



亚马逊 GuardDuty 用户指南

Amazon GuardDuty



Amazon GuardDuty: 亚马逊 GuardDuty 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 GuardDuty ?	1
的特点 GuardDuty	1
PCIDSS合规	4
定价在 GuardDuty	4
使用 GuardDuty 30 天免费试用	4
使用 S3 的恶意软件防护，免费套餐为 12 个月	6
正在访问 GuardDuty	6
概念和术语	7
开始使用	11
开始前的准备工作	11
第 1 步：启用 Amazon GuardDuty	12
步骤 2：生成示例调查发现并浏览基本操作	14
步骤 3：配置将 GuardDuty 结果导出到 Amazon S3 存储桶	15
第 4 步：通过设置 GuardDuty 查找提醒 SNS	17
后续步骤	20
基础数据来源	21
AWS CloudTrail 管理事件	21
如何 GuardDuty 处理 AWS CloudTrail 全球事件	22
VPC 流日志	22
Route53 解析器DNS查询日志	23
GuardDuty 功能激活	24
功能激活	24
GuardDuty API改变	24
相比于数据来源的功能激活	25
了解功能激活的工作原理	25
合并功能激活更改	26
将 dataSources 映射到 features	26
S3 防护	29
如何 GuardDuty 使用 S3 数据事件	29
功能	30
AWS CloudTrail S3 的数据事件	30
为独立账户配置 S3 保护	30
启用或禁用 S3 保护	30
在多账户环境中配置 S3 保护	31

EKS保护	39
功能	39
EKS审计日志监控	39
EKS审计日志监控	39
为独立账户配置EKS审核日志监控	30
在多账户环境中配置EKS审计日志监控	41
运行时监控	48
工作方式	49
使用亚马逊EC2实例	50
使用 Fargate (仅限亚马逊)	52
使用亚马逊EKS集群	53
运行时监控配置后	54
30 天免费试用	54
我正在使用 GuardDuty 试用期或者我从未启用过EKS运行时监控	54
我在启动EKS运行时监控之前启用了运行时监控	55
关键概念-管理 GuardDuty 安全代理的方法	56
Fargate (ECS仅限亚马逊) 资源-管理 GuardDuty 安全代理的方法	56
Amazon EKS 集群-管理 GuardDuty 安全代理的方法	57
启用运行时监控	60
先决条件	61
独立账户的步骤	71
多账户环境的步骤	71
管理 GuardDuty 安全代理	75
配置EKS运行时监控 (API仅限)	177
为独立账户配置EKS运行时监控	177
为多EKS账户环境配置运行时监控	183
从EKS运行时监控迁移到运行时监控	215
检查EKS运行时监控配置状态	216
禁用EKS运行时监控	217
评估运行时间覆盖率	218
Amazon EC2 实例的覆盖范围	219
Amazon ECS 集群的覆盖范围	227
Amazon EKS 集群的覆盖范围	236
常见问题 (FAQs)	244
设置CPU和内存监控	247
收集的运行时事件类型	248

处理事件	248
容器事件	250
AWS Fargate (ECS仅限亚马逊) 任务事件	250
Kubernetes 容器组事件	251
DNS事件	251
公开事件	252
加载模块事件	252
Mprotect 事件	252
挂载事件	252
链接事件	253
符号链接事件	253
Dup 事件	253
内存映射事件	254
套接字事件	254
连接事件	254
进程 VM Readv 事件	255
进程 VM Writev 事件	255
Ptrace 事件	255
绑定事件	256
收听事件	256
重命名事件	257
设置UID事件	257
Chmod 事件	257
Amazon ECR 存储库托管 GuardDuty 代理	257
适用于EKS代理版本 1.6.0 及更高版本	258
适用于EKS代理版本 1.5.0 及更早版本	260
对于 AWS Fargate (ECS仅限亚马逊)	262
GuardDuty 代理发布历史记录	264
禁用的影响	276
清理安全代理资源的流程	278
恶意软件防护 EC2	279
功能	280
弹性块存储 (EBS) 卷	280
支持的EBS卷	281
修改默认KMS密钥 ID	282
恶意软件防护中的自定义设置 EC2	283

常规设置	283
使用用户定义的标签扫描选项	284
全局 GuardDutyExcluded 标签	287
GuardDuty-启动的恶意软件扫描	287
30 天免费试用	289
配置 GuardDuty启动的恶意软件扫描	289
调用 GuardDuty启动的恶意软件扫描的发现	300
按需恶意软件扫描	302
按需恶意软件扫描工作原理	302
开始使用	303
监控恶意软件扫描状态和结果	305
GuardDuty 服务账号	307
EC2配额恶意软件防护	309
S3 恶意软件防护	312
定价	313
工作方式	314
概述	314
IAM角色权限	314
根据扫描结果对对象进行可选标记	315
为存储桶启用 S3 恶意软件防护之后的处理	315
S3 恶意软件防护功能	316
(可选) 开始使用仅适用于 S3 的恶意软件防护 (控制台)	317
为您的存储桶配置 S3 的恶意软件防护	318
先决条件-创建或更新IAM角色策略	319
为存储桶的 S3 威胁检测启用恶意软件防护	323
启用 S3 恶意软件防护后的步骤	326
恶意软件防护计划资源状态	327
恶意软件防护计划故障排除状态详细信息	328
EventBridge 此 S3 存储桶的通知已禁用	328
EventBridge 缺少用于接收 S3 存储桶事件的托管规则	329
S3 存储桶已不存在	330
无法放置测试对象	330
在 S3 的恶意软件防护中进行监控	331
使用亚马逊 EventBridge	332
CloudWatch 用于监控扫描状态指标	340
使用 S3 对象标签	343

使用基于标签的访问控制 () TBAC	344
TBAC在 S3 存储桶上添加资源	345
为受保护存储桶编辑 S3 的恶意软件防护	346
查看使用量和成本	347
为受保护的存储桶禁用 S3 的恶意软件防护	347
亚马逊 S3 功能的可支持性	348
S3 恶意软件防护配额	355
RDS保护	358
支持的数据库	358
Prot RDS ection 如何使用RDS登录活动监控	359
功能	360
RDS登录活动监控	360
为独立账户配置RDS保护	360
在多RDS账户环境中配置保护	361
Lambda 保护	368
功能	368
Lambda 网络活动监控	368
配置 Lambda 保护	369
为独立账户配置 Lambda 保护	369
在多账户环境中配置 Lambda 保护	370
保护 AI 工作负载	377
管理多个账户	378
管理员账户和成员账户关系	378
使用 AWS Organizations管理账户	381
注意事项和建议	382
指定委派 GuardDuty 管理员账号所需的权限	383
指定委派 GuardDuty 管理员账号	384
更新组织自动启用首选项	386
向组织添加成员	389
(可选) 为现有成员账户启用保护计划	390
在内部维护您的组织 GuardDuty	391
更改委派 GuardDuty 管理员账号	392
通过邀请管理账户	393
通过邀请添加和管理账户	394
将 GuardDuty 管理员账户整合到单个组织委托 GuardDuty 管理员账户下	398
同时 GuardDuty 在多个账户中启用	400

了解调查发现	402
GuardDuty 查找格式	402
威胁目的	403
GuardDuty 恶意软件检测扫描引擎	405
示例发现结果	406
通过 GuardDuty 控制台生成样本调查结果或 API	406
测试 GuardDuty 结果	407
注意事项	408
GuardDuty 调查结果测试器脚本可以生成	408
步骤 1-先决条件	411
步骤 2-部署 AWS 资源	411
步骤 3-运行测试器脚本	413
步骤 4-清理 AWS 测试资源	415
常见问题疑难解答。	415
GuardDuty 调查结果的严重性级别	416
审查 GuardDuty调查结果	418
调查发现详细信息	419
调查发现概览	419
资源	420
RDS数据库 (DB) 用户详细信息	425
运行时监控查找详细信息	426
EBS卷扫描详细信息	427
用于EC2查找详细信息的恶意软件防护	428
S3 恶意软件防护查找详情	429
操作	430
行动者或目标	431
其他信息	431
证据	432
异常行为	432
GuardDuty 查找聚合	436
调查发现类型	437
EC2 调查发现类型	437
Backdoor:EC2/C&CActivity.B	439
Backdoor:EC2/C&CActivity.B!DNS	439
Backdoor:EC2/DenialOfService.Dns	440
Backdoor:EC2/DenialOfService.Tcp	441

