 per il quale desideri abilitare Bucket Keys.
- KMSKeyId

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN), l'ID della chiave o l'alias chiave della chiave gestita dal cliente AWS Key Management Service (AWS KMS) che desideri utilizzare per la crittografia lato server.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Fasi del documento

- ChooseEncryptionType (aws:branch) - Valuta il valore fornito per il `KmsKeyId` parametro per determinare se verranno utilizzati SSE -S3 (AES256) o -. SSE KMS
- PutBucketKeysKMS(aws:executeAwsApi) - Imposta la `BucketKeyEnabled` proprietà su `true` per il bucket S3 specificato utilizzando lo specificato. `KmsKeyId`
- PutBucketKeysAES256(aws:executeAwsApi) - Imposta la `BucketKeyEnabled` proprietà su `true` per il bucket S3 specificato con crittografia. AES256
- verifyS3 BucketKeysEnabled (aws: assertAwsResource Property): verifica che le Bucket Keys siano abilitate sul bucket S3 di destinazione.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Descrizione

Il `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` runbook rimuove le principali dichiarazioni di policy che contengono caratteri speciali (`Principal: *`o`Principal: "AWS": *`) per `Allow` le azioni dalla tua policy sui bucket di Amazon Simple Storage Service (Amazon S3). Vengono inoltre rimosse le dichiarazioni politiche con condizioni.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 di cui desideri modificare la politica.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Fasi del documento

- `aws:executeScript`- Modifica la policy del bucket e verifica che le principali dichiarazioni politiche con caratteri jolly siano state rimosse dal bucket Amazon S3 specificato nel parametro. `BucketName`

`AWSConfigRemediation-RestrictBucketSSLRequestsOnly`

Descrizione

Il `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` runbook crea una dichiarazione sulla policy del bucket Amazon Simple Storage Service (Amazon S3) che nega esplicitamente le richieste HTTP al bucket Amazon S3 specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 a cui desideri HTTP rifiutare le richieste.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Fasi del documento

- `aws:executeScript`- Crea una policy sui bucket per il bucket S3 specificato nel `BucketName` parametro che nega esplicitamente le richieste. HTTP

`AWSSupport-TroubleshootS3PublicRead`

Descrizione

Il `AWSSupport-TroubleshootS3PublicRead` runbook diagnostica i problemi di lettura degli oggetti dal bucket pubblico Amazon Simple Storage Service (Amazon S3) specificato nel parametro. `S3BucketName` Un sottoinsieme di impostazioni viene inoltre analizzato per gli oggetti nel bucket S3.

Esegui questa automazione (console)

Limitazioni

- Questa automazione non verifica i punti di accesso che consentono l'accesso pubblico agli oggetti.
- Questa automazione non valuta le chiavi delle condizioni nella policy del bucket S3.
- Se utilizzi AWS Organizations, questa automazione non valuta le politiche di controllo del servizio per confermare che l'accesso ad Amazon S3 è consentito.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- CloudWatchLogGroupName

  Tipo: stringa

  Descrizione: (Facoltativo) Il gruppo di log di Amazon CloudWatch Logs a cui desideri inviare l'output di automazione. Se non viene trovato un gruppo di log che corrisponde al valore specificato, l'automazione creerà un gruppo di log utilizzando questo valore di parametro. Il periodo di conservazione per il gruppo di log creato da questa automazione è di 14 giorni.
- CloudWatchLogStreamName

  Tipo: stringa

  Descrizione: (Facoltativo) Il flusso di log di CloudWatch Logs a cui si desidera inviare l'output dell'automazione. Se non viene trovato un flusso di log che corrisponde al valore specificato, l'automazione creerà un flusso di log utilizzando questo valore di parametro. Se non si specifica un valore per questo parametro, l'automazione utilizzerà il `ExecutionId` come nome del flusso di log.
- HttpGet

  Tipo: Booleano

  Valori validi: true | false

Impostazione predefinita: true

Descrizione: (Facoltativo) Se questo parametro è impostato su`true`, l'automazione invia una HTTP richiesta parziale agli oggetti nel `S3BucketName` campo specificato. Solo il primo byte dell'oggetto viene restituito utilizzando l'HTTPintestazione Range.

- IgnoreBlockPublicAccess

  Tipo: Booleano

  Valori validi: true | false

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Se questo parametro è impostato su`true`, l'automazione ignora le impostazioni del blocco di accesso pubblico del bucket S3 specificato nel parametro. `S3BucketName` Non è consigliabile modificare questo parametro rispetto al valore predefinito.

- MaxObjects

  Tipo: integer

  Valori validi: 1-25

  Impostazione predefinita: 5

  Descrizione: (Facoltativo) Il numero di oggetti da analizzare nel bucket S3 specificato nel parametro. `S3BucketName`

- S3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del bucket S3 da risolvere.

- S3 PrefixName

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti che desideri analizzare nel tuo bucket S3. Per ulteriori informazioni, consulta Object keys nella Amazon Simple Storage Service User Guide.

- StartAfter

Tipo: stringa

Descrizione: (Facoltativo) Il nome della chiave dell'oggetto su cui desideri che l'automazione inizi ad analizzare gli oggetti nel tuo bucket S3.

- ResourcePartition

  Tipo: stringa

  Valori validi: `aws` | `aws-us-gov` | `aws-cn`

  Impostazione predefinita: `aws`

  Descrizione: (Obbligatoria) La partizione in cui si trova il bucket S3.

- Modalità dettagliata

  Tipo: Booleano

  Valori validi: true | false

  Impostazione predefinita: false

  Descrizione: (Facoltativo) Per restituire informazioni più dettagliate durante l'automazione, imposta questo parametro su. `true` Se il parametro è impostato su, verranno restituiti solo i messaggi di avviso e di error`false`.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Le `logs:PutLogEvents` autorizzazioni `logs:CreateLogGrouplogs:CreateLogStream`, e sono necessarie solo se si desidera che l'automazione invii i dati di registro a Logs. CloudWatch

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:SimulateCustomPolicy",
                "iam:GetContextKeysForCustomPolicy",
```

```
                "s3:ListAllMyBuckets",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy",
                "s3:GetAccountPublicAccessBlock"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
            "Effect": "Allow"
        }
    ]
}
```

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma l'esistenza e l'accessibilità del bucket S3.
- `aws:executeScript`- Restituisce la posizione del bucket S3 e il tuo ID utente canonico.
- `aws:executeScript`- Restituisce le impostazioni del blocco di accesso pubblico per il tuo account e il bucket S3.

- `aws:assertAwsResourceProperty`- Conferma che il bucket payer S3 è impostato su. `BucketOwner` Se `Requester Pays` è abilitato sul bucket S3, l'automazione termina.
- `aws:executeScript`- Restituisce lo stato della policy del bucket S3 e determina se è considerata pubblica. Per ulteriori informazioni sui bucket S3 pubblici, consulta Il significato di «pubblico» nella Guida per l'utente di Amazon Simple Storage Service.
- `aws:executeAwsApi`- Restituisce la policy sui bucket S3.
- `aws:executeAwsApi`- Restituisce tutte le chiavi di contesto presenti nella policy del bucket S3.
- `aws:assertAwsResourceProperty`- Conferma se esiste una negazione esplicita dell'azione nella policy del bucket S3. `GetObject` API
- `aws:executeAwsApi`- Restituisce l'elenco di controllo degli accessi (ACL) per il bucket S3.
- `aws:executeScript`- Crea un gruppo di log CloudWatch Logs e un flusso di log se si specifica un valore per il parametro. `CloudWatchLogGroupName`
- `aws:executeScript`- In base ai valori specificati nei parametri di input del runbook, valuta se alcune delle impostazioni del bucket S3 raccolte durante l'automazione impediscono l'accesso agli oggetti da parte del pubblico. Questo script esegue le seguenti funzioni:
  - Valuta le impostazioni dei blocchi di accesso pubblico
  - Restituisce gli oggetti dal bucket S3 in base ai valori specificati nei parametri `MaxObjects`S3PrefixName, e. `StartAfter`
  - Restituisce la policy del bucket S3 per simulare una IAM politica personalizzata per gli oggetti restituiti dal bucket S3.
  - Esegue una HTTP richiesta parziale agli oggetti restituiti se il parametro è impostato su. `HttpGet` `true` Solo il primo byte dell'oggetto viene restituito utilizzando l'HTTPintestazione Range.
  - Controlla il nome della chiave dell'oggetto restituito per confermare se termina con uno o due punti. I nomi delle chiavi degli oggetti che terminano in periodi non possono essere scaricati dalla console Amazon S3.
  - Verifica se il proprietario dell'oggetto restituito corrisponde al proprietario del bucket S3.
  - Verifica se le ACL concessioni `READ` o le `FULL_CONTROL` autorizzazioni dell'oggetto agli utenti anonimi.
  - Restituisce i tag associati all'oggetto.
  - Utilizza la IAM policy simulata per confermare se esiste una negazione esplicita per questo oggetto nella policy del bucket S3 per l'azione. `GetObject` API
  - Restituisce i metadati dell'oggetto per confermare che la classe di archiviazione è supportata.

- Verifica le impostazioni di crittografia lato server dell'oggetto per confermare se l'oggetto è crittografato utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente.

Output

AnalyzeObjects.bucket

AnalyzeObjects.oggetto

SageMaker

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. SageMaker Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-DisableSageMakerNotebookRootAccess

`AWS-DisableSageMakerNotebookRootAccess`

Descrizione

Il `AWS-DisableSageMakerNotebookRootAccess` runbook disabilita l'accesso root su un'istanza di SageMaker notebook Amazon. Durante l'automazione, l'istanza del notebook viene interrotta per apportare le modifiche richieste. SageMaker Le istanze di notebook Studio non sono supportate.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- NotebookInstanceName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome dell'istanza del SageMaker notebook su cui disabilitare l'accesso root.
- StartInstanceAfterUpdate

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Facoltativo) Determina se l'istanza del notebook viene avviata dopo aver disabilitato l'accesso root. L'impostazione predefinita per questo parametro è`true`. Se impostato su`true`, l'istanza viene avviata dopo la disabilitazione dell'accesso root. Se impostato su`false`, l'istanza viene lasciata nello `stopped` stato dopo la disabilitazione dell'accesso root.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Fasi del documento

- CheckNotebookInstanceStatus (aws:executeAwsApi): Verifica lo stato corrente dell'istanza del notebook.
- StopOrUpdateNotebookInstance (aws:branch): rami basati sullo stato dell'istanza del notebook.
- StopNotebookInstance (aws:executeAwsApi): avvia l'istanza se lo stato è. `stopped`
- WaitForInstanceToStop (aws: waitForAwsResourceProperty): Verifica che l'istanza sia`stopped`.
- UpdateNotebookInstance (aws:executeAwsApi): disabilita l'accesso root sull'istanza del notebook.
- WaitForNotebookUpdate (aws: waitForAwsResourceProperty): verifica che l'accesso root sia stato disabilitato e che l'istanza abbia uno `stopped` stato.
- ChooseInstanceStart (aws:branch): Branch in base al fatto che l'istanza debba essere avviata.
- StartNotebookInstance (aws:executeAwsApi): avvia l'istanza del notebook.
- VerifyNotebookInstanceStatus (aws: waitForAwsResourceProperty): Verifica se l'istanza è `available` prima di disabilitare l'accesso root.
- VerifyNotebookInstanceRootAccess (aws: assertAwsResource Property): verifica che l'impostazione di accesso root dell'istanza del notebook sia disabilitata correttamente.

Secrets Manager

AWS Systems Manager Automation fornisce runbook predefiniti per. AWS Secrets Manager Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

`AWSConfigRemediation-DeleteSecret`

Descrizione

Il `AWSConfigRemediation-DeleteSecret` runbook elimina un segreto e tutte le versioni memorizzate in. AWS Secrets Manager Facoltativamente, è possibile specificare la finestra di ripristino durante la quale è possibile ripristinare il segreto. Se non si specifica un valore per il `RecoveryWindowInDays` parametro, l'operazione ha come valore predefinito 30 giorni.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- RecoveryWindowInDays

  Tipo: integer

  Valori validi: 7-30

  Impostazione predefinita: 30

  Descrizione: (Facoltativo) Il numero di giorni in cui è possibile ripristinare il segreto.
- SecretId

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) del segreto che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

Fasi del documento

- `aws:executeAwsApi`- Elimina il segreto specificato nel parametro. `SecretId`
- `aws:executeScript`- Verifica che il segreto sia stato pianificato per l'eliminazione.

`AWSConfigRemediation-RotateSecret`

Descrizione

Il `AWSConfigRemediation-RotateSecret` runbook ruota un segreto memorizzato in. AWS Secrets Manager

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- RotationInterval

  Tipo: Intervallo

  Valori validi: 1-365

  Descrizione: (Obbligatorio) Il numero di giorni tra le rotazioni del segreto.

- RotationLambdaArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) della AWS Lambda funzione che può ruotare il segreto.

- SecretId

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) del segreto che desideri ruotare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Fasi del documento

- `aws:executeAwsApi`- Ruota il segreto specificato nel `SecretId` parametro.
- `aws:executeScript`- Verifica che la rotazione sia stata abilitata sul segreto.

Security Hub

AWS Systems Manager Automation fornisce runbook predefiniti per. AWS Security Hub Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

Descrizione

Il `AWSConfigRemediation-EnableSecurityHub` runbook abilita AWS Security Hub (Security Hub) per Account AWS e Regione AWS dove si esegue l'automazione. Per informazioni su Security Hub, vedi Cos'è AWS Security Hub? nella Guida AWS Security Hub per l'utente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EnableDefaultStandards

  Tipo: Booleano

  Impostazione predefinita: true

  Descrizione: (Obbligatorio) Se impostato su`true`, sono abilitati gli standard di sicurezza predefiniti designati da Security Hub.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Abilita Security Hub nell'account e nella regione correnti.
- `aws:executeAwsApi`- Verifica che Security Hub sia stato abilitato.

AWS Shield

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Shield Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSPremiumSupport-DDoSResiliencyAssessment

`AWSPremiumSupport-DDoSResiliencyAssessment`

Descrizione

Il `AWSPremiumSupport-DDoSResiliencyAssessment` runbook di AWS Systems Manager automazione consente di verificare DDoS le vulnerabilità e la configurazione delle risorse in base alla protezione prevista per l' AWS Shield Advanced utente. Account AWS Fornisce un rapporto sulle impostazioni di configurazione per le risorse vulnerabili agli attacchi Distributed Denial of Service ()DDoS. Viene utilizzato per raccogliere, analizzare e valutare le seguenti risorse: Amazon Route 53, Amazon Load Balancers, CloudFront distribuzioni Amazon AWS Global Accelerator ed AWS Elastic IPs per le relative impostazioni di configurazione in conformità con le migliori pratiche consigliate per la protezione. AWS Shield Advanced Il report di configurazione finale è disponibile in un bucket Amazon S3 a tua scelta come file. HTML

Come funziona?

Questo runbook contiene una serie di controlli relativi ai vari tipi di risorse abilitate all'accesso pubblico e alla presenza di protezioni configurate secondo le raccomandazioni contenute nel white paper sulle AWS DDoSmigliori pratiche. Il runbook esegue le seguenti operazioni:

- Verifica se AWS Shield Advanced è abilitato un abbonamento a.
- Se abilitato, rileva se ci sono risorse protette Shield Advanced.
- Trova tutte le risorse globali e regionali Account AWS e verifica se queste sono protette dallo Shield.
- Richiede i parametri del tipo di risorsa per la valutazione, il nome del bucket Amazon S3 e l'ID del Account AWS bucket Amazon S3 (S3). BucketOwner
- Restituisce i risultati sotto forma di HTML report archiviato nel bucket Amazon S3 fornito.

I parametri di input `AssessmentType` decidono se verranno eseguiti i controlli su tutte le risorse. Per impostazione predefinita, il runbook verifica la presenza di tutti i tipi di risorse. Se è selezionato solo il `RegionalResources` parametro `GlobalResources` or, il runbook esegue i controlli solo sui tipi di risorse selezionati.

> **Important**
>
> - L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, consulta Confronta AWS Support i piani.
> - Questo runbook richiede un `ACTIVE` AWS Shield Advanced abbonamento.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- AssessmentType

  Tipo: stringa

  Descrizione: (Facoltativo) Determina il tipo di risorse da valutare per la valutazione della resilienza. DDoS Per impostazione predefinita, il runbook valuterà sia le risorse globali che quelle regionali. Per le risorse regionali, il runbook descrive tutti i sistemi di bilanciamento del carico Application (ALBNLB) e Network (), nonché tutto il gruppo Auto Scaling presente in /region. Account AWS

  Valori validi: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  Impostazione predefinita: risorse globali e regionali
- S3 BucketName

  Tipo: `AWS::S3::Bucket::Name`

  Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 in cui verrà caricato il report.

  Modello consentito: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  Tipo: stringa

  Descrizione: (Facoltativo) Il Account AWS proprietario del bucket Amazon S3. Specificate questo parametro se il bucket Amazon S3 appartiene a un altro bucket Account AWS, altrimenti potete lasciare questo parametro vuoto.

  Pattern consentito: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  Tipo: `AWS::IAM::Role::Arn`

  Descrizione: (Facoltativo) Il ARN IAM ruolo con le autorizzazioni per descrivere il bucket Amazon S3 Account AWS e bloccare la configurazione dell'accesso pubblico se il bucket si trova in un altro. Account AWS Se questo parametro non è specificato, il runbook utilizza l'utente `AutomationAssumeRole` o l'IAMutente che avvia questo runbook (se non è specificato). `AutomationAssumeRole` Consulta la sezione sulle autorizzazioni richieste nella descrizione del runbook.

  Modello consentito: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) Il prefisso per il percorso all'interno di Amazon S3 per l'archiviazione dei risultati.

  Modello consentito: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:DescribeAutoScalingGroups`
- `cloudfront:ListDistributions`
- `ec2:DescribeAddresses`

- ec2:DescribeNetworkAcls
- ec2:DescribeInstances
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- globalaccelerator:ListAccelerators
- iam:GetRole
- iam:ListAttachedRolePolicies
- route53:ListHostedZones
- route53:GetHealthCheck
- shield:ListProtections
- shield:GetSubscriptionState
- shield:DescribeSubscription
- shield:DescribeEmergencyContactSettings
- shield:DescribeDRTAccess
- waf:GetWebACL
- waf:GetRateBasedRule
- wafv2:GetWebACL
- wafv2:GetWebACLForResource
- waf-regional:GetWebACLForResource
- waf-regional:GetWebACL
- s3:ListBucket
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketEncryption
- s3:GetAccountPublicAccessBlock
- s3:PutObject

Esempio IAM di policy per l'Automation Assume Role

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetAccountPublicAccessBlock"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetBucketLocation",
                    "s3:GetBucketPublicAccessBlock",
                    "s3:GetBucketPolicyStatus",
                    "s3:GetEncryptionConfiguration"
                ],
                "Resource": "arn:aws:s3:::<bucket-name>",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "s3:PutObject"
                ],
                "Resource": "arn:aws:s3:::<bucket-name>/*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "autoscaling:DescribeAutoScalingGroups",
                    "cloudfront:ListDistributions",
                    "ec2:DescribeInstances",
                    "ec2:DescribeAddresses",
                    "ec2:DescribeNetworkAcls",
                    "elasticloadbalancing:DescribeLoadBalancers",
                    "elasticloadbalancing:DescribeTargetGroups",
                    "globalaccelerator:ListAccelerators",
```

```
                                "iam:GetRole",
                                "iam:ListAttachedRolePolicies",
                                "route53:ListHostedZones",
                                "route53:GetHealthCheck",
                                "shield:ListProtections",
                                "shield:GetSubscriptionState",
                                "shield:DescribeSubscription",
                                "shield:DescribeEmergencyContactSettings",
                                "shield:DescribeDRTAccess",
                                "waf:GetWebACL",
                                "waf:GetRateBasedRule",
                                "wafv2:GetWebACL",
                                "wafv2:GetWebACLForResource",
                                "waf-regional:GetWebACLForResource",
                                "waf-regional:GetWebACL"
                            ],
                            "Resource": "*",
                            "Effect": "Allow"
                        },
                        {
                            "Action": "iam:PassRole",
                            "Resource": "arn:aws:iam::123456789012:role/
<AutomationAssumeRole-Name>",
                            "Effect": "Allow"
                        }
                    ]
                }
```

Istruzioni

1. Accedere al AWSPremiumSupportpulsante - DDoSResiliencyAssessment nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole(Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AssessmentType(Facoltativo):

  Determina il tipo di risorse da valutare per la valutazione DDoS della resilienza. Per impostazione predefinita, il runbook valuta sia le risorse globali che quelle regionali.