Backdoor:EC2/DenialOfService.Udp	441
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	442
Backdoor:EC2/DenialOfService.UnusualProtocol	443
Backdoor:EC2/Spambot	443
Behavior:EC2/NetworkPortUnusual	444
Behavior:EC2/TrafficVolumeUnusual	444
CryptoCurrency:EC2/BitcoinTool.B	445
CryptoCurrency:EC2/BitcoinTool.B!DNS	445
DefenseEvasion:EC2/UnusualDNSResolver	446
DefenseEvasion:EC2/UnusualDoHActivity	446
DefenseEvasion:EC2/UnusualDoTActivity	447
Impact:EC2/AbusedDomainRequest.Reputation	447
Impact:EC2/BitcoinDomainRequest.Reputation	448
Impact:EC2/MaliciousDomainRequest.Reputation	448
Impact:EC2/PortSweep	449
Impact:EC2/SuspiciousDomainRequest.Reputation	449
Impact:EC2/WinRMBruteForce	450
Recon:EC2/PortProbeEMRUnprotectedPort	451
Recon:EC2/PortProbeUnprotectedPort	451
Recon:EC2/Portscan	452
Trojan:EC2/BlackholeTraffic	453
Trojan:EC2/BlackholeTraffic!DNS	453
Trojan:EC2/DGADomainRequest.B	453
Trojan:EC2/DGADomainRequest.C!DNS	454
Trojan:EC2/DNSDataExfiltration	455
Trojan:EC2/DriveBySourceTraffic!DNS	455
Trojan:EC2/DropPoint	456
Trojan:EC2/DropPoint!DNS	456
Trojan:EC2/PhishingDomainRequest!DNS	457
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	457
UnauthorizedAccess:EC2/MetadataDNSRebind	458
UnauthorizedAccess:EC2/RDPBruteForce	458
UnauthorizedAccess:EC2/SSHBruteForce	459
UnauthorizedAccess:EC2/TorClient	460
UnauthorizedAccess:EC2/TorRelay	461
IAM查找类型	461

CredentialAccess:IAMUser/AnomalousBehavior	462
DefenseEvasion:IAMUser/AnomalousBehavior	463
Discovery:IAMUser/AnomalousBehavior	463
Exfiltration:IAMUser/AnomalousBehavior	464
Impact:IAMUser/AnomalousBehavior	465
InitialAccess:IAMUser/AnomalousBehavior	465
PenTest:IAMUser/KaliLinux	466
PenTest:IAMUser/ParrotLinux	466
PenTest:IAMUser/PentooLinux	467
Persistence:IAMUser/AnomalousBehavior	467
Policy:IAMUser/RootCredentialUsage	468
PrivilegeEscalation:IAMUser/AnomalousBehavior	468
Recon:IAMUser/MaliciousIPCaller	469
Recon:IAMUser/MaliciousIPCaller.Custom	469
Recon:IAMUser/TorIPCaller	470
Stealth:IAMUser/CloudTrailLoggingDisabled	470
Stealth:IAMUser/PasswordPolicyChange	471
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	471
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	472
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	473
UnauthorizedAccess:IAMUser/MaliciousIPCaller	474
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	474
UnauthorizedAccess:IAMUser/TorIPCaller	475
S3 调查发现类型	475
Discovery:S3/AnomalousBehavior	477
Discovery:S3/MaliciousIPCaller	477
Discovery:S3/MaliciousIPCaller.Custom	478
Discovery:S3/TorIPCaller	478
Exfiltration:S3/AnomalousBehavior	479
Exfiltration:S3/MaliciousIPCaller	479
Impact:S3/AnomalousBehavior.Delete	480
Impact:S3/AnomalousBehavior.Permission	480
Impact:S3/AnomalousBehavior.Write	481
Impact:S3/MaliciousIPCaller	481
PenTest:S3/KaliLinux	482
PenTest:S3/ParrotLinux	482

PenTest:S3/Pentoolinux	483
Policy:S3/AccountBlockPublicAccessDisabled	483
Policy:S3/BucketAnonymousAccessGranted	484
Policy:S3/BucketBlockPublicAccessDisabled	484
Policy:S3/BucketPublicAccessGranted	485
Stealth:S3/ServerAccessLoggingDisabled	486
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	486
UnauthorizedAccess:S3/TorIPCaller	487
EKS审核日志查找类型	487
CredentialAccess:Kubernetes/MaliciousIPCaller	489
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	489
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	490
CredentialAccess:Kubernetes/TorIPCaller	491
DefenseEvasion:Kubernetes/MaliciousIPCaller	491
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	492
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	492
DefenseEvasion:Kubernetes/TorIPCaller	493
Discovery:Kubernetes/MaliciousIPCaller	493
Discovery:Kubernetes/MaliciousIPCaller.Custom	494
Discovery:Kubernetes/SuccessfulAnonymousAccess	494
Discovery:Kubernetes/TorIPCaller	495
Execution:Kubernetes/ExecInKubeSystemPod	496
Impact:Kubernetes/MaliciousIPCaller	496
Impact:Kubernetes/MaliciousIPCaller.Custom	497
Impact:Kubernetes/SuccessfulAnonymousAccess	497
Impact:Kubernetes/TorIPCaller	498
Persistence:Kubernetes/ContainerWithSensitiveMount	498
Persistence:Kubernetes/MaliciousIPCaller	499
Persistence:Kubernetes/MaliciousIPCaller.Custom	499
Persistence:Kubernetes/SuccessfulAnonymousAccess	500
Persistence:Kubernetes/TorIPCaller	500
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	501
Policy:Kubernetes/AnonymousAccessGranted	501
Policy:Kubernetes/ExposedDashboard	502
Policy:Kubernetes/KubeflowDashboardExposed	502
PrivilegeEscalation:Kubernetes/PrivilegedContainer	503

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	503
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	504
Execution:Kubernetes/AnomalousBehavior.ExecInPod	505
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed! PrivilegedContainer	505
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount	506
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	507
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	508
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	509
运行时监控查找类型	509
CryptoCurrency:Runtime/BitcoinTool.B	511
Backdoor:Runtime/C&CActivity.B	512
UnauthorizedAccess:Runtime/TorRelay	512
UnauthorizedAccess:Runtime/TorClient	513
Trojan:Runtime/BlackholeTraffic	513
Trojan:Runtime/DropPoint	514
CryptoCurrency:Runtime/BitcoinTool.B!DNS	514
Backdoor:Runtime/C&CActivity.B!DNS	515
Trojan:Runtime/BlackholeTraffic!DNS	516
Trojan:Runtime/DropPoint!DNS	516
Trojan:Runtime/DGADomainRequest.C!DNS	517
Trojan:Runtime/DriveBySourceTraffic!DNS	518
Trojan:Runtime/PhishingDomainRequest!DNS	518
Impact:Runtime/AbusedDomainRequest.Reputation	519
Impact:Runtime/BitcoinDomainRequest.Reputation	519
Impact:Runtime/MaliciousDomainRequest.Reputation	520
Impact:Runtime/SuspiciousDomainRequest.Reputation	521
UnauthorizedAccess:Runtime/MetadataDNSRebind	521
Execution:Runtime/NewBinaryExecuted	522
PrivilegeEscalation:Runtime/DockerSocketAccessed	523
PrivilegeEscalation:Runtime/RuncContainerEscape	523
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	524
DefenseEvasion:Runtime/ProcessInjection.Proc	525
DefenseEvasion:Runtime/ProcessInjection.Ptrace	525
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	526

Execution:Runtime/ReverseShell	526
DefenseEvasion:Runtime/FilelessExecution	527
Impact:Runtime/CryptoMinerExecuted	527
Execution:Runtime/NewLibraryLoaded	528
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	528
PrivilegeEscalation:Runtime/UserfaultfdUsage	529
Execution:Runtime/SuspiciousTool	529
Execution:Runtime/SuspiciousCommand	530
DefenseEvasion:Runtime/SuspiciousCommand	531
DefenseEvasion:Runtime/PtraceAntiDebugging	531
Execution:Runtime/MaliciousFileExecuted	532
Execution:Runtime/SuspiciousShellCreated	532
PrivilegeEscalation:Runtime/ElevationToRoot	533
适用于 EC2 查找类型的恶意软件防护	533
Execution:EC2/MaliciousFile	534
Execution:ECS/MaliciousFile	535
Execution:Kubernetes/MaliciousFile	535
Execution:Container/MaliciousFile	536
Execution:EC2/SuspiciousFile	536
Execution:ECS/SuspiciousFile	537
Execution:Kubernetes/SuspiciousFile	537
Execution:Container/SuspiciousFile	538
适用于 S3 查找类型的恶意软件防护	538
Object:S3/MaliciousFile	539
RDS 保护查找类型	539
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	540
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	541
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	541
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	542
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	542
Discovery:RDS/MaliciousIPCaller	543
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	543
CredentialAccess:RDS/TorIPCaller.FailedLogin	544
Discovery:RDS/TorIPCaller	544
Lambda Protection 查找类型	545
Backdoor:Lambda/C&CActivity.B	545

CryptoCurrency:Lambda/BitcoinTool.B	546
Trojan:Lambda/BlackholeTraffic	546
Trojan:Lambda/DropPoint	547
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	547
UnauthorizedAccess:Lambda/TorClient	548
UnauthorizedAccess:Lambda/TorRelay	548
停用调查结果类型	548
Exfiltration:S3/ObjectRead.Unusual	549
Impact:S3/PermissionsModification.Unusual	550
Impact:S3/ObjectDelete.Unusual	551
Discovery:S3/BucketEnumeration.Unusual	551
Persistence:IAMUser/NetworkPermissions	552
Persistence:IAMUser/ResourcePermissions	552
Persistence:IAMUser/UserPermissions	553
PrivilegeEscalation:IAMUser/AdministrativePermissions	554
Recon:IAMUser/NetworkPermissions	554
Recon:IAMUser/ResourcePermissions	555
Recon:IAMUser/UserPermissions	556
ResourceConsumption:IAMUser/ComputeResources	556
Stealth:IAMUser/LoggingConfigurationModified	557
UnauthorizedAccess:IAMUser/ConsoleLogin	557
UnauthorizedAccess:EC2/TorIPCaller	558
Backdoor:EC2/XORDDOS	558
Behavior:IAMUser/InstanceLaunchUnusual	559
CryptoCurrency:EC2/BitcoinTool.A	559
UnauthorizedAccess:IAMUser/UnusualASNCaller	560
按资源类型列出的调查发现	560
调查发现表	560
管理 GuardDuty 调查结果	588
Summary	589
访问摘要控制面板	589
了解摘要控制面板	590
提供有关摘要控制面板的反馈	592
筛选调查发现	593
在 GuardDuty 控制台中创建过滤器	593
筛选条件属性	594

抑制规则	600
.....	600
抑制规则的常见用例和示例	601
创建抑制规则	604
删除抑制规则	606
.....	605
可信 IP 列表和威胁列表	607
列表格式	608
上传可信 IP 列表和威胁列表所需的权限	611
对可信 IP 列表和威胁列表使用服务器端加密	612
添加和激活可信 IP 列表或威胁 IP 列表	612
更新可信 IP 列表和威胁列表	614
停用或删除可信 IP 列表或威胁列表	615
导出调查发现	617
注意事项	617
步骤 1-导出调查结果所需的权限	618
第 2 步 — 将策略附加到您的密钥 KMS	618
第 3 步 — 将策略附加到 Amazon S3 存储桶	620
步骤 4-将调查结果导出到 S3 存储桶 (控制台)	623
步骤 5-导出调查结果的频率	625
使用 CloudWatch 事件自动响应	625
CloudWatch 的事件通知频率 GuardDuty	626
CloudWatch 的事件格式 GuardDuty	627
创建 CloudWatch 事件规则以通知您 GuardDuty 发现的结果 (控制台)	628
为 GuardDuty (CLI) 创建 CloudWatch 事件规则和目标	633
CloudWatch GuardDuty 多账户环境的事件	635
了解 CloudWatch 日志和跳过资源的原因	636
审计 EC2 GuardDuty 恶意软件防护中的 CloudWatch 日志	636
GuardDuty EC2 日志保留的恶意软件防护	637
跳过资源的原因	637
在 EC2 恶意软件防护中报告误报	640
误报文件提交	640
修复调查发现	642
修复可能遭到入侵的 Amazon 实例 EC2	642
修复可能遭到入侵的 S3 存储桶	643
基于特定 S3 存储桶访问需求的建议	645

修复可能有恶意的 S3 对象	645
修复可能受损的集群 ECS	646
修复可能被泄露的凭证 AWS	646
修复可能受损的独立容器	647
修复 EKS 审计日志监控调查发现	648
潜在的配置问题	649
修复可能受到威胁的 Kubernetes 用户	649
修复可能遭到入侵的 Kubernetes 吊舱	652
修复可能受损的容器镜像	653
修复可能受到威胁的 Kubernetes 节点	654
修复运行时监控结果	654
修复被盗用的容器映像	656
修复可能受损的数据库	656
通过成功登录事件修复可能受攻击的数据库	657
通过失败登录事件修复可能受攻击的数据库	657
修复可能遭泄露的凭证	658
限制网络访问	659
修复可能受损的 Lambda 函数	659
估算成本	661
了解如何 GuardDuty 计算使用成本	661
.....	662
运行时监控 — 来自EC2实例的VPC流日志如何影响使用成本	662
如何 GuardDuty 估算 CloudTrail 活动的使用成本	662
查看 GuardDuty 使用情况统计信息	662
安全性	665
数据保护	665
静态加密	666
传输中加密	666
选择不使用您的数据来改善服务	666
使用登录 CloudTrail	668
GuardDuty 信息在 CloudTrail	668
GuardDuty 控制飞机事件 CloudTrail	669
GuardDuty 中的数据事件 CloudTrail	669
示例：GuardDuty 日志文件条目	670
Identity and Access Management	672
受众	673

使用身份进行身份验证	673
使用策略管理访问	676
亚马逊是如何 GuardDuty 与之合作的 IAM	678
基于身份的策略示例	683
使用服务相关角色	691
AWS 托管策略	710
故障排除	718
合规性验证	719
故障恢复能力	720
基础设施安全性	720
与其他 AWS 服务集成	722
GuardDuty 与集成 AWS Security Hub	722
GuardDuty 与 Amazon Detective 集成	722
AWS Security Hub 整合	722
亚马逊如何 GuardDuty 将调查结果发送至 AWS Security Hub	723
在中查看 GuardDuty 调查结果 AWS Security Hub	724
启用和配置集成	741
在 Security Hub 中使用 GuardDuty 控件	742
停止向 Security Hub 发布调查发现	742
亚马逊 Detective 集成	742
启用集成	742
从一项发现转向 Amazon Detective GuardDuty	743
使用与 GuardDuty多账户环境的集成	743
暂停或禁用	745
GuardDuty 公告	746
Amazon SNS 消息格式	751
配额	756
故障排除	759
中的一般问题 GuardDuty	759
导出 GuardDuty 结果时出现访问错误。我该如何解决这个问题？	759
EC2 问题的恶意软件防护	759
我正在启动按需恶意软件扫描，但出现了缺少所需权限错误。	759
我在使用 EC2 恶意软件防护时收到iam:GetRole错误。	760
我是 GuardDuty 管理员帐户，需要启用 GuardDuty启动的恶意软件扫描，但不使用 AWS 托管策略：AmazonGuardDutyFullAccess进行管理 GuardDuty。	760
运行时监控问题	760

我的 AWS Step Functions 工作流程意外失败	760
排除内存不足错误	760
管理多个账户问题	761
我想管理多个账户，但没有所需的 AWS Organizations 管理权限。	761
对其他问题进行故障排除	761
区域和端点	762
特定于区域的功能可用性	762
旧版操作和参数	764
文档历史记录	765
早期更新	810
.....	dcccxix

什么是亚马逊 GuardDuty ?

Amazon GuardDuty 是一项威胁检测服务，可持续监控、分析和处理您 AWS 环境中的 AWS 数据源和日志。GuardDuty 使用威胁情报源（例如恶意 IP 地址和域名列表、文件哈希和机器学习 (ML) 模型）来识别 AWS 环境中的可疑活动和潜在的恶意活动。以下列表概述了 GuardDuty 可以帮助您检测的潜在威胁场景：

- 凭据被泄露和泄露。AWS
- 可能导致勒索软件事件的数据泄露和破坏。Amazon Aurora 和 Amazon RDS 数据库支持的引擎版本中的异常登录事件模式表明存在异常行为。
- 您的亚马逊弹性计算云 (AmazonEC2) 实例和容器工作负载中未经授权的加密采矿活动。
- 您的亚马逊EC2实例和容器工作负载中存在恶意软件，您的亚马逊简单存储服务 (Amazon S3) 存储桶中存在新上传的文件。
- 操作系统级、联网和文件事件，表明您的亚马逊 Elastic Kubernetes Service (Amazon) 集群、EKS 亚马逊弹性容器服务 ECS (Amazon AWS Fargate (Fargate))-任务以及亚马逊实例EC2和容器工作负载存在未经授权的行为。

[什么是亚马逊 GuardDuty](#)

内容

- [的特点 GuardDuty](#)
- [PCIDSS合规](#)
- [定价在 GuardDuty](#)
- [正在访问 GuardDuty](#)

的特点 GuardDuty

以下是 Amazon GuardDuty 可以帮助您监控、检测和管理 AWS 环境中潜在威胁的一些主要方式。

持续监控特定的数据源和事件日志

- **基础威胁检测** — 当您在 GuardDuty 中启用时 AWS 账户，GuardDuty 会自动开始提取与该账户关联的基础数据源。这些数据源包括 AWS CloudTrail 管理事件、VPC流日志（来自 Amazon

EC2 实例) 和 DNS 日志。您无需启用任何其他功能即可开始分析和处理这些数据源以生成相关的安全调查结果。GuardDuty 有关更多信息，请参阅 [GuardDuty 基础数据源](#)。

- 以@@ 用例为重点的 GuardDuty 保护计划 — 为了增强威胁检测对 AWS 环境安全的可见性，GuardDuty 提供您可以选择启用的专用保护计划。保护计划可帮助您监控来自其他 AWS 服务的日志和事件。这些来源包括 EKS 审计日志、RDS 登录活动、中的 Amazon S3 数据事件 CloudTrail、EBS 卷、跨亚马逊 EKS、亚马逊和亚马逊 ECS-Fargate 的运行时监控以及 Lambda 网络活动日志。EC2 GuardDuty 在“功能”一词下整合这些日志和事件源。您可以随时在支持的 AWS 区域中启用一个或多个专用保护计划。GuardDuty 将根据您启用的保护计划开始监控、处理和分析活动。有关每项保护计划及其运作方式的更多信息，请参阅相应的保护计划文档。