- S3 BucketName (richiesto):

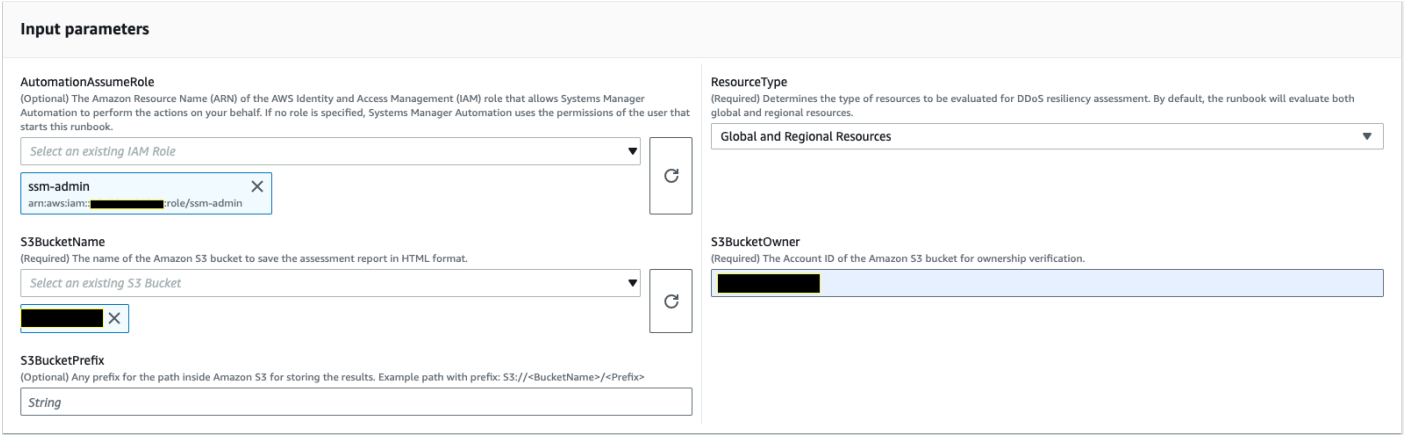
  Il nome del bucket Amazon S3 per salvare il report di valutazione in formato. HTML

- S3 BucketOwner (opzionale):

  L' Account AWS ID del bucket Amazon S3 per la verifica della proprietà. L' Account AWS ID è obbligatorio se il report deve essere pubblicato su un bucket Amazon S3 con più account e facoltativo se il bucket Amazon S3 è nella stessa fase di avvio dell'automazione. Account AWS

- S3 (opzionale): BucketPrefix

  Qualsiasi prefisso per il percorso all'interno di Amazon S3 per l'archiviazione dei risultati.



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:

   - CheckShieldAdvancedState:

     Verifica se il bucket Amazon S3 specificato in «S3BucketName» consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura, se il bucket ha la crittografia a riposo abilitata e se l' Account AWS ID fornito in «S3BucketOwner" è il proprietario del bucket Amazon S3.

   - S3: BucketSecurityChecks

Verifica se il bucket Amazon S3 specificato in «S3BucketName» consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura, se il bucket ha la crittografia a riposo abilitata e se l' Account AWS ID fornito in «S3BucketOwner" è il proprietario del bucket Amazon S3.

- BranchOnShieldAdvancedStatus:

  Le filiali documentano i passaggi in base allo stato dell' AWS Shield Advanced abbonamento e/o allo stato di proprietà del bucket Amazon S3.

- ShieldAdvancedConfigurationReview:

  Esamina le configurazioni Shield Advanced per garantire che siano presenti i dettagli minimi richiesti. Ad esempio: IAM Access for AWS Shield Response Team (SRT) Team, Contact List Details e SRT Proactive Engagement Status.

- ListShieldAdvancedProtections:

  Elenca le Shield Protected Resources e crea un gruppo di risorse protette per ogni servizio.

- BranchOnResourceTypeAndCount:

  I rami documentano i passaggi in base al valore del parametro Resource Type e al numero di risorse globali protette da Shield.

- ReviewGlobalResources:

  Esamina le risorse globali protette di Shield Advanced come Route 53 Hosted Zones, CloudFront Distributions e Global Accelerators.

- BranchOnResourceType:

  Le filiali documentano i passaggi in base alle selezioni del tipo di risorsa, se globale, regionale o entrambi.

- ReviewRegionalResources:

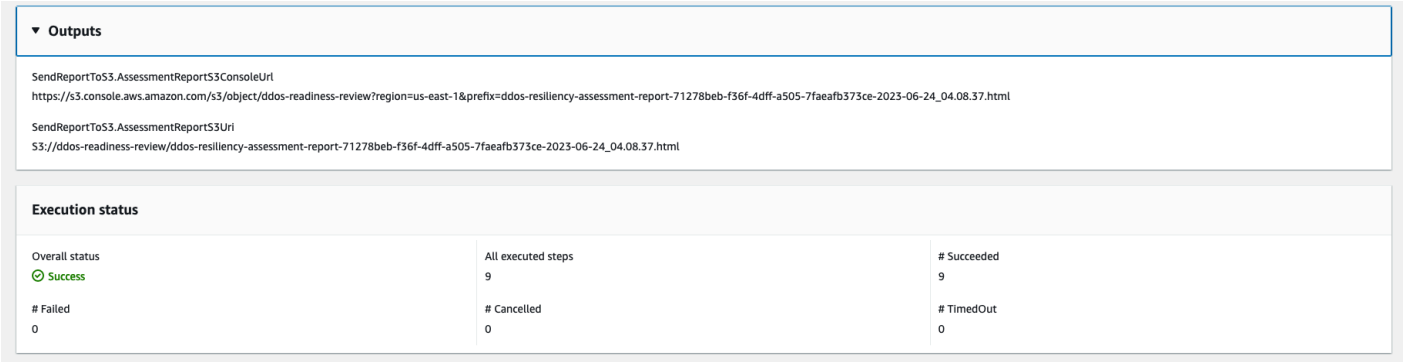
  Esamina le risorse regionali protette di Shield Advanced come Application Load Balancer, Network Load Balancers, Classic Load Balancer, Amazon Elastic Compute Cloud (Amazon) Instances (Elastic). EC2 IPs

- SendReportToS3:

  Carica i dettagli del rapporto di DDoS valutazione nel bucket Amazon S3.

7. Una volta completato, URI il HTML file del report di valutazione viene fornito nel bucket Amazon S3:

S3 Console link e Amazon URI S3 per il report sull'esecuzione riuscita del runbook



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Notification Service. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

AWS-EnableSNSTopicDeliveryStatusLogging

Descrizione

Il AWS-EnableSNSTopicDeliveryStatusLogging runbook configura la registrazione dello stato di consegna per un endpoint HTTP Amazon Data Firehose, Lambda Platform application o Amazon Simple Queue Service (Amazon). SQS Ciò consente SNS ad Amazon di registrare gli avvisi non riusciti e una percentuale campione di notifiche di avviso riuscite su Amazon CloudWatch. Se la registrazione dello stato della consegna è già configurata per l'argomento, il runbook sostituisce la configurazione esistente con i nuovi valori specificati per i parametri di input.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- EndpointType

  Tipo: stringa

  Valori validi:
  - HTTP
  - Firehose

- Lambda
- Applicazione
- SQS

Descrizione: (Obbligatorio) Il tipo di endpoint SNS tematico Amazon per cui desideri registrare i messaggi di notifica dello stato di consegna.

- TopicArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARNSNSargomento Amazon per cui desideri configurare la registrazione dello stato della spedizione.

- SuccessFeedbackRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN IAM ruolo SNS utilizzato da Amazon per inviare i log per i messaggi di notifica riusciti. CloudWatch

- SuccessFeedbackSampleRate

  Tipo: stringa

  Valori validi: 0-100

  Descrizione: (Obbligatorio) La percentuale di messaggi riusciti da campionare per l'SNSargomento Amazon specificato.

- FailureFeedbackRoleArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN IAM ruolo a cui Amazon SNS invia i log per i messaggi di notifica degli errori. CloudWatch

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Fasi del documento

- `aws:executeAwsApi`- Applica il valore del `SuccessFeedbackRoleArn` parametro all'SNSargomento Amazon.
- `aws:executeAwsApi`- Applica il valore del `SuccessFeedbackSampleRate` parametro all'SNSargomento Amazon.
- `aws:executeAwsApi`- Applica il valore del `FailureFeedbackRoleArn` parametro all'SNSargomento Amazon.
- `aws:executeScript`- Conferma che la registrazione dello stato della spedizione è abilitata sull'SNSargomento Amazon.

Output

VerifyDeliveryStatusLoggingEnabled. GetTopicAttributesResponse - Risposta delle `GetTopicAttributes` API operazioni.

VerifyDeliveryStatusLoggingEnabled. VerifyDeliveryStatusLoggingEnabled - Messaggio che indica l'avvenuta verifica della registrazione dello stato di consegna.

`AWSConfigRemediation-EncryptSNSTopic`

Descrizione

Il `AWSConfigRemediation-EncryptSNSTopic` runbook abilita la crittografia sull'argomento Amazon Simple Notification Service (AmazonSNS) specificato utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente. Questo runbook deve essere usato solo come base per garantire che i tuoi SNS argomenti Amazon siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Ti consigliamo di crittografare più argomenti con diverse chiavi gestite dal cliente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- KmsKeyArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome della risorsa Amazon (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare l'SNSargomento Amazon.
- TopicArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARNSNSargomento Amazon che desideri crittografare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Fasi del documento

- `aws:executeAwsApi`- Crittografa l'SNSargomento Amazon specificato nel `TopicArn` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la crittografia è abilitata sull'SNSargomento Amazon.

AWS-PublishSNSNotification

Descrizione

Pubblica una notifica su AmazonSNS.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Messaggio

  Tipo: stringa

  Descrizione: (Obbligatorio) Il messaggio da includere nella SNS notifica.

- TopicArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARNSNSargomento su cui pubblicare la notifica.

Amazon SQS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Queue Service (Amazon). SQS Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

Descrizione

Il `AWS-EnableSQSEncryption` runbook abilita la crittografia a riposo per una coda Amazon Simple Queue Service SQS (Amazon). Una SQS coda Amazon può essere crittografata con chiavi SQS gestite di Amazon (SSE-SQS) o con AWS Key Management Service (AWS KMS) chiavi gestite (SSE-KMS). La chiave che assegni alla coda deve avere una politica chiave che includa le autorizzazioni per tutti i principali che sono autorizzati a utilizzare la coda. Con la crittografia abilitata, le richieste anonime `SendMessage` e `ReceiveMessage` le richieste alla coda crittografata vengono rifiutate.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- QueueUrl

  Tipo: stringa

  Descrizione: (Obbligatorio) La URL SQS coda Amazon su cui desideri abilitare la crittografia.
- KmsKeyId

  Tipo: stringa

  Descrizione: (Facoltativo) La AWS KMS chiave da utilizzare per la crittografia. Questo valore può essere un identificatore univoco globale, un ARN alias o una chiave oppure un nome alias preceduto da «alias/». Puoi anche usare la chiave AWS gestita specificando l'alias aws/sqs.
- KmsDataKeyReusePeriodSeconds

  Tipo: stringa

  Valori validi: 60-86400

  Impostazione predefinita: 300

  Descrizione: (Facoltativo) Il periodo di tempo, in secondi, in cui una SQS coda Amazon può riutilizzare una chiave dati per crittografare o decrittografare i messaggi prima di effettuare una nuova chiamata. AWS KMS

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Fasi del documento

- SelectKeyType (`aws:branch`): rami basati sulla chiave specificata.
- PutAttributeSseKms (`aws:executeAwsApi`) - Aggiorna la SQS coda Amazon per utilizzare la AWS KMS chiave specificata per la crittografia.
- PutAttributeSseSqs (`aws:executeAwsApi`) - Aggiorna la SQS coda Amazon per utilizzare la chiave predefinita per la crittografia.
- VerifySqsEncryptionKms (`aws:assertAwsResourceProperty`) - Verifica che la crittografia sia abilitata nella SQS coda Amazon.
- VerifySqsEncryptionDefault (`aws:assertAwsResourceProperty`) - Verifica che la crittografia sia abilitata nella SQS coda Amazon.

Step Functions

AWS Systems Manager Automation fornisce runbook predefiniti per AWS Step Functions (Step Functions). Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-EnableStepFunctionsStateMachineLogging

`AWS-EnableStepFunctionsStateMachineLogging`

Descrizione

Il `AWS-EnableStepFunctionsStateMachineLogging` runbook abilita o aggiorna la registrazione sulla macchina a AWS Step Functions stati specificata. Il livello di registrazione minimo deve essere impostato su`ALL`, `ERROR` o. `FATAL`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Livello

  Tipo: stringa

  Valori validi: ALL | ERROR | FATAL

  Descrizione: (Obbligatorio) L'URL della coda Amazon SQS su cui desideri abilitare la crittografia.
- LogGroupArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN del gruppo di log Amazon CloudWatch Logs a cui desideri inviare i log della macchina a stati.
- StateMachineArn

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ARN della macchina a stati su cui si desidera abilitare l'accesso.
- IncludeExecutionData

  Tipo: Booleano

Impostazione predefinita: False

Descrizione: (Facoltativo) Determina se i dati di esecuzione sono inclusi nei log.

- TracingConfiguration

  Tipo: Booleano

  Impostazione predefinita: False

  Descrizione: (Facoltativo) Determina se la AWS X-Ray traccia è abilitata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Fasi del documento

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- Aggiorna la macchina a stati specificata con la configurazione di registrazione specificata.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- Verifica che la registrazione sia stata abilitata per la macchina a stati specificata.

Output

- EnableStepFunctionsStateMachineLogging.Response: risposta dalla chiamata API. UpdateStateMachine

Systems Manager

AWS Systems Manager Automation fornisce runbook predefiniti per Systems Manager. Per ulteriori informazioni sui runbook, vedere Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

`AWS-BulkDeleteAssociation`

Descrizione

Il `AWS-BulkDeleteAssociation` runbook consente di eliminare fino a 50 associazioni di Systems Manager State Manager alla volta.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- AssociationIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole IDs delle associazioni da eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DeleteAssociation`

Fasi del documento

- `aws:executeScript`- Elimina le associazioni specificate nel `AssociationIds` parametro.

AWS-BulkEditOpsItems

Descrizione

Il `AWS-BulkEditOpsItems` runbook consente di modificare lo stato, la gravità, la categoria o la priorità di AWS Systems Manager OpsItems. Questa automazione può modificarne un massimo di 50 OpsItems alla volta.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Categoria

  Tipo: stringa

  Valori validi:
  - Disponibilità
  - Costo
  - Nessuna modifica
  - Prestazioni
  - Ripristino
  - Sicurezza

  Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativo) La nuova categoria che desideri specificare per la modifica OpsItems.

- OpsItemIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole da OpsItems IDs modificare (ad esempio, oi-XXXXXXXXXXXX, oi-). XXXXXXXXXXXX

- Priority (Priorità)

  Tipo: stringa

  Valori validi:

  - Nessuna modifica
  - 1
  - 2
  - 3
  - 4
  - 5

  Impostazione predefinita: nessuna modifica

  Descrizione: (Facoltativo) L'importanza delle modifiche OpsItems rispetto agli altri OpsItems elementi del sistema.

- Gravità

  Tipo: stringa

  Valori validi:

  - Nessuna modifica
  - 1
  - 2
  - 3
  - 4

  Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativa) La gravità della modifica OpsItems.

- WaitTimeBetweenEditsInSecs

  Tipo: stringa

  Valori validi: 0.0-2.0

  Predefinito: 0.8

  Descrizione: (Facoltativo) Il tempo di attesa dell'automazione tra una chiamata all'operazione. `UpdateOpsItems`

- Stato

  Tipo: stringa

  Valori validi:

  - InProgress
  - Nessuna modifica
  - Aperta
  - Risolto

  Impostazione predefinita: nessuna modifica

  Descrizione: (Facoltativo) Il nuovo stato della modifica OpsItems.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Fasi del documento

- `aws:executeScript`- Modifica il valore OpsItems specificato nel `OpsItemIds` parametro in base ai valori specificati per i parametri`Category`, `PrioritySeverity`, `eStatus`.

AWS-BulkResolveOpsItems

Descrizione

Il `AWS-BulkResolveOpsItems` runbook risolve le risoluzioni AWS Systems Manager OpsItems che corrispondono al filtro specificato. È inoltre possibile specificare un elemento OpsItemId da aggiungere alla risoluzione OpsItems utilizzando il parametro. `OpsInsightsId` Se specifichi un valore per il `S3BucketName` parametro, viene inviato un riepilogo dei risultati al bucket Amazon Simple Storage Service (Amazon S3). Per ricevere una notifica dopo l'invio del riepilogo dei risultati al bucket Amazon S3, specifica un valore per il parametro. `SnsTopicArn` Questa automazione risolverà un massimo di 1.000 OpsItems alla volta.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Filtri

Tipo: stringa

Descrizione: (Obbligatorio) Le coppie di filtri chiave-valore da restituire. OpsItems Ad esempio, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Per ulteriori informazioni sulle opzioni disponibili per filtrare le OpsItems risposte, consulta OpsItemFiltersla Guida di riferimento.AWS Systems Manager API

- OpsInsightId

  Tipo: stringa

  Descrizione: (Facoltativo) L'identificatore di risorsa correlato che desideri aggiungere a risolto. OpsItems

- S3 BucketName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del bucket Amazon S3 a cui desideri inviare il riepilogo dei risultati.

- SnsMessage

  Tipo: stringa

  Descrizione: (Facoltativo) La notifica che desideri che Amazon Simple Notification Service (AmazonSNS) invii al termine dell'automazione.

- SnsTopicArn

  Tipo: stringa

  Descrizione: (Facoltativo) L'ARNSNSargomento Amazon che desideri notificare quando il riepilogo dei risultati viene inviato ad Amazon S3.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `s3:GetBucketAcl`
- `s3:PutObject`

- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Fasi del documento

- `aws:executeScript`- Raccoglie e risolve i dati in OpsItems base ai filtri specificati. Se è stato specificato un valore per il `OpsInsightId` parametro, il valore viene aggiunto come risorsa correlata.
- `aws:executeScript`- Se hai specificato un valore per il `S3BucketName` parametro, viene quindi inviato un riepilogo dei risultati al bucket Amazon S3.
- `aws:executeScript`- Se hai specificato un valore per il `SnsTopicArn` parametro, viene inviata una notifica all'SNSargomento Amazon dopo l'invio del riepilogo dei risultati ad Amazon S3, incluso il valore del `SnsMessage` parametro, se specificato.

`AWS-ConfigureMaintenanceWindows`

Descrizione

Il `AWS-ConfigureMaintenanceWindows` runbook consente di abilitare o disabilitare più finestre di manutenzione di Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- MaintenanceWindows

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole delle finestre IDs di manutenzione che si desidera abilitare o disabilitare.
- MaintenanceWindowsStatus

  Tipo: stringa

  Valori validi: «True» | «False»

  Predefinito: «False»

  Descrizione: (Obbligatorio) Determina se le finestre di manutenzione sono abilitate o disabilitate. Specificare «True» per abilitare le finestre di manutenzione e «False» per disabilitarle.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Fasi del documento

- `aws:executeScript`- Raccoglie lo stato delle finestre di manutenzione specificate nel `MaintenanceWindows` parametro e abilita o disabilita le finestre di manutenzione.

AWS-CreateManagedLinuxInstance

Descrizione

Crea un'EC2istanza per Linux configurata per Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AmiId

  Tipo: stringa

  Descrizione: (Obbligatorio) AMI ID da utilizzare per avviare l'istanza.
- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- GroupName

  Tipo: stringa

  Impostazione predefinita: SSMSecurityGroupForLinuxInstances

  Descrizione: (obbligatorio) nome del gruppo di sicurezza da creare.

- HttpTokens

  Tipo: stringa

  Valori validi: opzionale | obbligatorio

  Predefinito: opzionale

  Descrizione: (Facoltativo) IMDSv2 utilizza sessioni supportate da token. Imposta l'uso dei HTTP token su `optional` o per `required` determinare se IMDSv2 è facoltativo o obbligatorio.
- InstanceType

  Tipo: stringa

  Impostazione predefinita: t2.medium

  Descrizione: (obbligatorio) tipo di istanza da avviare. Impostazione predefinita: t2.medium
- KeyPairName

  Tipo: stringa

  Descrizione: (obbligatorio) coppia di chiavi da utilizzare durante la creazione dell'istanza.
- RemoteAccessCidr

  Tipo: stringa

  Impostazione predefinita: 0.0.0.0/0

  Descrizione: (Obbligatorio) Crea un gruppo di sicurezza con la porta per SSH (Intervallo di porte 22) aperta a IPs quanto specificato da CIDR (l'impostazione predefinita è 0.0.0.0/0). Se il gruppo di sicurezza esiste già, non verrà modificato e le regole non saranno modificate.
- RoleName

  Tipo: stringa

  Impostazione predefinita: SSMManagedInstanceProfileRole

  Descrizione: (obbligatorio) nome del ruolo da creare.
- StackName

  Tipo: stringa

Predefinito: CreateManagedInstanceStack {{automation: EXECUTION _ID}}

Descrizione: (Facoltativo) Specificare il nome dello stack utilizzato da questo runbook

- SubnetId

  Tipo: stringa

  Impostazione predefinita: Default

  Descrizione: (obbligatorio) la nuova istanza verrà distribuita nella sottorete oppure, se non ne è specificata una, nella sottorete predefinita.

- VpcId

  Tipo: stringa

  Impostazione predefinita: Default

  Descrizione: (Obbligatorio) La nuova istanza verrà distribuita in questo Amazon Virtual Private Cloud (AmazonVPC) o nell'Amazon predefinito, VPC se non specificato.

AWS-CreateManagedWindowsInstance

Descrizione

Crea un'EC2istanza per un Windows Server configurato per Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Parametri

- AmiId

  Tipo: stringa

  Impostazione predefinita: {{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}

  Descrizione: (Obbligatorio) AMI ID da utilizzare per avviare l'istanza.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- GroupName

  Tipo: stringa

  Impostazione predefinita: SSMSecurityGroupForLinuxInstances

  Descrizione: (obbligatorio) nome del gruppo di sicurezza da creare.

- HttpTokens

  Tipo: stringa

  Valori validi: opzionale | obbligatorio

  Predefinito: opzionale

  Descrizione: (Facoltativo) IMDSv2 utilizza sessioni supportate da token. Imposta l'uso dei HTTP token su `optional` o per `required` determinare se IMDSv2 è facoltativo o obbligatorio.

- InstanceType

  Tipo: stringa

  Impostazione predefinita: t2.medium

Descrizione: (obbligatorio) tipo di istanza da avviare. Impostazione predefinita: t2.medium

- KeyPairName

  Tipo: stringa

  Descrizione: (obbligatorio) coppia di chiavi da utilizzare durante la creazione dell'istanza.

- RemoteAccessCidr

  Tipo: stringa

  Impostazione predefinita: 0.0.0.0/0

  Descrizione: (Obbligatorio) Crea un gruppo di sicurezza con la porta per RDP (Intervallo di porte 3389) aperta a IPs quanto specificato da CIDR (l'impostazione predefinita è 0.0.0.0/0). Se il gruppo di sicurezza esiste già, non verrà modificato e le regole non saranno modificate.

- RoleName

  Tipo: stringa

  Impostazione predefinita: SSMManagedInstanceProfileRole

  Descrizione: (obbligatorio) nome del ruolo da creare.

- StackName

  Tipo: stringa

  Predefinito: CreateManagedInstanceStack {{automation: EXECUTION _ID}}

  Descrizione: (Facoltativo) Specificare il nome dello stack utilizzato da questo runbook

- SubnetId

  Tipo: stringa

  Impostazione predefinita: Default

  Descrizione: (obbligatorio) la nuova istanza verrà distribuita nella sottorete oppure, se non ne è specificata una, nella sottorete predefinita.

- VpcId

  Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Obbligatorio) La nuova istanza verrà distribuita in questo Amazon Virtual Private Cloud (AmazonVPC) o nell'Amazon predefinito, VPC se non specificato.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descrizione

Il `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook consente alle sessioni di AWS Systems Manager Session Manager (Session Manager) di archiviare i log di output in un gruppo di log Amazon CloudWatch (CloudWatch).

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DestinationLogGroup

  Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di CloudWatch log.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Fasi del documento

- `aws:executeScript`- Accetta il gruppo di CloudWatch log per aggiornare il documento che memorizza le preferenze dei log di output della sessione di Session Manager o ne crea uno se non esiste.

AWS-ExportOpsDataToS3

Descrizione

Questo runbook recupera un elenco di OpsData riepiloghi in AWS Systems Manager Explorer e li esporta in un oggetto in un bucket Amazon Simple Storage Service (Amazon S3) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- columnFields

  Tipo: StringList

  Descrizione: campi Colonna (Obbligatorio) da scrivere nel file di output.
- filtri

  Tipo: stringa

  Descrizione: (Facoltativo) Filtri per la getOpsSummary richiesta.
- resultAttribute

  Tipo: stringa

  Descrizione: (Facoltativo) L'attributo del risultato per la getOpsSummary richiesta.
- s3 BucketName

  Tipo: stringa

  Descrizione: (obbligatoria) bucket S3 in cui si desidera scaricare il file di output.
- snsSuccessMessage

  Tipo: stringa

  Descrizione: (Facoltativo) Messaggio da inviare al termine del runbook.
- snsTopicArn

Tipo: stringa

Descrizione: (Obbligatorio) Argomento Amazon Simple Notification Service (AmazonSNS) ARN per notificare il completamento del download.

- syncName

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome della sincronizzazione dei dati delle risorse.

Fasi del documento

getOpsSummaryPassaggio: recupera subito fino a 5.000 riepiloghi delle operazioni da esportare in un CSV file.

Output

OpsData oggetto: se il runbook viene eseguito correttamente, troverai l' OpsData oggetto esportato nel bucket S3 di destinazione.

AWS-ExportPatchReportToS3

Descrizione

Questo runbook recupera gli elenchi di dati di riepilogo delle patch e i dettagli delle AWS Systems Manager patch in Patch Manager e li esporta in file.csv in un bucket Amazon Simple Storage Service (Amazon S3) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- assumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che esegue questo documento.
- s3 BucketName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il bucket S3 in cui vuoi scaricare il file di output.
- snsTopicArn

  Tipo: stringa

  Descrizione: (Facoltativo) L'argomento Amazon Simple Notification Service (AmazonSNS) Amazon Resource Name (ARN) per notificare il completamento del download.
- snsSuccessMessage

  Tipo: stringa

  Descrizione: (Facoltativo) Testo del messaggio da inviare al termine del runbook.
- targets

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza o un carattere jolly (*) per indicare se riportare i dati della patch per un'istanza specifica o per tutte le istanze.

Fasi del documento

ExportReportStep — L'azione per questo passaggio dipende dal valore del `targets` parametro. Se `targets` è nel formato di`instanceids=*`, il passaggio recupera fino a 10.000 riepiloghi delle patch per le istanze presenti nell'account ed esporta i dati in un file.csv.

Se `targets` è nel formato`instanceids=<instance-id>`, il passaggio recupera sia il riepilogo delle patch che tutte le patch per l'istanza specificata nell'account e le esporta in un file.csv.

Output

PatchSummaryOggetto /Patches: se il runbook viene eseguito correttamente, l'oggetto del report sulle patch esportato viene scaricato nel bucket S3 di destinazione.

`AWS-SetupInventory`

Descrizione

Crea un'associazione Systems Manager Inventory per una o più istanze gestite. Il sistema raccoglie i metadati dalle istanze in base alla pianificazione definita nell'associazione. Per ulteriori informazioni, consulta AWS Systems Manager Inventario.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- Applicazioni

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (facoltativo) raccoglie i metadati relativi alle applicazioni installate.
- AssociatedDocName

  Tipo: stringa

  Impostazione predefinita: `AWS-GatherSoftwareInventory`

Descrizione: (Facoltativo) Il nome del runbook utilizzato per raccogliere l'inventario dall'istanza gestita.

- AssociationName

  Tipo: stringa

  Descrizione: (facoltativo) nome dell'associazione di Inventory che verrà assegnata all'istanza.

- AssocWaitTime

  Tipo: stringa

  Impostazione predefinita: PT5M

  Descrizione: (facoltativo) intervallo di tempo durante il quale la raccolta di Inventory deve essere messa in pausa quando viene raggiunta l'ora di inizio dell'associazione di Inventory. L'ora utilizza il formato ISO 8601.

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `AwsComponents`

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (Facoltativo) Raccogli metadati per AWS componenti come. amazon-ssm-agent

- CustomInventory

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (facoltativo) raccoglie i metadati di inventario personalizzati.

- File

Tipo: stringa

Descrizione: (facoltativo) raccoglie i metadati relativi ai file nelle istanze. Per ulteriori informazioni su come raccogliere questo tipo di dati di inventario, vedi Utilizzo dei file e dell'inventario del registro di Windows. Richiede SSMAgent versione 2.2.64.0 o successiva. Esempio di Linux: `[{"Path":"/usr/bin", "Pattern":["aws*", "*ssm*"],"Recursive":false}, {"Path":"/var/log", "Pattern":["amazon*.*"], "Recursive":true, "DirScanLimit":1000}] Windows example: [{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]`

- InstanceDetailedInformation

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (Facoltativo) Raccogli informazioni aggiuntive sull'istanza, tra cui CPU modello, velocità e numero di core, solo per citarne alcuni.

- InstanceIds

  Tipo: stringa

  Impostazione predefinita: *

  Descrizione: (Obbligatorio) EC2 istanze che desideri inventariare.

- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN ruolo che consente a Lambda creata da Automation di eseguire le azioni per tuo conto. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- NetworkConfig

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (facoltativo) raccoglie i metadati relativi alle configurazioni di rete.

- Uscite: 3 BucketName

Tipo: stringa

Descrizione: (Facoltativo) Nome di un bucket Amazon S3 in cui desideri scrivere i dati del registro di inventario.

- Uscite S3 KeyPrefix

  Tipo: stringa

  Descrizione: (Facoltativo) Un prefisso chiave Amazon S3 (sottocartella) in cui desideri scrivere i dati del registro di inventario.

- OutputS3Region

  Tipo: stringa

  Descrizione: (Facoltativo) Il nome del Regione AWS luogo in cui si trova Amazon S3.

- Pianificazione

  Tipo: stringa

  Impostazione predefinita: cron(0 */30 * * * ? *)

  Descrizione: (facoltativo) espressione cron per la pianificazione dell'associazione di Inventory. Il valore predefinito è ogni 30 minuti.

- Servizi

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (Facoltativo, solo sistema operativo Windows, richiede la SSMAgent versione 2.2.64.0 e successive) Raccogli dati per le configurazioni dei servizi.

- WindowsRegistry

  Tipo: stringa

  Descrizione: (facoltativo) raccoglie i metadati relativi alle chiavi del Registro di sistema di Microsoft Windows. Per ulteriori informazioni su come raccogliere questo tipo di dati di inventario, vedere Utilizzo dei file e dell'inventario del registro di Windows. Richiede la versione SSM dell'agente 2.2.64.0 o successiva. Esempio: [{"Path»:» HKEY _ CURRENT _CONFIG\ System»,

"Recursive» :true}, {"Path»:» HKEY _ _LOCAL\\ SOFTWARE AmazonMACHINE\ MachineImage «," «: [» ValueNames AMIName «]}]]

- WindowsRoles

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (facoltativo) raccoglie le informazioni sui ruoli di Windows nell'istanza. Si applica solo ai sistemi operativi Windows. Richiede SSMAgent versione 2.2.64.0 o successiva.

- WindowsUpdates

  Tipo: stringa

  Impostazione predefinita: Enabled

  Descrizione: (facoltativo) raccoglie i dati su tutti gli aggiornamenti di Windows nell'istanza.

AWS-SetupManagedInstance

Descrizione

Configura un'istanza con un ruolo AWS Identity and Access Management (IAM) per l'accesso a Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) ID dell'EC2istanza da configurare
- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN ruolo che consente a Lambda creata da Automation di eseguire le azioni per tuo conto. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.
- RoleName

  Tipo: stringa

  Impostazione predefinita: SSMRoleForManagedInstance

  Descrizione: (Facoltativo) Il nome del IAM ruolo per l'EC2istanza. Se il ruolo non esiste, ne verrà creato uno. Quando specificate questo valore, verificate che il ruolo contenga una politica mazonSSMManaged InstanceCore gestita A.

AWS-SetupManagedRoleOnEC2Instance

Descrizione

Configura un'istanza con il IAM ruolo SSMRoleForManagedInstance gestito per l'accesso a Systems Manager.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) ID dell'EC2istanza da configurare
- LambdaAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN ruolo che consente a Lambda creata da Automation di eseguire le azioni per tuo conto. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.
- RoleName

  Tipo: stringa

  Impostazione predefinita: SSMRoleForManagedInstance

  Descrizione: (Facoltativo) Il nome del IAM ruolo per l'EC2istanza. Se il ruolo non esiste, ne verrà creato uno. Quando specificate questo valore, verificate che il ruolo contenga una politica mazonSSMManaged InstanceCore gestita A.

AWSSupport-TroubleshootManagedInstance

Descrizione

Il `AWSSupport-TroubleshootManagedInstance` runbook ti aiuta a determinare perché un'istanza Amazon Elastic Compute Cloud (Amazon EC2) non riporta i report come gestita da. AWS Systems Manager Questo runbook esamina la configurazione VPC per l'istanza, incluse le regole dei gruppi di sicurezza, gli endpoint VPC, le regole della lista di controllo degli accessi alla rete (ACL) e le tabelle di routing. Inoltre, conferma che all'istanza è associato un profilo di istanza AWS Identity and Access Management (IAM) contenente le autorizzazioni richieste.

> **Important**
>
> Questo runbook di automazione non valuta le regole IPv6.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parameters (Parametri)

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 che non riporta come gestita da Systems Manager.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `iam:ListRoles`
- `iam:GetInstanceProfile`
- `iam:ListAttachedRolePolicies`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcEndpoints`

Fasi del documento

- `aws:executeScript`- Raccoglie l'`PingStatus`istanza.