保护计划	描述
S3 防护	识别潜在的安全风险，例如您的 Amazon S3 存储桶中的数据泄露和破坏企图。
EKS 保护	EKS 审计日志监控会分析来自您的 Amazon EKS 集群的 Kubernetes 审计日志，以发现潜在的可疑和恶意活动。
运行时监控	监控和分析您的亚马逊 EKS、亚马逊和亚马逊 ECS (包括 AWS Fargate) 上的操作系统级事件，以检测潜在的运行时威胁。EC2
恶意软件防护 EC2	通过扫描与您的 Amazon EC2 实例关联的 Amazon EBS 卷，检测可能存在的恶意软件。可以选择按需使用此功能。
S3 恶意软件防护	检测您的 Amazon S3 存储桶中新上传的对象中可能存在恶意软件。
RDS 保护	分析和分析您的 RDS 登录活动，以了解受支持的 Amazon Aurora 和 Amazon RDS 数据库是否存在潜在的访问威胁。
Lambda 保护	监控 Lambda 网络活动日志 (从 VPC 流日志开始) ，以检测对您的 AWS Lambda 函数的威胁。这些潜在威胁的示例包括加密挖矿和与恶意服务器通信。

i 单独为 S3 启用恶意软件防护

GuardDuty 无需启用 Amazon GuardDuty 服务，即可灵活地独立使用 S3 的恶意软件防护。有关开始使用仅适用于 S3 的恶意软件防护的更多信息，请参阅[GuardDuty S3 恶意软件防护](#)。要使用所有其他保护计划，必须启用该 GuardDuty 服务。

管理多账户环境

您可以使用 AWS Organizations（推荐）或旧版邀请方法来管理多账户 AWS 环境。有关更多信息，请参阅[管理多个账户](#)。

针对检测到的威胁生成安全调查结果

当 GuardDuty 检测到与您的 AWS 资源相关的潜在安全威胁时，它会开始生成安全调查结果，以提供有关可能受到威胁的资源的信息。GuardDuty 在您的账户中启用后，生成[示例发现结果](#)以查看关联的[调查发现详细信息](#)。有关安全发现的完整列表，请参阅[调查发现类型](#)。

借 GuardDuty 助，您还可以使用生成特定 GuardDuty 安全发现结果的测试脚本来了解如何查看和响应 GuardDuty 调查结果。有关更多信息，请参阅[专用账户中的测试 GuardDuty 结果](#)。

评估和管理安全调查结果

GuardDuty 整合各个账户的安全调查结果，并在控制台的“摘要”控制面板中显示结果。GuardDuty 您也可以通过 AWS Security Hub API、AWS Command Line Interface、或检索搜索结果 AWS SDK。通过对当前安全状态的全面了解，您可以识别趋势和潜在问题，并采取必要的补救措施。有关更多信息，请参阅[管理 GuardDuty 调查结果](#)。

与相关 AWS 安全服务集成

为了进一步帮助您分析和调查 AWS 环境中的安全趋势，请考虑将以下 AWS 与安全相关的服务与 GuardDuty 结合使用。

- AWS Security Hub— 此服务可让您全面了解 AWS 资源的安全状态，并帮助您根据安全行业标准和最佳实践检查您的 AWS 环境。其部分原因是使用、汇总、整理来自多种 AWS 服务（包括 Amazon Macie）和 AWS 支持的合作伙伴网络 APN（）产品的安全调查结果，并对其进行优先排序。Security Hub 可帮助您分析安全趋势，确定 AWS 环境中优先级最高的安全问题。

有关同时使用 GuardDuty 和 Security Hub 的信息，请参阅[GuardDuty 与集成 AWS Security Hub](#)。要了解有关 Security Hub 的更多信息，请参阅[AWS Security Hub 用户指南](#)。

- Amazon Detective — 此服务可帮助您分析、调查并快速确定安全发现或可疑活动的根本原因。Detective 会自动从您的 AWS 资源中收集日志数据。然后，它使用机器学习、统计分析和图

形理论生成可视化效果，帮助更快、更高效地进行安全调查。Detective 预建的数据聚合、摘要和上下文可帮助您分析和确定潜在安全问题的性质和程度。

有关同时使用 GuardDuty 和 Detective 的信息，请参阅 [GuardDuty 与 Amazon Detective 集成](#)。要了解有关 Detective 的更多信息，请参阅 [Amazon Detective 用户指南](#)。

- Amazon EventBridge — 该服务可帮助您近乎实时地接收通知并对 GuardDuty 安全发现作出回应。GuardDuty 当发现结果发生变化时创建事件。您可以选择接收通知的频率 EventBridge。有关更多信息，请参阅《[亚马逊 EventBridge 用户指南](#)》EventBridge 中的“[什么是亚马逊](#)”。

PCIDSS 合规

GuardDuty 支持商家或服务提供商处理、存储和传输信用卡数据，并且已被验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。有关更多信息 PCIDSS，包括如何索取 Compliance Packag AWS PCI e 的副本，请参阅 [PCIDSS 级别 1](#)。

有关更多信息，请参阅 AWS 安全博客中的 [新第三方测试 GuardDuty 将 Amazon 与网络入侵检测系统进行了比较](#)。

定价在 GuardDuty

AWS Free Tier 可帮助您 AWS 服务 免费探索和试用每项服务的指定限制。共有三个类别：12 个月免费试用、永久免费试用和短期免费试用。Amazon GuardDuty 属于短期免费试用类别，提供 30 天免费试用。当您在免费试用期结束 GuardDuty 后继续使用时，将根据您使用此服务的方式开始产生费用。

按需恶意软件扫描（在“恶意软件防护”下 EC2）和 S3 恶意软件防护不属于 GuardDuty 30 天短期免费试用类别。S3 的恶意软件防护属于 12 个月的免费类别，AWS Free Tier 而按需恶意软件扫描则遵循 pay-as-you-use 成本模式。没有 30 天免费试用，也没有 12 个月的免费套餐费用模式（带按需恶意软件扫描）。有关更多信息，请参阅 [GuardDuty 定价](#)。

使用 GuardDuty 30 天免费试用

首次在中使用 GuardDuty 时 AWS 区域，系统会自动注册该地区的 30 天免费试用。AWS 账户一些保护计划还将自动启用，并包含在 30 天免费试用期中。由于 GuardDuty 是一项区域性服务，因此当您在其他地区首次启用该服务时，您的账户将获得 30 天免费试用，GuardDuty 并在该地区获得一些支持的保护计划。

在 GuardDuty 组织中使用多个帐户时，每个账户都有自己的 30 天免费试用版 GuardDuty 和防护计划。

下表显示了首次启用时会自动启用 GuardDuty 哪些保护计划。

保护计划	包含在 GuardDuty 30 天免费试用中	有自己的 30 天免费试用 ¹
EKS保护	是	是
Lambda 保护	是	是
恶意软件防护 EC2 – GuardDuty-启动的恶意软件扫描	是	是
恶意软件防护 EC2 – 按需恶意软件扫描	否	否
GuardDuty S3 恶意软件防护	否	否
RDS保护	是	是
运行时监控	否	是
S3 防护	是	是

¹ 每个保护计划都有自己的免费试用版。例如，当您在账户的 GuardDuty 30 天免费试用期到期后启用保护计划并且新的保护计划发布时，您可以通过自己的免费试用版启用此保护计划。有关免费试用保护计划的更多信息，请参阅与每个保护计划相关的文档。

在免费试用期间查看预计使用成本 — 在 30 天免费试用期间（可能还包括保护计划），会 GuardDuty 提供您账户的预计使用成本。GuardDuty 如果您是委托 GuardDuty 管理员账户，则可以查看所有已启用的成员账户的预估总使用成本和账户级别明细。GuardDuty 有关更多信息，请参阅 [估算成本 GuardDuty](#)。

免费试用期结束后的使用费用 — 当您在免费试用期结束后继续使用 GuardDuty 或其任何保护计划时，将开始产生相关的使用费用。要查看账单，请在<https://console.aws.amazon.com/billing/>控制台中导航至 Cost Explorer。有关 AWS 账户账单的更多信息，请参阅[AWS Billing 用户指南](#)。

使用 S3 的恶意软件防护，免费套餐为 12 个月

适用于 S3 的恶意软件防护使用与您关联的免费套餐计划 AWS 账户，该计划要么是新的，要么是持续的免费套餐，要么是已过期的 12 个月免费套餐。有关更多信息，请参阅 [S3 恶意软件防护定价](#)。

正在访问 GuardDuty

您可以通过以下任何一种方式使用 GuardDuty：

GuardDuty 控制台

<https://console.aws.amazon.com/guardduty/>

控制台是一个基于浏览器的界面，可供访问和使用。GuardDuty GuardDuty 控制台提供对您的 GuardDuty 账户、数据和资源的访问权限。

AWS 命令行工具

使用 AWS 命令行工具，您可以在系统的命令行中发出命令来执行 GuardDuty 任务和 AWS 任务。如果要构建执行任务的脚本，命令行工具十分有用。

有关安装和使用的信息 AWS CLI，请参阅 [《AWS Command Line Interface 用户指南》](#)。要查看的可用 AWS CLI 命令 GuardDuty，请参阅 [CLI 命令参考](#)。