- `aws:branch`- Filiali a seconda che l'istanza stia già segnalando come gestita da Systems Manager.
- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza, inclusa la configurazione VPC.
- `aws:executeScript`- Se applicabile, raccoglie ulteriori dettagli relativi agli endpoint VPC che sono stati implementati per l'uso con Systems Manager e conferma che i gruppi di sicurezza collegati all'endpoint VPC consentano il traffico in entrata sulla porta TCP 443 dall'istanza.
- `aws:executeScript`- Verifica se la tabella delle rotte consente il traffico verso l'endpoint VPC o gli endpoint pubblici di Systems Manager.
- `aws:executeScript`- Verifica se le regole ACL di rete consentono il traffico verso l'endpoint VPC o gli endpoint pubblici di Systems Manager.
- `aws:executeScript`- Verifica se il traffico in uscita verso l'endpoint VPC o gli endpoint pubblici di Systems Manager è consentito dal gruppo di sicurezza associato all'istanza.
- `aws:executeScript`- Verifica se il profilo dell'istanza collegato all'istanza include una policy gestita che fornisce le autorizzazioni richieste.
- `aws:branch`- Filiali basate sul sistema operativo dell'istanza.
- `aws:executeScript`- Fornisce un riferimento allo script di `ssmagent-toolkit-linux` shell.
- `aws:executeScript`- Fornisce un riferimento allo `ssmagent-toolkit-windows` PowerShell script.
- `aws:executeScript`- Genera l'output finale per l'automazione.
- `aws:executeScript`- Se l'`PingStatus`istanza è`Online`, restituisce che l'istanza è già gestita da Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descrizione

Il `AWSSupport-TroubleshootPatchManagerLinux` runbook risolve i problemi più comuni che possono causare un errore di patch sui nodi gestiti basati su Linux utilizzando la AWS Systems Manager funzionalità «Patch Manager». L'obiettivo principale di questo runbook è identificare la causa principale dell'errore del comando patch e suggerire un piano di correzione.

Come funziona?

Il `AWSSupport-TroubleshootPatchManagerLinux` runbook considera la coppia ID di istanza/ID di comando forniti dall'utente per la risoluzione dei problemi. Se non viene fornito alcun Command ID,

seleziona l'ultimo comando di patch non riuscito negli ultimi 30 giorni sull'istanza fornita. Dopo aver verificato lo stato del comando, il rispetto dei prerequisiti e la distribuzione del sistema operativo, il runbook scarica ed esegue un pacchetto di analisi dei log. L'output include la causa principale del problema e l'azione necessaria per risolverlo.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

- Amazon Linux 2 e AL2 023
- Red Hat Enterprise Linux 8.X e 9.X
- Centos 8.X e 9.X
- SUSE15X

Parametri

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`

- `ssm:GetAutomationExecution`

Istruzioni

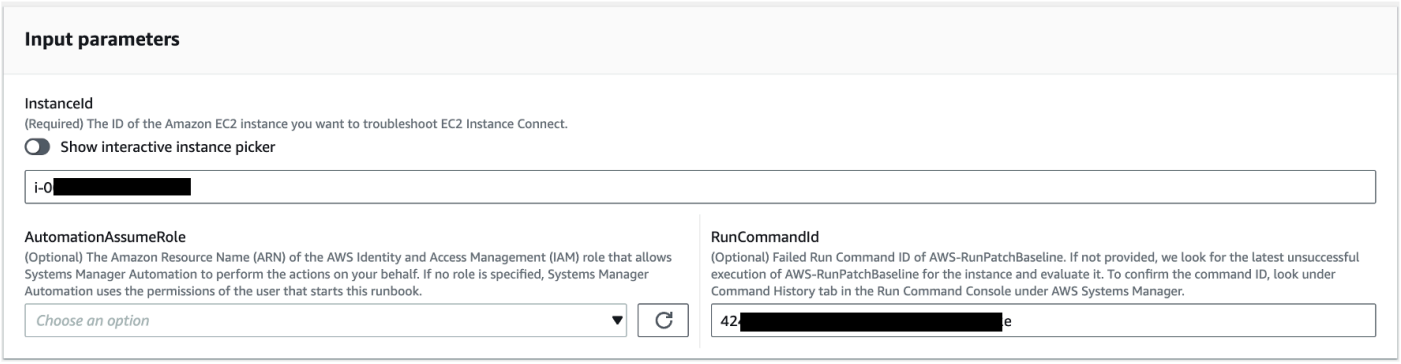
Segui questi passaggi per configurare l'automazione:

1. Passa a AWSSupport-TroubleshootPatchManagerLinuxnella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
   - InstanceId (Obbligatorio):

     Usa il selettore interattivo di istanze per scegliere l'ID del SSM Managed Node basato su Linux (Amazon Elastic Compute Cloud (AmazonEC2) o server Hybrid Activated) rispetto al quale il comando patch non è riuscito, oppure inserisci manualmente l'ID dell'istanza SSM gestita.
   - AutomationAssumeRole (Facoltativo):

     Inserisci il ARN IAM ruolo che consente all'automazione di eseguire azioni per tuo conto. Se non viene specificato un ruolo, Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - RunCommandId (Facoltativo):

     Immettere l'ID del comando Failed `AWS-RunPatchBaseline` Run del documento. Se non fornite un Command ID, il runbook cercherà l'ultimo comando di patch non riuscito negli ultimi 30 giorni sull'istanza selezionata.



4. Seleziona Esegui.
5. L'automazione viene avviata.
6. Il documento esegue le seguenti operazioni:

- CheckConcurrency:

  Assicura che esista una sola esecuzione di questo runbook destinata alla stessa istanza. Se il runbook rileva un'altra esecuzione in corso relativa alla stessa istanza, restituisce un errore e termina.

- ValidateCommandID:

  Verifica se l'ID di comando fornito, come parametro di input, è stato eseguito per il `AWS-RunPatchBaseline` SSM documento. Se non viene fornito alcun Command ID, il runbook prenderà in considerazione l'ultima esecuzione non riuscita degli `AWS-RunPatchBaseline` ultimi 30 giorni sull'istanza selezionata.

- BranchOnCommandStatus:

  Conferma che lo stato del comando fornito non è riuscito. In caso contrario, il runbook termina l'esecuzione e genera un rapporto che indica che il comando fornito è stato eseguito correttamente.

- VerifyPrerequistes:

  Conferma che i prerequisiti sopra menzionati sono soddisfatti.

- GetPlatformDetails:

  Recupera la distribuzione e la versione del sistema operativo (OS).

- GetDownloadURL:

  Recupera il download del pacchetto URL PatchManager Log Analyzer.

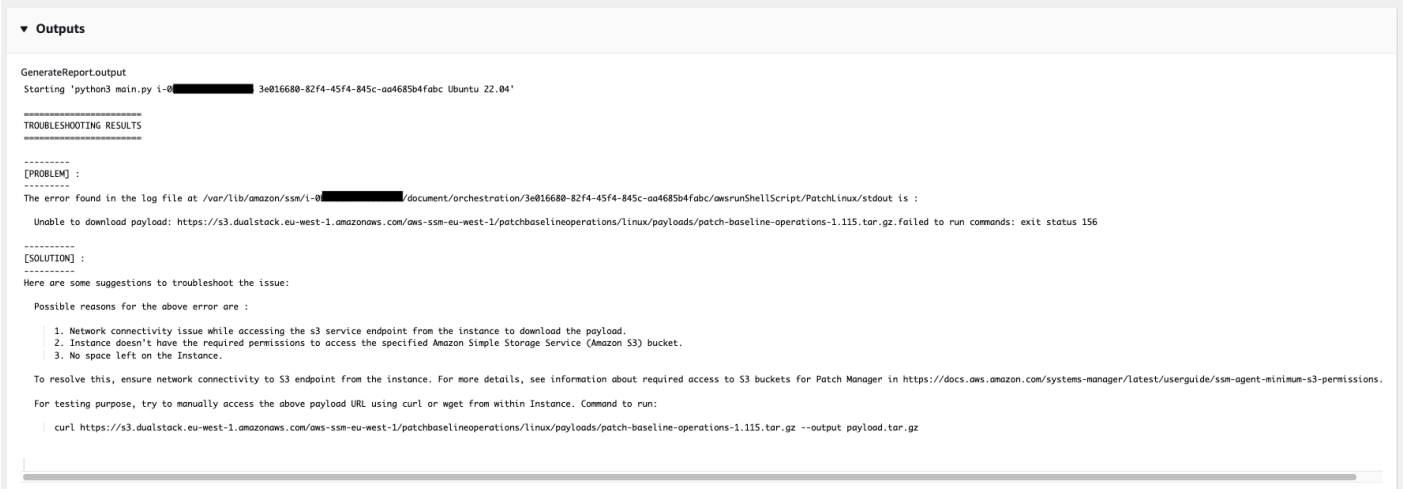
- EvaluatePatchManagerLogs:

  Scarica ed esegue il pacchetto python PatchManager Log Analyzer sull'istanza per valutare il file di registro.

- GenerateReport:

  Genera un rapporto finale sull'esecuzione del runbook che include il problema identificato e la soluzione suggerita.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWSSupport-TroubleshootSessionManager

Descrizione

Il `AWSSupport-TroubleshootSessionManager` runbook ti aiuta a risolvere i problemi più comuni che impediscono la connessione a istanze gestite di Amazon Elastic Compute Cloud (AmazonEC2) utilizzando Session Manager. Session Manager è una funzionalità di. AWS Systems Manager Questo runbook verifica quanto segue:

- Verifica se l'istanza è in esecuzione e riporta i report come gestito da Systems Manager.
- Esegue il `AWSSupport-TroubleshootManagedInstance` runbook se l'istanza non riporta i dati come gestiti da Systems Manager.
- Controlla la versione dell'SSMagente installata sull'istanza.
- Verifica se un profilo di istanza contenente una policy recommended AWS Identity and Access Management (IAM) per Session Manager è collegato all'EC2istanza Amazon.
- Raccoglie i log SSM dell'agente dall'istanza.

- Analizza le preferenze del Session Manager.
- Esegue il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook per analizzare la connettività dell'istanza agli endpoint per Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) e Amazon CloudWatch Logs (Logs). CloudWatch

Considerazioni

- I nodi gestiti ibridi non sono supportati.
- Questo runbook verifica solo se una IAM policy gestita consigliata è associata al profilo dell'istanza. Non analizza le IAM AWS KMS autorizzazioni contenute nel profilo dell'istanza.

> **Important**
>
> Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook utilizza VPCReachability Analyzer per analizzare la connettività di rete tra un endpoint di origine e un endpoint di servizio. Ti viene addebitato un costo per ogni esecuzione di analisi tra un'origine e una destinazione. Per ulteriori dettagli, consulta la pagina VPCdei prezzi di Amazon.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID dell'EC2istanza Amazon a cui non riesci a connetterti tramite Session Manager.

- SessionPreferenceDocument

  Tipo: stringa

  Predefinito: SSM - SessionManagerRunShell

  Descrizione: (Facoltativo) Il nome del documento delle preferenze di sessione. Se non specificate un documento personalizzato con le preferenze di sessione all'avvio delle sessioni, utilizzate il valore predefinito.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateNetworkInsightsPath`
- `ec2:DeleteNetworkInsightsAnalysis`
- `ec2:DeleteNetworkInsightsPath`
- `ec2:StartNetworkInsightsAnalysis`
- `tiros:CreateQuery`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`

- ec2:DescribeInternetGateways
- ec2:DescribeManagedPrefixLists
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInsightsAnalyses
- ec2:DescribeNetworkInsightsPaths
- ec2:DescribeNetworkInterfaces
- ec2:DescribePrefixLists
- ec2:DescribeRegions
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTransitGatewayAttachments
- ec2:DescribeTransitGatewayConnects
- ec2:DescribeTransitGatewayPeeringAttachments
- ec2:DescribeTransitGatewayRouteTables
- ec2:DescribeTransitGateways
- ec2:DescribeTransitGatewayVpcAttachments
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetManagedPrefixListEntries
- ec2:GetTransitGatewayRouteTablePropagations
- ec2:SearchTransitGatewayRoutes
- elasticloadbalancing:DescribeListeners

- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeRules
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- iam:GetInstanceProfile
- iam:ListAttachedRolePolicies
- iam:ListRoles
- iam:PassRole
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:StartAutomationExecution
- tiros:GetQueryAnswer
- tiros:GetQueryExplanation

Fasi del documento

1. aws:waitForAwsResourceProperty: Attende fino a 6 minuti che l'istanza di destinazione superi i controlli di stato.
2. aws:executeScript: analizza il documento delle preferenze di sessione.
3. aws:executeAwsApi: ottiene il profilo ARN dell'istanza associato all'istanza.
4. aws:executeAwsApi: verifica se l'istanza riporta i report come gestita da Systems Manager.
5. aws:branch: filiali in base al fatto che l'istanza riporti o meno come gestita da Systems Manager.
6. aws:executeScript: verifica se l'SSMagente installato sull'istanza supporta Session Manager.

7. `aws:branch`: filiali basate sulla piattaforma dell'istanza per la raccolta dei `ssm-cli` log.
8. `aws:runCommand`: raccoglie l'output dei log `ssm-cli` da un'Linuxistanza or. macOS
9. `aws:runCommand`: raccoglie l'output dei log da `ssm-cli` un'istanza. Windows
10. `aws:executeScript`: analizza i log. `ssm-cli`
11. `aws:executeScript`: verifica se una IAM politica consigliata è associata al profilo dell'istanza.
12. `aws:branch`: determina se valutare la connettività `ssmmessages` degli endpoint in base ai `ssm-cli` log.
13. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint. `ssmmessages`
14. `aws:branch`: determina se valutare la connettività degli endpoint Amazon S3 in base ai `ssm-cli` log e alle preferenze di sessione.
15. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint Amazon S3.
16. `aws:branch`: determina se valutare la connettività AWS KMS degli endpoint in base ai `ssm-cli` log e alle preferenze di sessione.
17. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint. AWS KMS
18. `aws:branch`: Determina se valutare la connettività CloudWatch degli endpoint di Logs in base ai `ssm-cli` log e alle preferenze di sessione.
19. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint Logs. CloudWatch
20. `aws:executeAutomation`: esegue il runbook. `AWSSupport-TroubleshootManagedInstance`
21. `aws:executeScript`: compila l'output dei passaggi precedenti e genera un rapporto.

Uscite

- `generateReport.EvalReport`- I risultati dei controlli eseguiti dal runbook in testo semplice.

Terze parti

AWS Systems Manager Automation fornisce runbook predefiniti per prodotti e servizi di terze parti. Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-CreateJiraIssue

- AWS-CreateServiceNowIncident
- AWS-RunPacker

AWS-CreateJiraIssue

Descrizione

Crea un problema in Jira.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AssigneeName

  Tipo: stringa

  Descrizione: (facoltativo) il nome utente della persona a cui assegnare il problema.
- DueDate

  Tipo: stringa

  Descrizione: (Facoltativa) La data di scadenza del problema in yyyy-mm-dd formato.
- IssueDescription

  Tipo: stringa

  Descrizione: (obbligatorio) una descrizione dettagliata del problema.
- IssueSummary

Tipo: stringa

Descrizione: (obbligatorio) breve riepilogo del problema.

- IssueTypeName

  Tipo: stringa

  Descrizione: (obbligatorio) il nome del tipo di problema da creare (ad esempio, attività, attività secondaria, bug e così via).

- Jira URL

  Tipo: stringa

  Descrizione: (obbligatorio) l'URL dell'istanza Jira.

- JiraUsername

  Tipo: stringa

  Descrizione: (obbligatorio) il nome dell'utente con cui sarà creato il problema.

- PriorityName

  Tipo: stringa

  Descrizione: (facoltativo) il nome della priorità del problema.

- ProjectKey

  Tipo: stringa

  Descrizione: (obbligatorio) la chiave del progetto in cui dovrebbe essere creato il problema.

- SSMParameterName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome di un SSM parametro crittografato contenente la API chiave o la password per l'utente Jira.

Fasi del documento

`aws:createStack`- Crea uno CloudFormation stack per creare ruoli e funzioni IAM Lambda.

`aws:invokeLambdaFunction`- Invoca la funzione Lambda per creare il problema Jira

`aws:deleteStack`- Elimina lo stack creato CloudFormation .

Output

IssueId: ID del problema Jira appena creato

`AWS-CreateServiceNowIncident`

Descrizione

Crea un incidente nella tabella degli ServiceNow incidenti.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Categoria

  Tipo: stringa

Descrizione: (Facoltativo) La categoria dell'incidente.

Valori validi: Nessuno | Richiesta/Guida | Software | Hardware | Rete | Database

Valore predefinito: nessuno

- Descrizione

  Tipo: stringa

  Descrizione: (Obbligatorio) Una spiegazione dettagliata dell'incidente.

- Impatto

  Tipo: stringa

  Descrizione: (Facoltativo) L'effetto che un incidente ha sul business.

  Valori validi: Alto | Medio | Basso

  Valore predefinito: Basso

- ServiceNowInstanceUsername

  Tipo: stringa

  Descrizione: (Obbligatorio) il nome dell'utente con cui sarà creato l'incidente.

- ServiceNowInstancePassword

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome di un SSM parametro crittografato contenente la password dell' ServiceNow utente.

- ServiceNowInstanceURL

  Tipo: stringa

  Descrizione: (Obbligatorio) L'URL ServiceNow istanza

- ShortDescription

  Tipo: stringa

  Descrizione: (Obbligatorio) Una breve descrizione dell'incidente.

- Sottocategoria

  Tipo: stringa

  Descrizione: (Facoltativo) La sottocategoria dell'incidente.

  Valori validi: Nessuno | Antivirus | Email | Applicazione interna | Sistema operativo | Disco CPU | Tastiera | Hardware | Memoria | Monitor | Mouse DHCP | DNS | Indirizzo IP | VPN | Wireless | DB2 | MS SQL Server | Oracle

  Valore predefinito: nessuno

Fasi del documento

push_incident — Invia le informazioni sull'incidente a. ServiceNow

Output

push_incident.incidentID — L'ID dell'incidente creato.

AWS-RunPacker

Descrizione

Questo runbook utilizza lo strumento HashiCorp Packer per convalidare, correggere o creare modelli di packer utilizzati per creare immagini di macchine. Questo runbook utilizza Packer v1.7.2.