GuardDuty HTTPS API

您可以通过使用 AWS 以编程方式访问 GuardDuty 和进行访问 GuardDuty HTTPS API，这样您就可以直接向服务发出 HTTPS 请求。有关更多信息，请参阅 [《GuardDuty API 参考》](#)。

AWS SDKs

AWS 提供软件开发套件 (SDKs)，其中包括适用于各种编程语言和平台 (Java、Python、Ruby 等) 的库和示例代码。NET、iOS、安卓等)。SDKs 提供了一种创建编程访问权限的便捷方式 GuardDuty。有关信息 AWS SDKs，包括如何下载和安装它们，请参阅 [适用于 Amazon Web Services 的工具](#)。

概念和术语

在您开始使用 Amazon 时 GuardDuty，您可以从了解其关键概念中受益。

账户

包含您的 AWS 资源的标准亚马逊 Web Services (AWS) 账户。您可以使用您的帐户登录 AWS 并启用 GuardDuty。

您也可以邀请其他账户在中启用您的 AWS 账户 GuardDuty 并与之建立关联 GuardDuty。如果您的邀请被接受，则您的账户将被指定为管理员 GuardDuty 账户，添加的账户将成为您的成员账户。然后，您可以代表他们查看和管理这些账户的 GuardDuty 调查结果。

管理员账户的用户可以配置 GuardDuty、查看和管理他们自己的账户和所有成员账户的 GuardDuty 调查结果。您最多可以拥有 10,000 个成员账户 GuardDuty。

成员账户的用户可以配置 GuardDuty、查看和管理其账户中的 GuardDuty 调查结果（通过 GuardDuty 管理控制台或 GuardDuty API）。成员账户的用户不能查看或管理其他成员的账户中的结果。

AWS 账户不能同时是 GuardDuty 管理员账户和成员账户。AWS 账户只能接受一份会员邀请。接受成员资格邀请是可选的。

有关更多信息，请参阅 [在 Amazon 中管理多个账户 GuardDuty](#)。

探测器

Amazon GuardDuty 是一项区域性服务。当您在特定的 GuardDuty 中启用时 AWS 区域，您 AWS 账户就会与探测器 ID 相关联。此 32 个字符的字母数字 ID 是您在该地区的账户所独有的。例如，当您 GuardDuty 为不同地区的同一个账户启用时，您的账户将与不同的探测器 ID 相关联。a 的格式 detectorId 是 12abc34d567e8fa901bc2d34e56789f0。

与管理 GuardDuty 调查结果和 GuardDuty 服务有关的所有发现、账户和操作都使用探测器 ID 来运行 API 操作。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

Note

在多账户环境中，成员账户的所有结果都会汇总到管理员账户的检测器中。

某些 GuardDuty 功能是通过探测器配置的，例如配置 CloudWatch 事件通知频率，以及启用或禁用 GuardDuty 要处理的可选保护计划。

在 S3 中使用恶意软件防护 GuardDuty

当您在已启用 S3 的账户中启用恶意软件防护时，S3 的恶意软件防护操作（例如启用、编辑和禁用受保护的资源）与检测器 ID 无关。GuardDuty

如果您未启用 GuardDuty 并选择威胁检测选项“适用于 S3 的恶意软件防护”，则不会为您的账户创建检测器 ID。

基础数据源

一组数据的源或位置。检测 AWS 环境中未经授权或意外的活动。GuardDuty 分析和处理来自 AWS CloudTrail 事件日志、AWS CloudTrail 管理事件、S3 AWS CloudTrail 的数据事件、VPC 流日志、DNS 日志中的数据，请参阅[GuardDuty 基础数据源](#)。

特征

为您的 GuardDuty 保护计划配置的功能对象有助于检测 AWS 环境中未经授权或意外的活动。每个 GuardDuty 保护计划都配置相应的功能对象来分析和处理数据。一些功能对象包括 EKS 审计日志、RDS 登录活动监控、Lambda 网络活动日志和 EBS 卷。有关更多信息，请参阅[中的功能激活 GuardDuty](#)。

调查发现

由 GuardDuty 发现的潜在安全问题。有关更多信息，请参阅[了解亚马逊的 GuardDuty 调查结果](#)。

调查结果显示在 GuardDuty 控制台中，并包含对安全问题的详细描述。您也可以通过调用[GetFindings](#)和[ListFindings](#) API 操作来检索生成的调查结果。

您还可以通过 Amazon CloudWatch 活动查看您的 GuardDuty 发现。GuardDuty CloudWatch 通过 HTTPS 协议将调查结果发送给 Amazon。有关更多信息，请参阅[使用 Amazon CloudWatch Events 创建对 GuardDuty 调查结果的自定义响应](#)。

IAM 角色

该 IAM 角色具有扫描 S3 对象所需的权限。启用标记扫描对象后，IAM PassRole 权限有助于向扫描对象 GuardDuty 添加标签。

恶意软件防护计划资源

为存储桶启用 S3 的恶意软件防护后，GuardDuty 会为 EC2 计划资源创建恶意软件防护。此资源与 EC2 计划 ID 的恶意软件防护相关联，该计划是受保护存储桶的唯一标识符。使用恶意软件防护计划资源对受保护的资源执行 API 操作。

受保护的存储桶 (受保护的资源)

如果您为 Amazon S3 存储桶启用 S3 恶意软件防护，且其保护状态更改为“活动”，则该存储桶被视为已受到保护。

GuardDuty 仅支持 S3 存储桶作为受保护资源。

保护状态

与您的恶意软件防护计划资源关联的状态。为存储桶启用 S3 恶意软件防护后，此状态表示您的存储桶设置是否正确。

S3 对象前缀

在亚马逊简单存储服务 (Amazon S3) Service 存储桶中，您可以使用前缀来组织存储。前缀是 S3 存储桶中对象的逻辑分组。有关更多信息，请参阅 Amazon S3 用户指南中的[组织和列出对象](#)。

扫描选项

启用 GuardDuty 恶意软件防护后，它允许您指定要扫描或跳过哪些亚马逊 EC2 实例和亚马逊弹性块存储 (EBS) 卷。EC2 此功能允许您将您的 EC2 实例和 EBS 卷关联的现有标签添加到包含标签列表或排除标签列表中。系统会扫描与添加到包含标签列表的标签关联的资源是否存在恶意软件，而不会扫描那些添加到排除标签列表的资源。有关更多信息，请参阅[使用用户定义的标签扫描选项](#)。

快照保留期

启用 GuardDuty 恶意软件防护后，它会提供在 AWS 账户中保留 EBS 卷快照的选项。EC2 GuardDuty 根据 EBS 卷的快照生成副本 EBS 卷。只有 EC2 扫描恶意软件防护检测到副本 EBS 卷中的恶意软件时，您才能保留 EBS 卷的快照。如果在副本 EBS 卷中未检测到恶意软件，则无论快照保留期设置如何，都会 GuardDuty 自动删除 EBS 卷的快照。有关更多信息，请参阅[快照保留](#)。

抑制规则

利用禁止规则，您可以创建非常具体的属性组合来隐藏发现结果。例如，您可以通过 GuardDuty 筛选器定义规则，仅 Recon:EC2/Portscan 从特定实例中 VPC、运行特定实例或带有特定 EC2 标签的实例中自动存档。AMI 此规则将导致自动从满足条件的实例存档端口扫描结果。但是，它仍然允许在 GuardDuty 检测到这些实例进行其他恶意活动（例如加密货币挖矿）时发出警报。

GuardDuty 管理员账户中定义的禁止规则适用于 GuardDuty 成员账户。GuardDuty 成员账户无法修改禁止规则。

使用抑制规则，GuardDuty 仍会生成所有调查结果。禁止规则可禁止显示发现结果，并保留所有活动的完整、不可变的历史记录。

通常，禁止规则用于隐藏已确定为环境中误报的发现结果，并减少低值发现结果带来的噪点，让您可以专注于处理较大的威胁。有关更多信息，请参阅 [抑制规则](#)。

可信 IP 列表

可信 IP 地址列表，用于与您的 AWS 环境进行高度安全的通信。GuardDuty 不会根据可信 IP 列表生成调查结果。有关更多信息，请参阅 [使用可信 IP 列表和威胁列表](#)。

威胁 IP 列表

已知恶意 IP 地址的列表。除了由于可能存在可疑活动而生成发现结果外，GuardDuty 还会根据这些威胁列表生成调查结果。有关更多信息，请参阅 [使用可信 IP 列表和威胁列表](#)。

入门 GuardDuty

本教程提供了动手操作介绍 GuardDuty。步骤 1 中介绍了以独立账户或 GuardDuty 管理员 GuardDuty 身份启用的最低要求。AWS Organizations 步骤 2 到 5 使用推荐的其他功能进行介绍，GuardDuty 以充分利用您的发现。

主题

- [开始前的准备工作](#)
- [第 1 步：启用 Amazon GuardDuty](#)
- [步骤 2：生成示例调查发现并浏览基本操作](#)
- [步骤 3：配置将 GuardDuty 结果导出到 Amazon S3 存储桶](#)
- [第 4 步：通过设置 GuardDuty 查找提醒 SNS](#)
- [后续步骤](#)