> **Note**
>
> Se specifichi un valore `vpc_id`, devi anche specificare il valore `subnet_id` di una sottorete pubblica. A meno che non modifichi l'attributo di indirizzamento IPv4 pubblico della sottorete, è necessario impostare anche su true. `associate_public_ip_address`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- Force

  Tipo: Booleano

  Descrizione: un'opzione Packer per forzare l'esecuzione di un costruttore quando gli artefatti di una build precedente impediscono l'esecuzione di una build.
- Modalità

  Tipo: stringa

  Descrizione: la modalità o il comando in cui utilizzare Packer durante la convalida rispetto al modello. Le opzioni includono `BuildValidate`, e. `Fix`
- TemplateFileName

  Tipo: stringa

  Descrizione: il nome o la chiave del file modello nel bucket S3.
- Modelli 3 BucketName

  Tipo: stringa

  Descrizione: il nome del bucket S3 contenente il modello di packer.

Fasi del documento

RunPackerProcessTemplate — Esegue la modalità selezionata sul modello utilizzando lo strumento Packer.

Output

RunPackerProcessTemplate.output — Lo stdout dello strumento Packer.

RunPackerProcessTemplate.fixed_template_key — Il nome del modello memorizzato in un bucket S3 da utilizzare solo durante l'esecuzione in modalità «Fix».

RunPackerProcessTemplate.s3_bucket: il nome del bucket S3 che contiene il modello fisso da utilizzare solo durante l'esecuzione in modalità «Fix».

Amazon VPC

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Virtual Private Cloud. Per ulteriori informazioni sui runbook, consulta Working with runbooks. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-CloseSecurityGroup
- AWSSupport-ConfigureDNSQueryLogging
- AWSSupport-ConfigureTrafficMirroring
- AWSSupport-ConnectivityTroubleshooter
- AWSSupport-TroubleshootVPN
- AWSConfigRemediation-DeleteEgressOnlyInternetGateway
- AWSConfigRemediation-DeleteUnusedENI
- AWSConfigRemediation-DeleteUnusedSecurityGroup
- AWSConfigRemediation-DeleteUnusedVPCNetworkACL
- AWSConfigRemediation-DeleteVPCFlowLog
- AWSConfigRemediation-DetachAndDeleteInternetGateway
- AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway
- AWS-DisableIncomingSSHOnPort22
- AWS-DisablePublicAccessForSecurityGroup
- AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

- AWSSupport-EnableVPCFlowLogs
- AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch
- AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket
- AWS-ReleaseElasticIP
- AWS-RemoveNetworkACLUnrestrictedSSHRDP
- AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules
- AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules
- AWSSupport-SetupIPMonitoringFromVPC
- AWSSupport-TerminateIPMonitoringFromVPC

AWS-CloseSecurityGroup

Descrizione

Questo runbook rimuove tutte le regole di ingresso e uscita dal gruppo di sicurezza specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SecurityGroupId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza che si desidera chiudere.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeScript`- Rimuove tutte le regole di ingresso e uscita dal gruppo di sicurezza specificato nel parametro. `SecurityGroupId`

AWSSupport-ConfigureDNSQueryLogging

Descrizione

Il `AWSSupport-ConfigureDNSQueryLogging` runbook configura la registrazione per DNS le query che provengono dal tuo cloud privato virtuale () VPC o per le zone ospitate di Amazon Route 53. Puoi scegliere di pubblicare i log delle query su Amazon Logs, Amazon CloudWatch Simple Storage Service (Amazon S3) o Amazon Data Firehose. Per ulteriori informazioni sulla registrazione delle query e sui log delle query con resolver, consulta Public query logging e Resolver query logging. DNS

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LogDestinationArn

  Tipo: stringa

  Descrizione: (Facoltativo) Il ARN gruppo CloudWatch Logs, il bucket Amazon S3 o lo stream Firehose a cui desideri inviare i log delle query. Tieni presente che la registrazione delle DNS query pubbliche di Route 53 supporta solo i gruppi Logs. CloudWatch Se non si specifica un valore per questo parametro, l'automazione crea un gruppo CloudWatch Logs con il formato `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` e una politica IAM delle risorse per pubblicare i log delle query. Il gruppo CloudWatch Logs creato dall'automazione ha un periodo di conservazione di 14 giorni.
- QueryLogType

  Tipo: stringa

  Descrizione: (Facoltativo) I tipi di interrogazioni che si desidera registrare.

  Valori validi: Public | Resolver/Private

  Impostazione predefinita: Pubblico
- ResourceId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa di cui desideri registrare le interrogazioni. Se si specifica `Public` il `QueryLogType` parametro, la risorsa deve essere l'ID di una zona ospitata privata sulla Route 53. Se si specifica `Resolver/Private` il `QueryLogType` parametro, la risorsa deve essere l'ID di unVPC.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeVpcs`
- `firehose:ListTagsForDeliveryStream`
- `firehose:PutRecord`
- `firehose:PutRecordBatch`
- `firehose:TagDeliveryStream`
- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateRole`
- `iam:CreateServiceLinkedRole`
- `iam:DeletePolicy`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetPolicy`
- `iam:GetRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:TagRole`
- `iam:UpdateRole`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`

- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:DescribeResourcePolicies
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:PutRetentionPolicy
- logs:UpdateLogDelivery
- route53:CreateQueryLoggingConfig
- route53:DeleteQueryLoggingConfig
- route53:GetHostedZone
- route53resolver:AssociateResolverQueryLogConfig
- route53resolver:CreateResolverQueryLogConfig
- route53resolver:DeleteResolverQueryLogConfig
- s3:GetBucketAcl

Fasi del documento

- aws:executeScript- Verifica l'esistenza della risorsa specificata per il ResourceId parametro e verifica se il tipo di risorsa corrisponde all'opzione richiestaQueryLogType.
- aws:executeScript- Verifica che il valore specificato per il LogDestinationArn parametro corrisponda a quello richiesto. QueryLogType
- aws:executeScript- Verifica le autorizzazioni richieste a Route 53 per pubblicare i log nel gruppo CloudWatch Logs log e crea la politica IAM delle risorse richiesta se non esiste.
- aws:executeScript- Abilita la registrazione delle DNS interrogazioni sulla destinazione selezionata.

AWSSupport-ConfigureTrafficMirroring

Descrizione

Il `AWSSupport-ConfigureTrafficMirroring` runbook configura il mirroring del traffico per aiutarti a risolvere i problemi di connettività tra un sistema di bilanciamento del carico e le istanze Amazon Elastic Compute Cloud (Amazon). EC2 Il mirroring del traffico copia il traffico in entrata e in uscita dalle interfacce di rete collegate alle istanze. Per configurare il mirroring del traffico, questo runbook crea gli obiettivi, i filtri e le sessioni richiesti. Per impostazione predefinita, il runbook configura il mirroring per tutto il traffico in entrata e in uscita per tutti i protocolli tranne Amazon. DNS Se desideri rispecchiare il traffico proveniente da fonti e destinazioni specifiche, puoi modificare le regole in entrata e in uscita dopo il completamento dell'automazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- Fonte ENI

  Tipo: stringa

  Descrizione: (Obbligatorio) L'interfaccia elastica di rete per cui desideri configurare il mirroring del traffico.
- Target

  Tipo: stringa

Descrizione: (Obbligatorio) La destinazione per il traffico rispecchiato. È necessario specificare l'ID di un'interfaccia di rete, un Network Load Balancer o un endpoint Gateway Load Balancer. Se si specifica un Network Load Balancer, devono essere presenti UDP listener sulla porta 4789.

- SessionNumber

  Tipo: stringa

  Valori validi: 1-32766

  Descrizione: (Obbligatorio) Il numero della sessione mirror che desideri utilizzare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilter`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

Fasi del documento

- `aws:executeScript`- Esegue uno script per creare un obiettivo.
- `aws:executeAwsApi`- Crea una regola di filtro.
- `aws:executeAwsApi`- Crea una regola di filtro speculare per tutto il traffico in entrata.
- `aws:executeAwsApi`- Crea una regola di filtro speculare per tutto il traffico in uscita.

- `aws:executeAwsApi`- Crea una sessione mirror sul traffico.
- `aws:executeAwsApi`- Elimina il filtro se la creazione del filtro o della sessione fallisce.
- `aws:executeAwsApi`- Elimina la destinazione se la creazione del filtro o della sessione fallisce.

Output

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget- T. argetIDOutput

`AWSSupport-ConnectivityTroubleshooter`

Descrizione

Il `AWSSupport-ConnectivityTroubleshooter` runbook diagnostica i problemi di connettività tra i seguenti:

- AWS risorse all'interno di un Amazon Virtual Private Cloud (AmazonVPC)
- AWS risorse in diversi Amazon VPCs all'interno dello stesso Regione AWS che sono collegate tramite VPC peering
- AWS risorse in Amazon VPC e risorse Internet che utilizzano un gateway Internet
- AWS risorse in un Amazon VPC e una risorsa Internet che utilizza un gateway di traduzione degli indirizzi di rete (NAT)

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- IP di destinazione

  Tipo: stringa

  Descrizione: (Obbligatorio) L'IPv4indirizzo della risorsa a cui desideri connetterti.

- DestinationPort

  Tipo: stringa

  Impostazione predefinita: true

  Descrizione: (Obbligatorio) Il numero di porta a cui vuoi connetterti sulla risorsa di destinazione.

- DestinationVpc

  Tipo: stringa

  Impostazione predefinita: Tutto

  Descrizione: (Facoltativo) L'ID dell'Amazon a VPC cui desideri testare la connettività.

- SourceIP

  Tipo: stringa

  Descrizione: (Obbligatorio) L'IPv4indirizzo privato della AWS risorsa in Amazon da VPC cui desideri testare la connettività.

- SourcePortRange

  Tipo: stringa

  Descrizione: (Facoltativo) L'intervallo di porte utilizzato dalla AWS risorsa in Amazon da VPC cui desideri testare la connettività.

- SourceVpc

Tipo: stringa

Impostazione predefinita: Tutte

Descrizione: (Facoltativo) L'ID dell'Amazon da VPC cui desideri testare la connettività.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

Fasi del documento

- `aws:executeScript`- Raccoglie dettagli sulla AWS risorsa specificata nel `SourceIP` parametro.
- `aws:executeScript`- Determina la destinazione del traffico di rete proveniente dalla AWS risorsa utilizzando le rotte raccolte nel passaggio precedente.
- `aws:branch`- Filiali in base alla destinazione del traffico di rete.
- `aws:executeAwsApi`- Raccoglie dettagli sulla risorsa di destinazione.
- `aws:executeScript`- Conferma che l'ID restituito per la destinazione Amazon VPC corrisponde al valore specificato, se presente, nel `DestinationVpc` parametro.
- `aws:executeAwsApi`- Raccoglie le regole del gruppo di sicurezza per le risorse di origine e di destinazione.
- `aws:executeScript`- Conferma se le regole del gruppo di sicurezza consentono il traffico necessario tra le risorse di origine e di destinazione.
- `aws:executeAwsApi`- Raccoglie gli elenchi di controllo degli accessi alla rete (NACLs) associati alle sottoreti per le risorse di origine e di destinazione.

- `aws:executeScript`- Conferma se NACLs consente il traffico necessario tra le risorse di origine e di destinazione.
- `aws:executeScript`- Conferma se la sorgente ha un indirizzo IP pubblico associato alla risorsa, se la destinazione del percorso è un gateway Internet.
- `aws:executeAwsApi`- Raccoglie le regole del gruppo di sicurezza per la risorsa di origine.
- `aws:executeScript`- Conferma se le regole del gruppo di sicurezza consentono il traffico necessario dalla risorsa di origine alla risorsa di destinazione.
- `aws:executeAwsApi`- Raccoglie i dati NACLs associati alla sottorete per la risorsa di origine.
- `aws:executeScript`- Conferma se NACLs consente il traffico necessario dalla risorsa di origine.
- `aws:executeAwsApi`- Raccoglie i dettagli sul NAT gateway.
- `aws:executeAwsApi`- Raccoglie i dati NACLs associati alla sottorete per il gateway. NAT
- `aws:executeScript`- Conferma se NACLs consente il traffico necessario dalla sottorete per il gateway. NAT
- `aws:executeScript`- Raccoglie le rotte associate alla sottorete per il gateway. NAT
- `aws:executeScript`- Conferma se il NAT gateway dispone di un percorso verso un gateway Internet.
- `aws:executeAwsApi`- Raccoglie dettagli sulla connessione VPC peering.
- `aws:executeScript`- Conferma che entrambi VPCs si trovano nella stessa regione e che l'ID restituito per la destinazione VPC corrisponde al valore specificato, se presente, nel `DestinationVpc` parametro.
- `aws:executeAwsApi`- Restituisce la sottorete della risorsa di destinazione.
- `aws:executeScript`- Raccoglie le rotte associate alla sottorete per il peering. VPC
- `aws:executeScript`- Conferma se il peer VPC dispone di un percorso verso la connessione peering.
- `aws:executeScript`- Conferma se il traffico è consentito dalla risorsa di origine se la destinazione non è supportata dall'automazione.

AWSSupport-TroubleshootVPN

Descrizione

Il `AWSSupport-TroubleshootVPN` runbook ti aiuta a tracciare e risolvere gli errori in una AWS Site-to-Site VPN connessione. L'automazione include diversi controlli automatici progettati

per tracciare `IKEv2` gli errori `IKEv1` relativi ai tunnel di AWS Site-to-Site VPN connessione. L'automazione cerca di individuare errori specifici e la relativa risoluzione forma un elenco di problemi comuni.

Nota: questa automazione non corregge gli errori. Viene eseguito per l'intervallo di tempo indicato e analizza il gruppo di log alla ricerca di errori nel gruppo di VPN CloudWatch log.

Come funziona?

Il runbook esegue una convalida dei parametri per confermare se il gruppo di CloudWatch log Amazon incluso nel parametro di input esiste, se vi sono flussi di log nel gruppo di log che corrispondono al VPN tunnel logging, se esiste l'id di VPN connessione e se esiste l'indirizzo IP del tunnel. Effettua API chiamate Logs Insights sul tuo gruppo di CloudWatch log configurate per la registrazione. VPN

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- LogGroupName

  Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di CloudWatch log Amazon configurato per la registrazione delle AWS Site-to-Site VPN connessioni

Pattern consentito: `^[\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID di AWS Site-to-Site VPN connessione da risolvere.

  Modello consentito: `^vpn-[0-9a-f]{8,17}$`

- T unnelAIPAddress

  Tipo: stringa

  Descrizione: (Obbligatorio) L'IPv4indirizzo del tunnel numero 1 associato al tuo AWS Site-to-Site VPN.

  Modello consentito: `^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}$`

- T unnelBIPAddress

  Tipo: stringa

  Descrizione: (Facoltativo) L'IPv4indirizzo del tunnel numero 2 associato al tuo AWS Site-to-Site VPN.

  Modello consentito: `^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

  Tipo: stringa

  Descrizione: (Obbligatorio) Seleziona IKE la versione che stai utilizzando. Valori consentiti:IKEv1, IKEv2

  Valori validi: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

Tipo: stringa

Descrizione: (Facoltativo) Ora di inizio dell'analisi del registro. È possibile utilizzare StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod per l'analisi dei log

Modello consentito: `^\d{10}|^$`

- EndTimeinEpoch

  Tipo: stringa

  Descrizione: (Facoltativo) Ora di fine dell'analisi dei log. È possibile utilizzare StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod per l'analisi dei log. Se vengono dati entrambi StartTimeinEpoch/EndTimeinEpoch e LookBackPeriod allora hanno la LookBackPeriod precedenza

  Modello consentito: `^\d{10}|^$`

- LookBackPeriod

  Tipo: stringa

  Descrizione: (Facoltativo) Tempo a due cifre in ore per esaminare l'analisi dei log. Intervallo valido: 01 - 99. Questo valore ha la precedenza se dai StartTimeinEpoch anche e EndTime

  Modello consentito: `^(\d?[1-9]|[1-9]0)|^$`

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Istruzioni

Nota: questa automazione funziona sui gruppi di CloudWatch log configurati per la registrazione VPN del tunnel, quando il formato di output della registrazione è. JSON

Segui questi passaggi per configurare l'automazione:

1. Vai alla sezione AWSSupport-Troubleshoot VPN nella console. AWS Systems Manager
2. Per i parametri di input, inserisci quanto segue:
   - AutomationAssumeRole (Facoltativo):

     L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
   - LogGroupName (Obbligatorio):

     Il nome del gruppo di CloudWatch log Amazon da convalidare. Questo deve essere il gruppo di CloudWatch log a cui è configurato VPN l'invio dei log.
   - VpnConnectionId (Obbligatorio):

     L'ID di AWS Site-to-Site VPN connessione il cui gruppo di log viene tracciato per rilevare eventuali VPN errori.
   - T unnelAIPAddress (obbligatorio):

     Il tunnel Un indirizzo IP associato alla AWS Site-to-Site VPN connessione.
   - T unnelBIPAddress (opzionale):

     L'indirizzo IP B del tunnel associato alla AWS Site-to-Site VPN connessione.
   - IKEVersion(Obbligatorio):

     Seleziona quello IKEversion che stai usando. Valori consentiti:IKEv1,IKEv2.
   - StartTimeinEpoch (Facoltativo):

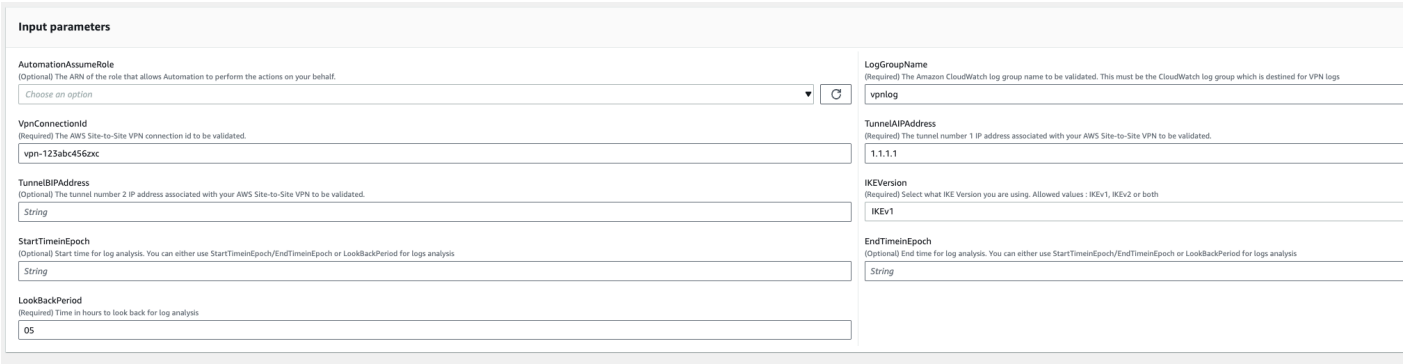
     L'inizio dell'intervallo di tempo in cui eseguire la ricerca di errori. L'intervallo è inclusivo, quindi l'ora di inizio specificata viene inclusa nella query. Specificato come ora dell'epoca, il numero di secondi trascorsi dal 1° gennaio 1970, 00:00:00. UTC
   - EndTimeinEpoch (Facoltativo):

La fine dell'intervallo di tempo in cui eseguire la ricerca di errori. L'intervallo è inclusivo, quindi l'ora di fine specificata viene inclusa nella query. Specificato come ora dell'epoca, il numero di secondi trascorsi dal 1° gennaio 1970, 00:00:00. UTC

- LookBackPeriod (Obbligatorio):

  Tempo, espresso in ore, per verificare la presenza di errori nella ricerca di errori.