开始前的准备工作

GuardDuty 是一项威胁检测服务，用于监控[GuardDuty 基础数据源](#) AWS CloudTrail 事件日志、AWS CloudTrail 管理事件、Amazon VPC Flow Logs 和 DNS 日志等。GuardDuty 还会分析与其保护类型相关的功能，前提是您单独启用了这些功能。[功能](#)包括 Kubernetes 审核日志、RDS 登录活动、S3 日志、EBS 卷、运行时监控和 Lambda 网络活动日志。使用这些数据源和功能（如果启用），GuardDuty 可以为您的账户生成安全调查结果。

启用后 GuardDuty，它会开始监视您的环境。您可以随时 GuardDuty 为任何地区的任何账户禁用。这将停止 GuardDuty 处理基础数据源和任何单独启用的功能。

您不需要显式启用任何 [GuardDuty 基础数据源](#)。Amazon 直接从这些服务中 GuardDuty 提取独立的数据流。对于新 GuardDuty 账户，默认情况下，支持的所有可用保护类型 AWS 区域 均已启用并包含在 30 天免费试用期内。您可以选择退出其中任何一个或全部退出。如果您是现有 GuardDuty 客户，则可以选择启用您的任何或所有可用的保护计划 AWS 区域。有关更多信息，请参阅中与每种保护类型相关的[功能](#) GuardDuty。

启用时 GuardDuty，请考虑以下事项：

- GuardDuty 是一项区域服务，这意味着您在此页面上遵循的任何配置过程都必须在要监控的每个区域中重复执行 GuardDuty。

我们强烈建议您在所有支持的 AWS 区域 GuardDuty 中启用。这样 GuardDuty，即使在您未积极使用的区域，也可以生成有关未经授权或异常活动的调查结果。这还 GuardDuty 允许监控全球 AWS 服务 AWS CloudTrail 的事件，例如 IAM。如果 GuardDuty 未在所有支持的区域中都启用该功能，则其检测涉及全球服务的活动的的能力就会降低。有关可用地区的完整列表，请参阅[区域和端点](#)。

GuardDuty

- AWS 账户中任何具有管理员权限的用户都可以启用 GuardDuty，但是，按照最低权限的安全最佳实践，建议您创建要 GuardDuty 专门管理的 IAM 角色、用户或组。有关启用所需的权限的信息，GuardDuty 请参阅[启用 GuardDuty 所需的权限](#)。
- 当您在任何区域 GuardDuty 首次启用时 AWS 区域，默认情况下，它还会启用该区域支持的所有可用保护类型，包括针对的恶意软件防护 EC2。GuardDuty 为您的账户创建一个名为的服务关联角色。AWSServiceRoleForAmazonGuardDuty 此角色包括权限和信任策略，GuardDuty 允许直接使用和分析来自的事件[GuardDuty 基础数据源](#)以生成安全调查结果。的恶意软件防护会为您的账户 EC2 创建另一个名为的服务关联角色。AWSServiceRoleForAmazonGuardDutyMalwareProtection 此角色包括允许恶意软件防护 EC2 执行无代理扫描以检测您 GuardDuty 账户中的恶意软件的权限和信任策略。它 GuardDuty 允许在您的帐户中创建 EBS 卷快照，并与 GuardDuty 服务帐户共享该快照。有关更多信息，请参阅[的服务相关角色权限 GuardDuty](#)。有关服务相关角色的更多信息，请参阅[使用服务相关角色](#)。
- 当您在任何地区 GuardDuty 首次启用时，您的 AWS 账户将自动注册该地区的 30 天 GuardDuty 免费试用。

[入门：GuardDuty 为独立或多账户环境启用 Amazon](#)

第 1 步：启用 Amazon GuardDuty

使用的第一步 GuardDuty 是在您的账户中将其启用。启用后，GuardDuty 将立即开始监控当前区域中的安全威胁。

如果您想以 GuardDuty 管理员身份管理组织内其他账户的 GuardDuty 调查结果，则必须添加成员账户 GuardDuty 并为其启用。

Note

如果您想在不启用 S3 的情况下启用 GuardDuty 恶意软件防护 GuardDuty，则有关步骤，请参阅 [GuardDuty S3 恶意软件防护](#)。

Standalone account environment

1. 在以下位置打开 GuardDuty 控制台 <https://console.aws.amazon.com/guardduty/>
2. 选择“A mazon GuardDuty -所有功能”选项。
3. 选择开始。
4. 在“欢迎使用 GuardDuty”页面上，查看服务条款。选择“启用”GuardDuty。

Multi-account environment

Important

作为此过程的先决条件，您必须与要管理的所有账户属于同一个组织，并且有权访问 AWS Organizations 管理账户，才能在组织 GuardDuty 内委派管理员。委托管理员可能需要其他权限，有关更多信息，请参阅 [指定委派 GuardDuty 管理员账号所需的权限](#)。

指定委派 GuardDuty 管理员账户

1. 使用管理账户在上 <https://console.aws.amazon.com/organizations/> 打开 AWS Organizations 控制台。
2. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

您的账户 GuardDuty 已经启用了吗？

- 如果 GuardDuty 尚未启用，则可以选择“开始”，然后在“欢迎使用”GuardDuty 页面上指定 GuardDuty 委派管理员。
 - 如果 GuardDuty 已启用，则可以在“设置”页面上指定 GuardDuty 委派管理员。
3. 输入要指定为组织 GuardDuty 委托管理员的账户的十二位数 AWS 账户 ID，然后选择“委托”。

Note

如果尚未启用，GuardDuty 则指定委托管理员将在您当前区域 GuardDuty 为该账户启用。

要添加成员账户

此过程包括通过向 GuardDuty 委派管理员账户添加成员帐户 AWS Organizations。还可以选择通过邀请添加成员。要详细了解中两种关联成员的方法 GuardDuty，请参阅[在 Amazon 中管理多个账户 GuardDuty](#)。

1. 登录到委托管理员账户
2. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
3. 在导航窗格中，选择 Settings (设置)，然后选择 Accounts (账户)。

账户表显示组织中的所有账户。

4. 选中账户 ID 旁边的框，选择要添加作为成员的账户。然后从操作菜单中选择添加成员。

Tip

您可以打开自动启用功能，自动添加新账户作为成员；但这仅适用于启用该功能后加入组织的账户。

步骤 2：生成示例调查发现并浏览基本操作


当 GuardDuty 发现安全问题时，它会生成调查结果。GuardDuty 调查结果是一个数据集，其中包含与该独特安全问题相关的详细信息。调查发现的详细信息可以帮助您调查问题。

GuardDuty 支持生成带有占位符值的样本调查结果，这些占位符值可用于测试 GuardDuty 功能并熟悉调查结果，然后再需要对发现的实际安全问题做出响应。GuardDuty 按照以下指南为中提供的每种发现类型生成样本调查结果 GuardDuty，有关生成样本调查结果的其他方法，包括在您的账户中生成模拟安全事件，请参阅[示例发现结果](#)。

要创建和浏览示例调查发现

1. 在导航窗格中，选择设置。

2. 在设置页面上的示例调查发现下，选择生成示例调查发现。
3. 在导航窗格中，选择 Summary 以查看有关在您的 AWS 环境中生成的发现的见解。有关“摘要”控制面板组件的更多信息，请参阅 [摘要控制面板](#)。
4. 在导航窗格中，选择 调查发现。样本发现结果显示在“当前查找结果”页面上，前缀为 [SAMPLE]。
5. 从列表中选择一個调查发现，显示该调查发现的详细信息。
 - 您可以查看调查发现详细信息窗格中可用的不同信息字段。不同类型的调查发现可能有不同的字段。有关所有调查发现类型中的可用字段的更多信息，请参阅 [调查发现详细信息](#)。在详细信息窗格中，您可以执行以下操作：
 - 选择窗格顶部的查找 ID 以打开查找结果的完整JSON详细信息。也可以从此面板下载完整JSON文件。JSON包含一些未包含在控制台视图中的其他信息，并且是其他工具和服务可以提取的格式。
 - 查看受影响的资源部分。实际调查结果是，此处的信息将帮助您确定账户中应进行调查的资源，并将包括指向相应 AWS Management Console 可操作资源的链接。
 - 选择“+”或“-”视镜图标，为详细信息创建包含或排除筛选条件。有关调查发现筛选条件的更多信息，请参阅 [筛选调查发现](#)。
6. 存档所有示例调查发现
 - a. 选中列表顶部的复选框以选择所有调查发现。
 - b. 取消选择您要保留的所有调查发现。
 - c. 选择操作菜单，然后选择存档以隐藏示例调查发现。

 Note

要查看存档的调查发现，选择当前，然后选择已存档以切换调查发现视图。

步骤 3：配置将 GuardDuty 结果导出到 Amazon S3 存储桶

GuardDuty 建议配置设置以导出调查结果，因为它允许您将调查结果导出到 S3 存储桶，以便在 GuardDuty 90 天保留期之后无限期存储。这使您可以记录发现结果或跟踪 AWS 环境中一段时间内的问题。此处概述的过程将引导您设置新的 S3 存储桶，并创建用于在控制台中加密发现结果的新KMS密钥。有关这方面的更多信息，包括如何使用您自己的现有存储桶或其他账户中的存储桶，请参阅 [导出调查发现](#)。