Nota: configura un StartTimeinEpoch EndTimeinEpoch, o fissa LookBackPeriod l'intervallo di tempo per l'analisi dei log. Fornisci un numero a due cifre in ore per verificare la presenza di errori passati dall'ora di inizio dell'automazione. Oppure, se l'errore riguarda il passato e rientra in un intervallo di tempo specifico, includi StartTimeinEpoch e EndTimeinEpoch, invece di. LookBackPeriod



3. Seleziona Esegui.
4. L'automazione si avvia.
5. Il runbook di automazione esegue i seguenti passaggi:
   - parameterValidation:

     Esegue una serie di convalide sui parametri di input inclusi nell'automazione.
   - branchOnValidationOfLogGroup:

     Verifica se il gruppo di log menzionato nel parametro è valido. Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.
   - branchOnValidationOfLogStream:

     Verifica se il flusso di log esiste nel gruppo di log incluso. CloudWatch Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.
   - branchOnValidationOfVpnConnectionId:

Verifica se l'ID di VPN connessione incluso nel parametro è valido. Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.

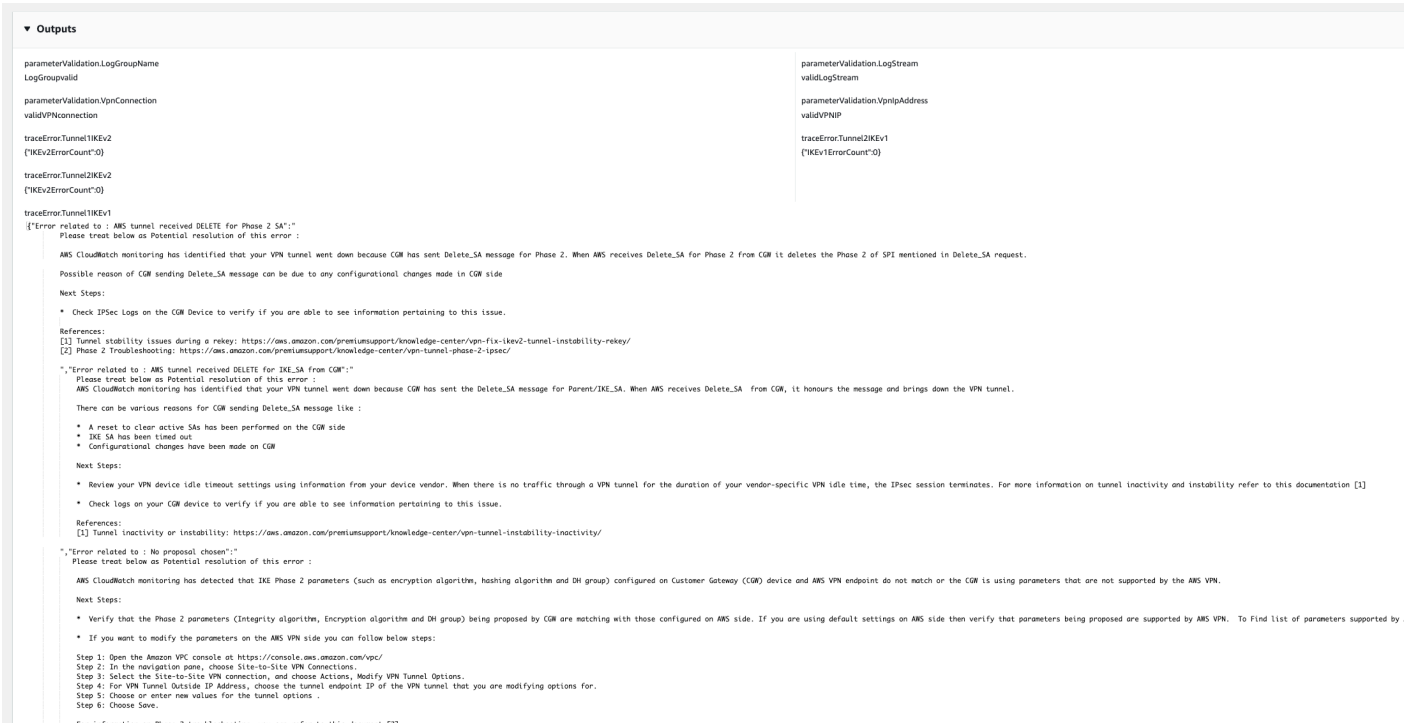
- branchOnValidationOfVpnIp:

  Verifica se l'indirizzo IP del tunnel menzionato nel parametro è valido o meno. Se non è valido, interrompe l'ulteriore esecuzione delle fasi di automazione.

- traceError:

  Effettua una API chiamata logs insight nel gruppo di CloudWatch log incluso e cerca l'errore relativo aIKEv1/IKEv2insieme a una relativa risoluzione suggerita.

6. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.



Riferimenti

Systems Manager Automation

- Esegui questa automazione (console)
- Esegui un'automazione
- Configurazione di un'automazione
- Pagina iniziale Support Automation Workflows

AWS documentazione di servizio

- Contenuto dei log da sito a sito VPN

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descrizione

Il `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` runbook elimina il gateway Internet di sola uscita specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- EgressOnlyInternetGatewayId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gateway Internet di sola uscita che desideri eliminare.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Fasi del documento

- `aws:executeScript`- Elimina il gateway Internet di sola uscita specificato nel parametro. `EgressOnlyInternetGatewayId`
- `aws:executeScript`- Verifica che il gateway Internet di sola uscita sia stato eliminato.

`AWSConfigRemediation-DeleteUnusedENI`

Descrizione

Il `AWSConfigRemediation-DeleteUnusedENI` runbook elimina un'elastic network interface (ENI) con uno stato di allegato pari a. `detached`

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- NetworkInterfaceId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del file ENI che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Fasi del documento

- `aws:executeAwsApi`- Elimina quanto ENI specificato nel parametro. `NetworkInterfaceId`
- `aws:executeScript`- Verifica che ENI sia stato eliminato.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descrizione

Il `AWSConfigRemediation-DeleteUnusedSecurityGroup` runbook elimina il gruppo di sicurezza specificato nel `GroupId` parametro. Se tenti di eliminare un gruppo di sicurezza associato a un'istanza Amazon Elastic Compute Cloud (AmazonEC2) o a cui fa riferimento un altro gruppo di sicurezza, l'automazione fallisce. Questa automazione non elimina un gruppo di sicurezza predefinito.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- GroupId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Fasi del documento

- `aws:executeAwsApi`- Restituisce il nome del gruppo di sicurezza utilizzando il valore fornito nel `GroupId` parametro.

- `aws:branch`- Conferma che il nome del gruppo non è «predefinito».
- `aws:executeAwsApi`- Elimina il gruppo di sicurezza specificato nel `GroupId` parametro.
- `aws:executeScript`- Conferma che il gruppo di sicurezza è stato eliminato.

`AWSConfigRemediation-DeleteUnusedVPCNetworkACL`

Descrizione

Il `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` runbook elimina una lista di controllo dell'accesso alla rete (ACL) che non è associata a una sottorete.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- NetworkAclId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della rete ACL che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Fasi del documento

- `aws:executeAwsApi`- Elimina la rete ACL specificata nel parametro. `NetworkAclId`
- `aws:executeScript`- Conferma che la rete ACL specificata nel `NetworkAclId` parametro è stata eliminata.

AWSConfigRemediation-DeleteVPCFlowLog

Descrizione

Il `AWSConfigRemediation-DeleteVPCFlowLog` runbook elimina il log di flusso del cloud privato virtuale (VPC) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- FlowLogId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del log di flusso che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Fasi del documento

- `aws:executeAwsApi`- Elimina il log di flusso specificato nel `FlowLogId` parametro.
- `aws:executeScript`- Verifica che il log di flusso sia stato eliminato.

`AWSConfigRemediation-DetachAndDeleteInternetGateway`

Descrizione

Il `AWSConfigRemediation-DetachAndDeleteInternetGateway` runbook scollega ed elimina il gateway Internet specificato. Se EC2 alcune istanze Amazon nel tuo cloud privato virtuale (VPC) hanno indirizzi IP elastici o IPv4 indirizzi pubblici associati, il runbook fallisce.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- InternetGatewayId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gateway Internet che desideri eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà di stato del gateway privato virtuale cambi `available` o scada.
- `aws:executeAwsApi`- Recupera una configurazione di gateway privato virtuale specificata.
- `aws:branch`- Rami basati sul VpcAttachments valore del parametro .state.

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà VpcAttachments .state del gateway privato virtuale cambi `attached` o scada.
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale e l'ID di Amazon VPC come input e scollega il gateway privato virtuale da AmazonVPC.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà VpcAttachments .state del gateway privato virtuale cambi `detached` o scada.

- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale come input e lo elimina.

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale come input e ne verifica l'eliminazione.

  `aws:executeAwsApi`- Raccoglie l'VPCID dall'ID del gateway Internet.
- `aws:executeAwsApi`- Rimuove l'ID del gateway Internet da. VPC
- `aws:executeAwsApi`- Elimina il gateway Internet.

`AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway`

Descrizione

Il `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` runbook scollega ed elimina un determinato gateway privato virtuale Amazon Elastic Compute Cloud (AmazonEC2) collegato a un cloud privato virtuale (VPC) creato con Amazon Virtual Private Cloud (Amazon). VPC

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- VpnGatewayId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gateway privato virtuale da eliminare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà di stato del gateway privato virtuale cambi `available` o scada.

- `aws:executeAwsApi`- Recupera una configurazione di gateway privato virtuale specificata.
- `aws:branch`- Rami basati sul VpcAttachments valore del parametro .state.

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà VpcAttachments .state del gateway privato virtuale cambi `attached` o scada.
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale e l'ID di Amazon VPC come input e scollega il gateway privato virtuale da AmazonVPC.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà VpcAttachments .state del gateway privato virtuale cambi `detached` o scada.

- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale come input e lo elimina.

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale come input e ne verifica l'eliminazione.

`AWS-DisableIncomingSSHOnPort22`

Descrizione

Il `AWS-DisableIncomingSSHOnPort22` runbook rimuove le regole che consentono il SSH traffico in entrata senza restrizioni sulla TCP porta 22 per i gruppi di sicurezza.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SecurityGroupIds

  Tipo: stringa

  Descrizione: (Obbligatorio) Un elenco separato da virgole IDs dei gruppi di sicurezza per i quali si desidera limitare il SSH traffico.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeAwsApi`- Rimuove tutte le regole che consentono SSH il traffico in entrata sulla TCP porta 22 dai gruppi di sicurezza specificati nel `SecurityGroupIds` parametro.

Output

DisableIncomingSSHTemplate. RestrictedSecurityGroupIds - Un elenco dei gruppi IDs di sicurezza a cui sono state rimosse SSH le regole in entrata.

AWS-DisablePublicAccessForSecurityGroup

Descrizione

Questo runbook disabilita le porte predefinite SSH e RDP le porte aperte a tutti gli indirizzi IP.

Important

Questo runbook fallisce con un ". InvalidPermission NotFound"errore per i gruppi di sicurezza che soddisfano entrambi i seguenti criteri: 1) Il gruppo di sicurezza si trova in una posizione non predefinitaVPC; e 2) Le regole in entrata per il gruppo di sicurezza non specificano le porte aperte utilizzando tutti e quattro i seguenti schemi:

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

Note

Questo runbook non è disponibile in Cina Regioni AWS .

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- GroupId

  Tipo: stringa

  Descrizione: (obbligatorio) ID del gruppo di sicurezza per il quale dovrebbero essere disabilitate le porte.

- IpAddressToBlock

  Tipo: stringa

  Descrizione: (Facoltativo) IPv4 Indirizzi aggiuntivi da cui bloccare l'accesso, nel formato. `1.2.3.4/32`

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descrizione

Il `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` runbook disabilita l'attributo IPv4 public address per la sottorete specificata.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- SubnetId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della sottorete su cui si desidera disabilitare l'attributo di assegnazione automatica dell'IPv4indirizzo pubblico.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Fasi del documento

- `aws:executeAwsApi`- Disattiva l'attributo di IPv4 indirizzo pubblico di assegnazione automatica per la sottorete specificata nel parametro. `SubnetId`
- `aws:assertAwsResourceProperty`- Verifica che l'attributo sia stato disabilitato.

AWSSupport-EnableVPCFlowLogs

Descrizione

Il `AWSSupport-EnableVPCFlowLogs` runbook crea log di flusso di Amazon Virtual Private Cloud (Amazon VPC) per sottoreti, interfacce di rete e VPC del tuo. Account AWS Se crei un log di flusso per una sottorete o un VPC, viene monitorata ogni interfaccia di rete elastica in quella sottorete o Amazon VPC. I dati del log di flusso vengono pubblicati nel gruppo di log Amazon CloudWatch Logs o nel bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Per ulteriori informazioni sui log di flusso, consulta VPC Flow Logs nella Amazon VPC User Guide.

> **Important**
>
> I costi di inserimento e archiviazione dei dati per i log venduti si applicano quando si pubblicano i log di flusso su Logs CloudWatch o su Amazon S3. Per ulteriori informazioni, consulta i prezzi di Flow Logs

Esegui questa automazione (console)

> **Note**
>
> Quando selezioni `s3` come destinazione del log, assicurati che la policy del bucket consenta al servizio di consegna dei log di accedere al bucket. Per ulteriori informazioni, consulta le autorizzazioni del bucket Amazon S3 per i log di flusso

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  -Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- DeliverLogsPermissionArn

  -Tipo: stringa

Descrizione: (Facoltativo) L'ARN per il ruolo IAM che consente ad Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute EC2) di pubblicare i log di flusso nel gruppo di log CloudWatch Logs del tuo account. Se specifichi il `LogDestinationType` parametro, non fornire un valore `s3` per questo parametro. Per ulteriori informazioni, consulta Publish flow logs to CloudWatch Logs nella Amazon VPC User Guide.

- LogDestinationARN

  ▬Tipo: stringa

  Descrizione: (Facoltativo) L'ARN della risorsa in cui vengono pubblicati i dati del log di flusso. Se `cloud-watch-logs` è specificato per il `LogDestinationType` parametro, fornisci l'ARN del gruppo di log CloudWatch Logs in cui desideri pubblicare i dati del log di flusso. In alternativa, utilizza `LogGroupName`. Se `s3` è specificato per il `LogDestinationType` parametro, è necessario specificare l'ARN del bucket Amazon S3 in cui si desidera pubblicare i dati del log di flusso per questo parametro. Puoi anche specificare una cartella nel bucket.

  > **Important**
  >
  > Quando scegli `s3` come bucket, assicurati che il bucket selezionato segua le best practice di sicurezza di Amazon S3 Bucket e che rispetti le leggi sulla privacy dei dati per la tua organizzazione e area geografica. `LogDestinationType`

- LogDestinationType

  ▬Tipo: stringa

  Valori validi: | s3 cloud-watch-logs

  Descrizione: (Obbligatorio) Determina dove vengono pubblicati i dati del log di flusso. Se specificate `LogDestinationType` ass3, non specificate `DeliverLogsPermissionArn` o`LogGroupName`.

- LogFormat

  ▬Tipo: stringa

  Descrizione: (Facoltativo) I campi da includere nel log di flusso e l'ordine in cui devono apparire nel record. Per un elenco dei campi disponibili, consulta Flow log records nella Amazon VPC User

Guide. Se non fornisci un valore per questo parametro, il log di flusso viene creato utilizzando il formato predefinito. Se specifichi questo parametro, è necessario specificare almeno un campo.

- LogGroupName

  - Tipo: stringa

  Descrizione: (Facoltativo) Il nome del gruppo di log CloudWatch Logs in cui vengono pubblicati i dati del log di flusso. Se si specifica `s3` il `LogDestinationType` parametro, non fornire un valore per questo parametro.

- ResourceIds

  Tipo: StringList

  Descrizione: (Obbligatorio) Un elenco separato da virgole degli ID per le sottoreti, le interfacce di rete elastiche o il VPC per cui si desidera creare un log di flusso.

- TrafficType

  - Tipo: stringa

  Valori validi: ACCEPT | REJECT | ALL

  Descrizione: (Obbligatorio) Il tipo di traffico da registrare. Puoi registrare il traffico che la risorsa accetta o rifiuta oppure tutto il traffico.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:CreatePolicy`

- iam:DeletePolicy
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:TagRole
- iam:PassRole
- iam:PutRolePolicy
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs:DeleteLogDelivery
- logs:DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

Politica di esempio

```
       {
           "Version": "2012-10-17",
           "Statement": [
               {
                   "Sid": "SSM Execution Permissions",
                   "Effect": "Allow",
                   "Action": [
```

```
                        "ssm:StartAutomationExecution",
                        "ssm:GetAutomationExecution"
                    ],
                    "Resource": "*"
                },
                {
                    "Sid": "EC2 FlowLogs Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:CreateFlowLogs",
                        "ec2:DeleteFlowLogs",
                        "ec2:DescribeFlowLogs"
                    ],
                    "Resource": "arn:{partition}:ec2:{region}:{account-id}:{instance|
subnet|vpc|transit-gateway|transit-gateway-attachment}/{resource ID}"
                },
                {
                    "Sid": "IAM CreateRole Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "iam:AttachRolePolicy",
                        "iam:CreateRole",
                        "iam:CreatePolicy",
                        "iam:DeletePolicy",
                        "iam:DeleteRole",
                        "iam:DeleteRolePolicy",
                        "iam:GetPolicy",
                        "iam:GetRole",
                        "iam:TagRole",
                        "iam:PassRole",
                        "iam:PutRolePolicy",
                        "iam:UpdateRole"
                    ],
                    "Resource": [
                        "arn:{partition}:iam::{account-id}:role/{role name}",
                        "arn:{partition}:iam::{account-id}:role/
AWSSupportCreateFlowLogsRole"
                    ]
                },
                {
                    "Sid": "CloudWatch Logs Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "logs:CreateLogDelivery",
```

```
                        "logs:CreateLogGroup",
                        "logs:DeleteLogDelivery",
                        "logs:DeleteLogGroup",
                        "logs:DescribeLogGroups",
                        "logs:DescribeLogStreams"
                    ],
                    "Resource": [
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}",
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}:*"
                    ]
                },
                {
                    "Sid": "S3 Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "s3:GetBucketLocation",
                        "s3:GetBucketPublicAccessBlock",
                        "s3:GetAccountPublicAccessBlock",
                        "s3:GetBucketPolicyStatus",
                        "s3:GetBucketAcl",
                        "s3:ListBucket",
                        "s3:PutObject"
                    ],
                    "Resource": [
                        "arn:{partition}:s3:::{bucket name}",
                        "arn:{partition}:s3:::{bucket name}/*"
                    ]
                }
            ]
        }
```

Fasi del documento

- `aws:branch`- Rami basati sul valore specificato per il `LogDestinationType` parametro.
- `aws:executeScript`- Verifica se l'Amazon Simple Storage Service (Amazon S3) di destinazione concede potenzialmente l'accesso in lettura o `public` scrittura ai suoi oggetti.
- `aws:executeScript`- Crea un gruppo di log se non viene specificato alcun valore per il `LogDestinationARN` parametro e `cloud-watch-logs` viene specificato per il `LogDestinationType` parametro.

- `aws:executeScript`- Crea registri di flusso in base ai valori specificati nei parametri del runbook.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Descrizione

Il `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook sostituisce un log di VPC flusso Amazon esistente che pubblica i dati del log di flusso su Amazon Simple Storage Service (Amazon S3) con un log di flusso che pubblica i dati del log di flusso nel gruppo di log CloudWatch Amazon CloudWatch Logs (Logs) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DestinationLogGroup

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del gruppo di log CloudWatch Logs in cui desideri pubblicare i dati del log di flusso.

- DeliverLogsPermissionArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN ruolo AWS Identity and Access Management (IAM) che desideri utilizzare che fornisce ad Amazon Elastic Compute Cloud (AmazonEC2) le autorizzazioni necessarie per pubblicare i dati del log di flusso su Logs. CloudWatch

- FlowLogId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del log di flusso pubblicato su Amazon S3 che desideri sostituire.

- MaxAggregationInterval

  Tipo: integer

  Valori validi: 60 | 600

  Descrizione: (Facoltativo) L'intervallo di tempo massimo, in secondi, durante il quale un flusso di pacchetti viene acquisito e aggregato in un record del log di flusso.

- TrafficType

  Tipo: stringa

  Valori validi: | | ACCEPT REJECT ALL

  Descrizione: (Obbligatorio) Il tipo di dati del log di flusso che si desidera registrare e pubblicare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'utente VPC dal valore specificato nel `FlowLogId` parametro.
- `aws:executeAwsApi`- Crea un log di flusso basato sui valori specificati per i parametri del runbook.
- `aws:assertAwsResourceProperty`- Verifica che il log di flusso appena creato venga pubblicato su Logs. CloudWatch
- `aws:executeAwsApi`- Elimina il log di flusso pubblicato su Amazon S3.
- `aws:executeScript`- Conferma che il log di flusso pubblicato su Amazon S3 è stato eliminato.

`AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket`

Descrizione

Il `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook sostituisce un log di VPC flusso Amazon esistente che pubblica i dati del log di flusso su Amazon CloudWatch Logs (CloudWatch Logs) con un log di flusso che pubblica i dati del log di flusso nel bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Destinazioni 3 BucketArn

  Tipo: stringa

  Descrizione: (Obbligatorio) Il ARN bucket Amazon S3 su cui desideri pubblicare i dati del log di flusso.

- FlowLogId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del log di flusso che viene pubblicato nei CloudWatch log che desideri sostituire.

- MaxAggregationInterval

  Tipo: integer

  Valori validi: 60 | 600

  Descrizione: (Facoltativo) L'intervallo di tempo massimo, in secondi, durante il quale un flusso di pacchetti viene acquisito e aggregato in un record del log di flusso.

- TrafficType

  Tipo: stringa

  Valori validi: | | ACCEPT REJECT ALL

  Descrizione: (Obbligatorio) Il tipo di dati del log di flusso che si desidera registrare e pubblicare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'utente VPC dal valore specificato nel `FlowLogId` parametro.
- `aws:executeAwsApi`- Crea un log di flusso basato sui valori specificati per i parametri del runbook.
- `aws:assertAwsResourceProperty`- Verifica la pubblicazione del log di flusso appena creato su Amazon S3.
- `aws:executeAwsApi`- Elimina il log di flusso che viene pubblicato su Logs. CloudWatch
- `aws:executeScript`- Conferma che il log di flusso pubblicato su CloudWatch Logs è stato eliminato.

`AWS-ReleaseElasticIP`

Descrizione

Rilascia l'indirizzo IP elastico specificato utilizzando ID allocazione.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- AllocationId

  Tipo: stringa

  Descrizione: (obbligatorio) l'ID allocazione dell'indirizzo IP elastico.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descrizione

Il AWS-RemoveNetworkACLUnrestrictedSSHRDP runbook rimuove tutte le regole della lista di controllo degli accessi alla rete (ACL) dalla rete specificata ACL che consentono il traffico in ingresso da tutti gli indirizzi di origine alle porte SSH e RDP alle impostazioni predefinite. Le regole che includono intervalli di porte che si sovrappongono a quelle predefinite SSH e le RDP porte non vengono rimosse.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- NetworkAclId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della rete ACL da cui si desidera rimuovere le regole illimitate che consentono il traffico in ingresso da tutti gli indirizzi di origine alle porte e alle impostazioni predefinite. SSH RDP

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Fasi del documento

- `aws:executeScript`- Rimuove tutte le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine del gruppo di sicurezza specificato nel `SecurityGroupId` parametro.

Output

RemoveNaclEntriesAndVerify. VerificationMessage - Messaggi di verifica delle ACL regole di rete eliminate con successo.

RemoveNaclEntriesAndVerify. RulesDeletedAndApiResponses - Le ACL regole di rete che sono state eliminate e le risposte `DeleteNetworkAclEntry` API operative.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Descrizione

Il `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` runbook rimuove tutte le regole di ingresso dal gruppo di sicurezza specificato che consentono il traffico da tutti gli indirizzi di origine.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- SecurityGroupId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza da cui desideri rimuovere le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeScript`- Rimuove tutte le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine del gruppo di sicurezza specificato nel `SecurityGroupId` parametro.

`AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules`

Descrizione

Il `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` runbook rimuove tutte le regole dal gruppo di sicurezza predefinito del cloud privato virtuale (VPC) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- GroupId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza da cui desideri rimuovere tutte le regole.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il gruppo di sicurezza specificato nel `GroupId` parametro è denominato default.
- `aws:executeScript`- Rimuove tutte le regole dal gruppo di sicurezza specificato nel `GroupId` parametro.

AWSSupport-SetupIPMonitoringFromVPC

Descrizione

`AWSSupport-SetupIPMonitoringFromVPC`crea un'istanza Amazon Elastic Compute Cloud (AmazonEC2) nella sottorete specificata e monitora la destinazione IPs (IPv4oIPv6) selezionata eseguendo continuamente test pingMTR, traceroute e tracetcp. I risultati vengono archiviati nei log di Amazon CloudWatch Logs e vengono applicati filtri metrici per visualizzare rapidamente le statistiche sulla latenza e sulla perdita di pacchetti in una dashboard. CloudWatch

Informazioni aggiuntive

I dati di CloudWatch Logs possono essere utilizzati per la risoluzione dei problemi di rete e l'analisi di pattern e tendenze. Inoltre, puoi configurare CloudWatch allarmi con le SNS notifiche di Amazon quando la perdita di pacchetti e/o la latenza raggiungono una soglia. I dati possono essere utilizzati anche per aprire un caso AWS Support, per aiutare a isolare rapidamente un problema e ridurre i tempi di risoluzione quando si indaga su un problema di rete.

> **Note**
>
> Per ripulire le risorse create da`AWSSupport-SetupIPMonitoringFromVPC`, puoi usare il runbook. `AWSSupport-TerminateIPMonitoringFromVPC` Per ulteriori informazioni, consulta `AWSSupport-TerminateIPMonitoringFromVPC`.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- CloudWatchLogGroupNamePrefix

  Tipo: stringa

Impostazione predefinita:/AWSSupport-SetupIPMonitoringFromVPC

Descrizione: (Facoltativo) Prefisso utilizzato per ogni gruppo di CloudWatch log creato per i risultati del test.

- CloudWatchLogGroupRetentionInDays

  Tipo: stringa

  Valori validi: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  Impostazione predefinita: 7

  Descrizione: (facoltativo) numero di giorni che definisce l'intervallo di tempo durante il quale si desidera conservare i risultati del monitoraggio della rete.

- InstanceType

  Tipo: stringa

  Valori validi: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

  Impostazione predefinita: t2.micro

  Descrizione: (EC2Facoltativo) EC2Rescue Il tipo di istanza per l'istanza. Dimensioni consigliate: t2.micro.

- SubnetId

  Tipo: stringa

  Descrizione: (obbligatorio) ID sottorete dell'istanza di monitoraggio. Tieni presente che se specifichi una sottorete privata, devi assicurarti che sia disponibile l'accesso a Internet per consentire all'istanza di monitoraggio di configurare il test (ovvero installare l'agente CloudWatch Logs, interagire con Systems Manager e CloudWatch).

- T argetIPs

  Tipo: stringa

  Descrizione: (Obbligatorio) Elenco separato da virgole di IPv4s e/o IPv6s da monitorare. Gli spazi non sono consentiti. La dimensione massima è pari a 255 caratteri. Se si specifica un indirizzo IP

non valido, l'automazione avrà esito negativo e verrà eseguito il rollback della configurazione dei test.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia di allegare la policy IAM gestita A mazonSSMAutomation Role all'utente che esegue l'automazione. L'utente deve inoltre disporre della seguente policy associata al proprio account utente, gruppo o ruolo:

```
            {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreateInstanceProfile",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:DetachRolePolicy",
                "iam:AttachRolePolicy",
                "iam:PassRole",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteRole",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::
                AWS_account_ID
                :role/AWSSupport/SetupIPMonitoringFromVPC_*",
                "arn:aws:iam::
                AWS_account_ID
                :instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
            ],
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "iam:DetachRolePolicy",
                "iam:AttachRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:DeleteDashboards"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstanceTypes",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceStatus"
                "ec2:CreateTags",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeTags",
                "ec2:DescribeInstances",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ssm:GetParameter",
                "ssm:SendCommand",
```

```
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Fasi del documento

1. **aws:executeAwsApi**- descrivi la sottorete fornita.
2. **aws:branch**- valuta l'argetIPs ingresso T.

   (IPv6) Se T argetIPs contiene unIPv6:

   aws:assertAwsResourceProperty- verifica che la sottorete fornita abbia un IPv6 pool associato
3. **aws:executeScript**- ottieni l'architettura del tipo di istanza e il percorso dei parametri pubblici per la versione più recente di Amazon Linux 2AMI.
4. **aws:executeAwsApi**- scarica la versione più recente di Amazon Linux 2 AMI da Parameter Store.
5. **aws:executeAwsApi**- crea un gruppo di sicurezza per il test nella sottorete. VPC

   (Pulizia) Se la creazione del gruppo di sicurezza ha esito negativo:

   aws:executeAwsApi- elimina il gruppo di sicurezza creato dall'automazione, se esiste.
6. **aws:executeAwsApi**- consentire tutto il traffico in uscita nel gruppo di sicurezza di test.

   (Pulizia) Se la creazione della regola in uscita del gruppo di sicurezza ha esito negativo:

   aws:executeAwsApi- elimina il gruppo di sicurezza creato dall'automazione, se esiste.
7. **aws:executeAwsApi**- creare un IAM ruolo per l'EC2istanza di test

   (Pulizia) Se la creazione del ruolo ha esito negativo:

   a. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione, se esiste.

b. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

8. **aws:executeAwsApi**- allegare la politica mazonSSMManaged InstanceCore gestita A

   (Pulizia) Se il collegamento della policy ha esito negativo:

   a. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione, se allegato.

   b. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

   c. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

9. **aws:executeAwsApi**- allega una politica in linea per consentire l'impostazione delle conservazioni dei gruppi di CloudWatch log e la creazione di una dashboard CloudWatch

   (Pulizia) Se il collegamento della policy inline ha esito negativo:

   a. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione, se creato.

   b. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

   c. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

   d. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

10. **aws:executeAwsApi**- creare un profilo di IAM istanza.

    (Pulizia) Se la creazione del profilo dell'istanza ha esito negativo:

    a. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione, se esiste.

    b. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

    c. **aws:executeAwsApi**- elimina la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

    d. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

    e. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

11. **aws:executeAwsApi**- associare il profilo dell'IAMistanza al IAM ruolo.

    (Pulizia) Se l'associazione tra profilo dell'istanza e ruolo ha esito negativo:

    a. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo, se associato.

    b. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione

c. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

d. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

12 **aws:sleep**- attendi che il profilo dell'istanza diventi disponibile.

13 **aws:runInstances**- crea l'istanza di test nella sottorete specificata e allegando il profilo di istanza creato in precedenza.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

14 **aws:branch**- valuta l'argetIPs ingresso T.

(IPv6) Se T argetIPs contiene unIPv6:

aws:executeAwsApi- IPv6 assegna an all'istanza di test.

15 **aws:waitForAwsResourceProperty**- attendi che l'istanza di test diventi un'istanza gestita.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

16 **aws:runCommand**- installa i prerequisiti di test:

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

17 **aws:runCommand**- verificare che gli indirizzi forniti IPs siano sintatticamente corretti e/o che gli indirizzi siano correttiIPv4: IPv6

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

18 **aws:runCommand**- definire il MTR test per ciascuno dei dati fornitiIPs.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

19 **aws:runCommand**- definire il primo test di ping per ciascuno dei test fornitiIPs.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

20 **aws:runCommand**- definire il secondo test di ping per ciascuno dei test fornitiIPs.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

21 **`aws:runCommand`**- definire il test tracepath per ciascuno dei test forniti. IPs

(Pulizia) Se la fase ha esito negativo:

a. **`aws:changeInstanceState`**- terminare l'istanza di test.

b. **`aws:executeAwsApi`**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **`aws:executeAwsApi`**- elimina il profilo di IAM istanza creato dall'automazione.

d. **`aws:executeAwsApi`**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **`aws:executeAwsApi`**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **`aws:executeAwsApi`**- elimina il IAM ruolo creato dall'automazione.

g. **`aws:executeAwsApi`**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

22 **`aws:runCommand`**- definire il test traceroute per ciascuno dei test forniti. IPs

(Pulizia) Se la fase ha esito negativo:

a. **`aws:changeInstanceState`**- terminare l'istanza di test.

b. **`aws:executeAwsApi`**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **`aws:executeAwsApi`**- elimina il profilo di IAM istanza creato dall'automazione.

d. **`aws:executeAwsApi`**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **`aws:executeAwsApi`**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **`aws:executeAwsApi`**- elimina il IAM ruolo creato dall'automazione.

g. **`aws:executeAwsApi`**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

23 **`aws:runCommand`**- configura CloudWatch i log.

(Pulizia) Se la fase ha esito negativo:

a. **`aws:changeInstanceState`**- terminare l'istanza di test.

b. **`aws:executeAwsApi`**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **`aws:executeAwsApi`**- elimina il profilo di IAM istanza creato dall'automazione.

d. **`aws:executeAwsApi`**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

24 **aws:runCommand**- pianifica i cronjob per eseguire ogni test ogni minuto.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

25 **aws:sleep**- attendi che i test generino dei dati.

26 **aws:runCommand**- imposta le conservazioni desiderate per i gruppi di CloudWatch log.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

27 **aws:runCommand**- imposta i filtri metrici del gruppo di CloudWatch log.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- termina l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

d. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

28 **aws:runCommand**- crea la CloudWatch dashboard.

(Pulizia) Se la fase ha esito negativo:

a. **aws:executeAwsApi**- elimina la CloudWatch dashboard, se esiste.

b. **aws:changeInstanceState**- terminare l'istanza di test.

c. **aws:executeAwsApi**- rimuove il profilo dell'IAMistanza dal ruolo.

d. **aws:executeAwsApi**- elimina il profilo di IAM istanza creato dall'automazione.

e. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il IAM ruolo creato dall'automazione.

h. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

Output

createCloudWatchDashboards.Output: il URL pannello di controllo. CloudWatch

createManagedInstance. InstanceIds - l'ID dell'istanza di test.

AWSSupport-TerminateIPMonitoringFromVPC

Descrizione

`AWSSupport-TerminateIPMonitoringFromVPC`termina un test di monitoraggio IP precedentemente avviato da. `AWSSupport-SetupIPMonitoringFromVPC` I dati relativi all'ID test specificato verranno eliminati.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- AutomationExecutionId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID di esecuzione dell'automazione utilizzato al momento dell'esecuzione precedente del `AWSSupport-SetupIPMonitoringFromVPC` runbook. Tutte le risorse associate a questo ID di esecuzione vengono eliminate.
- InstanceId

  Tipo: stringa

  Descrizione: (obbligatorio) ID istanza dell'istanza di monitoraggio.
- SubnetId

  Tipo: stringa

  Descrizione: (obbligatorio) ID sottorete dell'istanza di monitoraggio.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia di allegare la policy IAM gestita A mazonSSMAutomation Role all'utente che esegue l'automazione. Inoltre, l'utente deve avere la seguente politica allegata al proprio utente, gruppo o ruolo:

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Action": [
            "iam:DetachRolePolicy",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:DeleteRole",
            "iam:DeleteInstanceProfile",
            "iam:DeleteRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport/
SetupIPMonitoringFromVPC_*",
            "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport/
SetupIPMonitoringFromVPC_*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:DetachRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "cloudwatch:DeleteDashboards"
        ],
        "Resource": [
            "*"
```

```
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:DescribeTags",
            "ec2:DescribeInstances",
            "ec2:DescribeSecurityGroups",
            "ec2:DeleteSecurityGroup",
            "ec2:TerminateInstances",
            "ec2:DescribeInstanceStatus"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    ]
}
```

Fasi del documento

1. `aws:assertAwsResourceProperty`- InstanceId controllano AutomationExecutionId e sono correlati allo stesso test.
2. `aws:assertAwsResourceProperty`- InstanceId controllano SubnetId e sono correlati allo stesso test.
3. `aws:executeAwsApi`- recupera il gruppo di sicurezza del test.
4. `aws:executeAwsApi`- elimina la CloudWatch dashboard.
5. `aws:changeInstanceState`- terminare l'istanza di test.
6. `aws:executeAwsApi`- rimuove il profilo dell'IAMistanza dal ruolo.
7. `aws:executeAwsApi`- elimina il profilo di IAM istanza creato dall'automazione.
8. `aws:executeAwsApi`- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione.
9. `aws:executeAwsApi`- scollegare la politica mazonSSMManaged InstanceCore gestita A dal ruolo creato dall'automazione.
10. `aws:executeAwsApi`- elimina il IAM ruolo creato dall'automazione.
11. `aws:executeAwsApi`- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

Output

Nessuno

AWS WAF

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS WAF Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Descrizione

Il `AWS-AddWAFRegionalRuleToRuleGroup` runbook aggiunge una regola AWS WAF regionale esistente a un gruppo di regole AWS WAF regionali. Sono supportati solo i gruppi di regole regionali AWS WAF classici. AWS WAF I gruppi di regole regionali classici possono avere un massimo di 10 regole.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- RuleGroupId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del gruppo di regole che si desidera aggiornare.