要配置 S3 导出调查发现选项

1. 要对调查结果进行加密，您需要一个带有允许使用该KMS密钥 GuardDuty 进行加密的策略的密钥。以下步骤将帮助您创建新KMS密钥。如果您使用的是其他账户的KMS密钥，则需要通过登录拥有 AWS 账户 该密钥的账户来应用密钥策略。您的KMS密钥和 S3 存储桶的区域必须相同。但对于要从中导出调查发现的每个区域，可以使用相同的存储桶和密钥对。
 - a. 在 <https://console.aws.amazon.com/kms> 处打开控制台。
 - b. 要更改 AWS 区域，请使用页面右上角的区域选择器。
 - c. 在导航窗格中，选择客户托管密钥。
 - d. 选择 Create key。
 - e. 在密钥类型下选择对称，然后选择下一步。

Note

有关创建KMS密钥的详细步骤，请参阅《AWS Key Management Service 开发者指南》中的[创建密钥](#)。

- f. 为您的密钥提供别名，然后选择下一步。
- g. 选择下一步，然后再次选择下一步以接受默认的管理和使用权限。
- h. 查看配置后，选择完成以创建密钥。
- i. 在客户管理的密钥页面上，选择密钥别名。
- j. 在密钥策略选项卡中，选择切换到策略视图。
- k. 选择编辑并将以下密钥策略添加到您的KMS密钥中，授予对您的密钥的 GuardDuty 访问权限。此语句仅 GuardDuty 允许使用您添加此策略的密钥。编辑密钥策略时，请确保JSON语法有效。如果在最后一条语句之前添加语句，则必须在右括号之后加一个逗号。

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333",
```

```
    "aws:SourceArn":  
      "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"  
    }  
  }  
}
```

Replace (替换) *Region1* 使用您的KMS密钥所在区域。Replace (替换) *444455556666* 用 AWS 账户 拥有KMS钥匙的。Replace (替换) *KMSKeyId* 使用您选择进行加密的KMS 密钥的密钥 ID。要识别所有这些值 (区域 AWS 账户、和密钥 ID)，请查看您的KMS密钥 的。ARN要找到密钥ARN，请参阅[查找密钥 ID 和ARN](#)。

同样，替换 *111122223333* 用 GuardDuty 账户 AWS 账户 的。Replace (替换) *Region2* 使用 GuardDuty 账户所在的地区。Replace (替换) *SourceDetectorID* 使用 GuardDuty 账户的探测器 ID *Region2*。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectorsAPI](#)。

1. 选择保存。
2. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
3. 在导航窗格中，选择 Settings (设置)。
4. 在调查发现导出选项下，选择立即配置。
5. 选择新存储桶。为 S3 存储桶提供一个唯一名称。
6. (可选) 您可以通过生成示例调查发现来测试新的导出设置。在导航窗格中，选择 Settings (设置)。
7. 在示例调查发现部分，选择生成示例调查发现。新的示例发现结果将在最多五分钟后作为条目显示 GuardDuty 在创建的 S3 存储桶中。

第 4 步：通过设置 GuardDuty 查找提醒 SNS

GuardDuty 与 Amazon 集成 EventBridge，可用于将调查结果数据发送到其他应用程序和服务进行处理。通过将查找事件与 EventBridge 目标 (例如 AWS Lambda 函数、Amazon Systems Manager 自动化、Amazon S EC2 systems Manager 自动化、Amazon 简单通知服务 (SNS) 等) 关联起来，您可以使用 GuardDuty 调查结果启动对发现结果的自动响应。

在此示例中，您将创建一个SNS主题作为 EventBridge 规则的目标，然后使用它 EventBridge 来创建从中捕获结果数据的规则 GuardDuty。生成的规则会将调查发现详细信息转发到电子邮件地址。要了


解如何将调查发现发送到 Slack 或 Amazon Chime，以及如何修改发送警报的调查发现类型，请参阅 [设置 Amazon SNS 主题和端点](#)。

为你的发现创建 SNS 主题提醒

1. 在 <https://console.aws.amazon.com/sns/v3/> 上打开亚马逊主机。
2. 在导航窗格中，选择 Topics (主题)。
3. 选择创建主题。
4. 对于类型，选择标准。
5. 对于名称，请输入 **GuardDuty**。
6. 选择创建主题。这将打开新主题的主题详细信息。
7. 在订阅部分中，选择创建订阅。
8. 对于协议，选择电子邮件。
9. 对于端点，输入要向其发送通知的电子邮件地址。
10. 选择创建订阅。

创建订阅后，必须通过电子邮件确认订阅。

11. 要查看订阅消息，请进入您的电子邮件收件箱，然后在订阅消息中选择确认订阅。

 Note

要查看电子邮件确认状态，请转到 SNS 控制台并选择“订阅”。

创建用于捕获 GuardDuty 发现结果并对其进行格式化的 EventBridge 规则

1. 打开 EventBridge 控制台，网址为 <https://console.aws.amazon.com/events/>。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。

规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

5. 对于事件总线，选择默认。
6. 对于规则类型，选择具有事件模式的规则。
7. 选择下一步。

8. 对于事件源，选择 AWS 事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择AWS 服务。
11. 对于 AWS Service，选择 GuardDuty。
12. 对于事件类型，选择GuardDuty查找。
13. 选择下一步。
14. 对于目标类型，选择AWS 服务。
15. 在“选择目标”中，选择SNS主题，在“主题”中，选择您之前创建的SNS主题的名称。
16. 在其他设置部分，对于配置目标输入，选择输入转换器。

添加输入转换器会将从中发送的JSON查找数据格式 GuardDuty 化为人类可读的消息。

17. 选择 Configure input transformer (配置输入转换器) 。
18. 在目标输入转换器部分，对于输入路径，粘贴以下代码：

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. 要格式化电子邮件，请在“模板”中粘贴以下代码，并确保将红色文本替换为适合您所在地区的值：