- RulePriority

  Tipo: integer

  Descrizione: (Obbligatorio) La priorità per la nuova regola. La priorità delle regole determina l'ordine in cui vengono valutate le regole in un gruppo regionale. Le regole con un valore inferiore hanno una priorità maggiore rispetto alle regole con un valore più alto. Il valore deve essere un numero intero univoco. Se aggiungi più regole a un gruppo di regole regionali, i valori non devono essere consecutivi.

- RuleId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della regola che desideri aggiungere al gruppo di regole regionali.

- RuleAction

  Tipo: stringa

  Descrizione: (Obbligatorio) Specifica l' AWS WAF azione da eseguire quando una richiesta Web soddisfa le condizioni della regola.

  Valori validi: ALLOW | | BLOCK COUNT

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Fasi del documento

- G etWAFChange Token (aws:executeAwsApi) - Recupera un token di AWS WAF modifica per garantire che il runbook non invii richieste in conflitto al servizio.
- A ddWAFRule T oWAFRegional RuleGroup (aws:executeScript) - Aggiunge la regola specificata al gruppo di regole AWS WAF regionali.
- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty) - Verifica che il token di modifica abbia lo stato `PENDING` o`INSYNC`.
- VerifyRuleAddedToRuleGroup (aws:executeScript) - Verifica che la AWS WAF regola specificata sia stata aggiunta al gruppo di regole regionali di destinazione.

Output

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Risultato della fase di verifica dell'aggiunta della nuova regola al gruppo di regole regionali.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Risultato dell'`ListActivatedRulesInRuleGroup`APIoperazione.

AWS-AddWAFRegionalRuleToWebAcl

Descrizione

Il `AWS-AddWAFRegionalRuleToWebAcl` runbook aggiunge una regola AWS WAF regionale, un gruppo di regole o una regola basata sulla tariffa esistente a un elenco di controllo dell'accesso Web

regionale AWS WAF classico (). ACL Questo runbook non aggiorna i siti Web regionali AWS WAF Classic esistenti gestiti ACL da. AWS Firewall Manager

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- W ebACLId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del Web ACL che desideri aggiornare.
- ActivatedRulePriority

  Tipo: integer

  Descrizione: (Obbligatorio) La priorità per la nuova regola. La priorità delle regole determina l'ordine in cui ACL vengono valutate le regole in un Web. Le regole con un valore inferiore hanno una priorità maggiore rispetto alle regole con un valore più alto. Il valore deve essere un numero intero univoco. Se aggiungi più regole a un Web regionaleACL, i valori non devono essere consecutivi.
- ActivatedRuleRuleId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della regola normale, della regola basata sulla tariffa o del gruppo che desideri aggiungere al Web. ACL

- ActivatedRuleAction

  Tipo: stringa

  Valori validi: | | ALLOW BLOCK COUNT

  Descrizione: (Facoltativo) Specifica l' AWS WAF azione da eseguire quando una richiesta Web soddisfa le condizioni della regola.

- ActivatedRuleType

  Tipo: stringa

  Valori validi: REGULAR | RATE _ BASED | GROUP

  Predefinito: REGULAR

  Descrizione: (Facoltativo) Il tipo di regola che stai aggiungendo al WebACL. Sebbene questo campo sia facoltativo, tieni presente che se provi ad aggiungere una `RATE_BASED` regola a un Web ACL senza impostarne il tipo, la richiesta ha esito negativo perché per impostazione predefinita è una `REGULAR` regola.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Fasi del documento

- DetermineWebACLNotInFMSAndRulePriority(aws:executeScript) - Verifica se il AWS WAF Web ACL rientra in una politica di sicurezza di Firewall Manager e verifica che l'ID di priorità non sia in conflitto con uno esistente. ACL
- AddRuleOrRuleGroupToWebACL(aws:executeScript) - Aggiunge la regola specificata al AWS WAF Web. ACL
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:executeScript) - Verifica che la AWS WAF regola specificata sia stata aggiunta al web ACL di destinazione.

Output

- DetermineWebACLNotInFMSAndRulePriority. PrereqResponse: Uscita dalla `DetermineWebACLNotInFMSAndRulePriority` fase.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Uscita dalla `AddRuleOrRuleGroupToWebACL` fase.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Uscita del `VerifyRuleOrRuleGroupAddedToWebAcl` passo.

AWSConfigRemediation-EnableWAFClassicLogging

Descrizione

Il `AWSConfigRemediation-EnableWAFClassicLogging` runbook consente la registrazione su Amazon Data Firehose (Firehose) per AWS WAF la lista di controllo degli accessi Web (Web) specificata. ACL

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- DeliveryStreamName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome del flusso di distribuzione Firehose a cui si desidera inviare i log.
- W ebACLId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del AWS WAF Web a ACL cui desideri abilitare l'accesso.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Conferma il flusso di consegna specificato in `DeliveryStreamName` exists.
- `aws:executeAwsApi`- Raccoglie il ARN contenuto del AWS WAF web ACL specificato nel `WebACLId` parametro.

- `aws:executeAwsApi`- Abilita la registrazione per il Web. ACL
- `aws:assertAwsResourceProperty`- Verifica che la registrazione sia stata abilitata sul Web. AWS WAF ACL

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Descrizione

Il `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook consente la registrazione su Amazon Data Firehose (Firehose) per la lista di controllo degli AWS WAF accessi Web () specificata. ACL

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- LogDestinationConfigs

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del flusso di distribuzione Firehose a cui desideri inviare i log.

- W ebACLId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del AWS WAF Web a ACL cui desideri abilitare l'accesso.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il ARN contenuto del AWS WAF Web ACL specificato nel `WebACLId` parametro.
- `aws:executeAwsApi`- Abilita la registrazione per il Web. ACL
- `aws:assertAwsResourceProperty`- Verifica che la registrazione sia stata abilitata sul Web. AWS WAF ACL

AWSConfigRemediation-EnableWAFV2Logging

Descrizione

Il `AWSConfigRemediation-EnableWAFV2Logging` runbook consente la registrazione di una lista di controllo degli accessi Web AWS WAF (AWS WAF V2) (webACL) con il flusso di distribuzione Amazon Data Firehose (Firehose) specificato.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LogDestinationConfigs

  Tipo: stringa

  Descrizione: (Obbligatorio) Il flusso di distribuzione di Firehose ARN che desideri associare al Web. ACL

  > **Note**
  >
  > Il flusso di distribuzione di Firehose ARN deve iniziare con il prefisso. `aws-waf-logs-` Ad esempio, `aws-waf-logs-us-east-2-analytics`. Per ulteriori informazioni, consulta Amazon Data Firehose.

- WebAclArn

  Tipo: stringa

  Descrizione: (Obbligatoria) ARN del Web ACL per il quale verrà abilitata la registrazione.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Fasi del documento

- `aws:executeScript`- Abilita la registrazione per il Web AWS WAF V2 ACL e verifica che la registrazione abbia la configurazione specificata.

Amazon WorkSpaces

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. WorkSpaces Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

`AWS-CreateWorkSpace`

Descrizione

Il `AWS-CreateWorkSpace` runbook crea un nuovo desktop WorkSpaces virtuale Amazon, noto come a WorkSpace, in base ai valori specificati per i parametri di input. Per informazioni su WorkSpaces, consulta What is Amazon WorkSpaces? nella Amazon WorkSpaces Administration Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- BundleId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID del pacchetto da utilizzare per. WorkSpace
- ComputeTypeName

  Tipo: stringa

  Valori validi: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO GRAPHICSPRO

  Descrizione: (Facoltativo) Il tipo di calcolo per il tuo WorkSpace.
- DirectoryId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'ID della directory a cui WorkSpace aggiungere il tuo.
- RootVolumeEncryptionEnabled

  Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Determina se il volume principale di WorkSpace è crittografato.

- RootVolumeSizeGib

  Tipo: integer

  Descrizione: (Obbligatorio) La dimensione del volume radice per WorkSpace.

- RunningMode

  Tipo: stringa

  Valori validi: ALWAYS _ON | AUTO _ STOP

  Descrizione: (Obbligatorio) La modalità di esecuzione di WorkSpace.

- RunningModeAutoStopTimeoutInMinutes

  Tipo: integer

  Descrizione: (Facoltativo) Il tempo dopo che un utente si disconnette quando si WorkSpaces interrompe. Specificate un valore a intervalli di 60 minuti.

- Tag

  Tipo: stringa

  Descrizione: (Facoltativo) Tag che si desidera applicare a. WorkSpace

- UserName

  Tipo: stringa

  Descrizione: (Obbligatorio) Il nome utente da associare a WorkSpace.

- UserVolumeEncryptionEnabled

  Tipo: Booleano

  Valori validi: true | false

  Impostazione predefinita: false

Descrizione: (Facoltativo) Determina se il volume utente di WorkSpace è crittografato.

- UserVolumeSizeGib

  Tipo: integer

  Descrizione: (Obbligatorio) La dimensione del volume utente per WorkSpace.

- VolumeEncryptionKey

  Tipo: stringa

  Descrizione: (Facoltativo) La AWS Key Management Service chiave simmetrica che desideri utilizzare per crittografare i dati archiviati su. WorkSpace

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Fasi del documento

- `aws:executeScript`- Crea un WorkSpace file basato sui valori specificati per i parametri di input.
- `aws:waitForAwsResourceProperty`- Verifica lo stato di WorkSpace is`AVAILABLE`.

Output

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

Descrizione

Il `AWSSupport-RecoverWorkSpace` runbook esegue le fasi di ripristino sul desktop WorkSpaces virtuale Amazon, noto come a WorkSpace, specificato dall'utente. Il runbook riavvia e WorkSpace,

se lo stato è fermoUNHEALTHY, lo ripristina o ricostruisce in WorkSpace base ai valori specificati per i parametri di input. Prima di utilizzare questo runbook, ti consigliamo di consultare la sezione Troubleshooting WorkSpaces Issues nella Amazon WorkSpaces Administration Guide.

> **Important**
>
> Il ripristino o la ricostruzione di un WorkSpace è un'azione potenzialmente distruttiva che può causare la perdita di dati. Questo perché WorkSpace viene ripristinato dall'ultima istantanea disponibile e i dati recuperati dalle istantanee possono durare fino a 12 ore.
> L'opzione di ripristino ricrea sia il volume root che il volume utente in base alle istantanee più recenti. L'opzione rebuild ricrea il volume utente dall'istantanea più recente e ricrea quello WorkSpace dall'immagine associata al pacchetto da cui è stato creato. WorkSpace Le applicazioni installate o le impostazioni di sistema modificate dopo la WorkSpace creazione vengono perse. Per ulteriori informazioni sul ripristino e la ricostruzione WorkSpaces, consulta Restore a WorkSpace e Rebuild a WorkSpace nella Amazon WorkSpaces Administration Guide.

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Riconoscere

  Tipo: stringa

  Valori validi: Sì

  Descrizione: (Obbligatorio) Se si digita sì, si accetta che le azioni di ripristino e ricostruzione tenteranno di ripristinare l'istantanea più recente e che i dati ripristinati da queste istantanee possono durare fino a 12 ore. WorkSpace

- Riavvio

  Tipo: stringa

  Valori validi: Sì | No

  Impostazione predefinita: Sì

  Descrizione: (Obbligatorio) Determina se WorkSpace viene riavviato.

- Ricostruire

  Tipo: stringa

  Valori validi: Sì | No

  Predefinito: No

  Descrizione: (Obbligatorio) Determina se WorkSpace viene ricostruito.

- Ripristino

  Tipo: stringa

  Valori validi: Sì | No

  Predefinito: No

  Descrizione: (Obbligatorio) Determina se WorkSpace viene ripristinato.

- WorkspaceId

  Tipo: stringa

Descrizione: (Obbligatorio) L'ID del file che WorkSpace desideri ripristinare.

IAMAutorizzazioni richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie lo stato WorkSpace specificato nel `WorkspaceId` parametro.
- `aws:assertAwsResourceProperty`- Verifica lo stato di WorkSpace is`AVAILABLE`,, `ERROR` `IMPAIREDSTOPPED`, o. `UNHEALTHY`
- `aws:branch`- Filiali in base allo stato del WorkSpace.
- `aws:executeAwsApi`- Avvia il WorkSpace.
- `aws:branch`- Rami basati sul valore specificato per il `Action` parametro.
- `aws:waitForAwsResourceProperty`- Attende lo WorkSpace stato dopo l'avvio.
- `aws:waitForAwsResourceProperty`- Attende che lo WorkSpace stato cambi in`AVAILABLE`, `ERRORIMPAIRED`, o `UNHEALTHY` dopo l'avvio.
- `aws:executeAwsApi`- Raccoglie lo stato di WorkSpace dopo l'avvio.
- `aws:branch`- Filiali in base allo stato del WorkSpace dopo l'avvio.
- `aws:executeAwsApi`- Raccoglie le istantanee disponibili per il ripristino o la ricostruzione di. WorkSpace
- `aws:branch`- Rami basati sul valore specificato per il parametro. `Reboot`

- `aws:executeAwsApi`- Riavvia il. WorkSpace
- `aws:executeAwsApi`- Raccoglie lo stato di WorkSpace dopo l'avvio.
- `aws:waitForAwsResourceProperty`- Attende che lo stato del WorkSpace cambi. `REBOOTING`
- `aws:waitForAwsResourceProperty`- Attende che lo WorkSpace stato cambi o `UNHEALTHY` dopo `AVAILABLE` il `ERROR` riavvio.
- `aws:executeAwsApi`- Raccoglie lo stato di dopo il riavvio. WorkSpace
- `aws:branch`- Rami in base allo stato del dopo il WorkSpace riavvio.
- `aws:branch`- Rami basati sul valore specificato per il `Restore` parametro.
- `aws:executeAwsApi`- Ripristina il. WorkSpace Se il ripristino fallisce, il runbook tenta di ricostruire il. WorkSpace
- `aws:waitForAwsResourceProperty`- Attende che lo stato WorkSpace di. `RESTORING`
- `aws:waitForAwsResourceProperty`- Attende che lo WorkSpace stato cambi a `AVAILABLEERROR`, o `UNHEALTHY` dopo essere stato ripristinato.
- `aws:executeAwsApi`- Raccoglie lo stato di WorkSpace dopo il ripristino.
- `aws:branch`- Rami in base allo stato dell'ambiente WorkSpace dopo il ripristino.
- `aws:branch`- Rami basati sul valore specificato per il `Rebuild` parametro.
- `aws:executeAwsApi`- Ricostruisce il. WorkSpace
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cambi WorkSpace in. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Attende che lo WorkSpace stato cambi a `AVAILABLEERROR`, o `UNHEALTHY` dopo essere stato ricostruito.
- `aws:executeAwsApi`- Raccoglie lo stato di WorkSpace dopo la ricostruzione.
- `aws:assertAwsResourceProperty`- Conferma lo stato di is. WorkSpace `AVAILABLE`

X-Ray

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS X-Ray Per ulteriori informazioni sui runbook, consulta Working with runbook. Per informazioni su come visualizzare il contenuto dei runbook, consulta. Visualizza il contenuto del runbook

Argomenti

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

Descrizione

Il AWSConfigRemediation-UpdateXRayKMSKey runbook abilita la crittografia AWS X-Ray dei dati utilizzando una chiave AWS Key Management Service (AWS KMS). Questo runbook deve essere usato solo come base per garantire che AWS X-Ray i dati siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più set di dati con chiavi diverse. KMS

Esegui questa automazione (console)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- KeyId

  Tipo: stringa

  Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN), l'ID della chiave o l'alias della KMS chiave che desideri utilizzare AWS X-Ray per crittografare i dati.

Autorizzazioni richieste IAM

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia dei dati X-Ray utilizzando la KMS chiave specificata nel `KeyId` parametro.
- `aws:waitForAwsResourceProperty`- Attende lo stato di configurazione della crittografia dell'X-Ray. `ACTIVE`
- `aws:executeAwsApi`- Raccoglie ARN la chiave specificata nel parametro. `KeyId`
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata sul sistema X-Ray.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.