```
"You have a severity severity GuardDuty finding type Finding_Type in
the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=region#/findings?search=id%3DFinding\_ID"
```

20. 选择确认。
21. 选择下一步。

22. (可选) 为规则输入一个或多个标签。有关更多信息，请参阅《[亚马逊 EventBridge 用户指南](#)》中的[亚马逊 EventBridge 标签](#)。
23. 选择下一步。
24. 查看规则详细信息并选择创建规则。
25. (可选) 使用步骤 2 中的过程生成示例调查发现来测试新规则。对于生成的每个示例调查发现，您都会收到一封电子邮件。

后续步骤

在您继续使用时 GuardDuty，您将逐渐了解与您的环境相关的发现类型。每当收到新调查发现时，您都可以从调查发现详细信息窗格上的调查发现描述中选择了解更多，或在 [调查发现类型](#) 上搜索调查发现名称来查找信息，包括有关调查发现的修复建议。

以下功能将帮助您进行调整，GuardDuty 使其能够为您的 AWS 环境提供最相关的发现：

- 要根据特定标准（例如实例 ID、账户 ID、S3 存储桶名称等）轻松对结果进行排序，您可以在其中创建和保存筛选条件 GuardDuty。有关更多信息，请参阅 [筛选调查发现](#)。
- 如果您收到有关环境中预期行为的调查发现，则可以根据您使用[抑制规则](#)定义的标准自动存档调查发现。
- 为了防止从受信任的子集生成调查结果IPs，或者将 GuardDuty 监视器置于正常监控范围IPs之外，您可以设置可[信 IP 和威胁列表](#)。

GuardDuty 基础数据源

GuardDuty 使用基础数据源来检测与已知恶意域和 IP 地址的通信，并识别潜在的异常行为和未经授权的活动。从这些源传输到时 GuardDuty，所有日志数据都经过加密。GuardDuty 从这些日志源中提取各种字段以进行性能分析和异常检测，然后丢弃这些日志。

首次在某些区域启用 GuardDuty 时，将提供 30 天的免费试用期，其中包括对所有基础数据源的威胁检测。在此免费试用期间，您可以监控按每个基础数据源细分的估计每月使用量。作为委托 GuardDuty 管理员账户，您可以查看按属于您的组织并已启用的每个成员账户细分的每月估计使用费用 GuardDuty。30 天试用期结束后，您可以使用获取 AWS Billing 有关使用费用的信息。

从这些基础数据源 GuardDuty 访问事件和日志时，无需支付额外费用。

GuardDuty 在中启用后 AWS 账户，它会自动开始监视以下各节中介绍的日志源。您无需启用任何其他功能即可开始分析和处理这些数据源以生成相关的安全调查结果。GuardDuty

主题

- [AWS CloudTrail 管理事件](#)
- [VPC 流日志](#)
- [Route53 解析器 DNS 查询日志](#)

AWS CloudTrail 管理事件

AWS CloudTrail 为您提供账户的 AWS API 呼叫历史记录，包括使用 AWS Management Console、命令行工具和某些 AWS 服务进行的 API 呼叫。AWS SDKs CloudTrail 还可以帮助您识别 AWS APIs 为支持的服务调用了哪些用户和帐户 CloudTrail、调用呼叫的源 IP 地址以及调用呼叫的时间。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 [什么是 AWS CloudTrail](#)。

GuardDuty 监视 CloudTrail 管理事件，也称为控制平面事件。这些事件可让您深入了解对 AWS 账户中的资源执行的管理操作。

以下是 GuardDuty 监控的 CloudTrail 管理事件的示例：

- 配置安全 (IAMAttachRolePolicy API 操作)
- 配置数据路由规则 (Amazon EC2 CreateSubnet API 运营)
- 设置日志 (AWS CloudTrail CreateTrail API 操作)

启用后 GuardDuty，它会直接 CloudTrail 通过独立且重复的事件流开始使用 CloudTrail 管理事件，并分析您的 CloudTrail 事件日志。

GuardDuty 不会管理您的 CloudTrail 事件或影响您的现有 CloudTrail 配置。同样，您的 CloudTrail 配置不会影响事件 GuardDuty 日志的使用和处理方式。要管理 CloudTrail 事件的访问和保留，请使用 CloudTrail 服务控制台或 API。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的[使用 CloudTrail 事件历史查看事件](#)。

如何 GuardDuty 处理 AWS CloudTrail 全球事件

对于大多数 AWS 服务，CloudTrail 事件都记录在创建 AWS 区域 地点。对于诸如 AWS Identity and Access Management (IAM)、(AWS STS)、亚马逊简单存储服务 AWS Security Token Service (Amazon S3)、Amazon 和 A CloudFront mazon Route 53 (Route 53) 之类的全球服务，事件仅在事件发生的地区生成，但具有全球意义。

使用具有安全价值（例如网络配置或用户权限）的 CloudTrail [全球服务事件](#)时，它会在您启 GuardDuty 用的每个区域复制这些事件并对其进行处理。GuardDuty 此行为有助于 GuardDuty 维护每个区域的用户和角色资料，这对于检测异常事件至关重要。

我们强烈建议您在所有已启 AWS 区域 用的选项 GuardDuty 中启用 AWS 账户。这有助于 GuardDuty 生成有关未经授权或异常活动的调查结果，即使在您可能未积极使用的地区也是如此。

VPC 流日志

Amazon 的 VPC Flow Logs 功能 VPC 可捕获有关您 AWS 环境中连接至亚马逊弹性计算云 (Amazon EC2) 实例的网络接口的 IP 流量的信息。

启用后 GuardDuty，它会立即开始分析您账户内的 Amazon EC2 实例中的 VPC 流日志。它通过 VPC 独立且重复的 VPC 流日志流直接使用流日志功能中的流日志事件。此过程不会影响任何现有的流日志配置。

[Lambda 保护](#)

Lambda 保护是亚马逊的一项可选增强功能。GuardDuty 目前，Lambda 网络活动监控包括来自您账户所有 Lambda 函数的 Amazon VPC 流日志，甚至包括那些不使用联网功能的日志。VPC 为了保护您的 Lambda 函数免受潜在的安全威胁，您需要在账户中配置 Lambda 保护。GuardDuty 有关更多信息，请参阅 [Lambda 保护](#)。

[GuardDuty 运行时监控](#)

当您在“运行时监控”或“EKS运行时监控”中管理EC2实例的安全代理（手动或通过 GuardDuty），并且GuardDuty 目前部署在 Amazon EC2 实例上并[收集的运行时事件类型](#)从该实例接收时，GuardDuty 不会向您 AWS 账户 收取分析来自此 Amazon EC2 实例的VPC流日志的费用。这有助于 GuardDuty 避免账户中的双重使用成本。

GuardDuty 不会管理您的流程日志，也无法在您的账户中访问这些日志。要管理对流日志的访问和保留，必须配置VPC流日志功能。

Route53 解析器DNS查询日志

如果您的 Amazon EC2 实例使用 AWS DNS解析器（默认设置），则 GuardDuty 可以通过内部解析器访问和处理您的请求和响应 Route53 Resolver DNS 查询日志。AWS DNS如果您使用其他DNS解析器（例如 Open DNS 或 Google）DNS，或者您设置了自己的DNS解析器，则 GuardDuty 无法访问和处理来自该数据源的数据。

启用后 GuardDuty，它会立即开始分析来自独立数据流的 Route53 Resolver DNS 查询日志。该数据流与通过 [Route 53 解析程序查询日志记录](#)功能提供的数据是分开的。此功能的配置不会影响 GuardDuty分析。

Note

GuardDuty 不支持在上启动的 Amazon EC2 实例的监控DNS日志，AWS Outposts 因为该环境中没有 Amazon Route 53 Resolver 查询日志功能。

中的功能激活 GuardDuty

当您首次启用 GuardDuty 用 Amazon 或在其中启用保护类型时 GuardDuty，将 GuardDuty 开始在您的 AWS 环境[基础数据来源](#)中处理相应的保护类型。GuardDuty 使用这些数据源来处理事件流，例如 VPC 流日志、DNS 日志以及 AWS CloudTrail 事件和管理日志。然后，GuardDuty 会分析这些事件以识别潜在的安全威胁，并在您的账户中生成调查发现。

除了日志数据源之外，GuardDuty 还可以使用来自 AWS 环境中其他 AWS 服务的其他数据来监控和分析潜在的安全威胁。

功能激活

添加其他 GuardDuty 保护（例如 S3 保护、运行时监控或 EKS 保护）时，可以配置与保护类型对应的 GuardDuty 功能。从历史上看，GuardDuty 保护措施 dataSources 被称为 APIs。但是，在 2023 年 3 月之后，新的 GuardDuty 保护类型现在配置为 features “不是” dataSources。GuardDuty 仍然支持配置 2023 年 3 月之前发布的保护类型，就像 dataSources 通过一样 API，但是新的保护类型只能通过以下方式提供 features。

如果您通过控制台管理 GuardDuty 配置和保护类型，则不会受到此更改的直接影响，也无需采取任何操作。功能激活会影响为启用 GuardDuty 或 APIs 其中的保护类型而调用的行为 GuardDuty。有关更多信息，请参阅 [GuardDuty API 改变](#)。

GuardDuty API 2023 年 3 月的变化

GuardDuty APIs 配置不属于列表的保护功能 [GuardDuty 基础数据来源](#)。功能对象包含功能详细信息，比如功能名称和状态，还可能包含某些功能的其他配置。此次迁移会影响 Amazon GuardDuty API 参考 APIs 中的以下内容：

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

相比于数据来源的功能激活

从历史上看，所有 GuardDuty 要素都是通过中的 dataSources 对象传递的 API。从 2023 年 3 月起，GuardDuty 首选 features dataSources 对象而不是中的 API 对象。所有较早的数据来源都有相应的功能，但较新的功能可能没有相应的数据来源。

以下列表显示了通过时 dataSources 和 features 对象之间的比较 API：

- dataSources 对象包含每种保护类型及其状态的对象。该 features 对象是与其中的每种保护类型相对应的可用功能列表 GuardDuty。

从 2023 年 3 月起，功能激活将是在您的 AWS 环境中配置新 GuardDuty 功能的唯一方法。

- API 请求或响应中的 dataSources 架构在每个可用 AWS 区域的地方 GuardDuty 都相同。但并非所有功能在每个区域都可用。因此，可用功能的名称可能因区域而异。

了解功能激活的工作原理

GuardDuty APIs 将继续返回适用的 dataSources 对象，它们还将以不同的格式返回一个包含相同信息的 features 对象。GuardDuty 2023 年 3 月之前推出的功能将通过 dataSources 物体和 features 物体提供。GuardDuty 自 2023 年 3 月起推出的功能只能通过该 features 对象使用。你不能创建或更新探测器，也不能描述你在同一个 API 请求中同时 AWS Organizations 使用两者 dataSources 兼而有之的 features 对象符号。要启用 GuardDuty 保护类型，您需要使用现在也包含该 features 对象的相同 APIs 数据源将现有数据源迁移到 features 对象。

Note

GuardDuty 修改后不会添加新的数据源。

GuardDuty 已弃用数据源。但仍然支持 [GuardDuty 基础数据源](#)。GuardDuty 最佳做法建议对已经为您的账户启用的任何保护类型使用功能激活。最佳实践还要求在为账户启用新的保护类型时使用功能激活。

合并功能激活更改

- 如果您通过APIsSDKs、或 AWS CloudFormation 模板管理 GuardDuty 配置，并且想要启用潜在的新 GuardDuty 功能，则需要分别修改代码和模板。有关更多信息，请参阅 [Amazon GuardDuty API 参考APIs](#)中更新的内容。
- 对于在此升级之前配置的 GuardDuty 功能，您可以继续使用APIsSDKs、或 AWS CloudFormation 模板。但我们建议您改用 feature 对象。

所有数据来源都有一个等效的功能对象。有关更多信息，请参阅 [将 dataSources 映射到 features](#)。

- 目前，features 对象中的 additionalConfiguration 仅适用于某些保护类型。
 - 对于此类保护类型，如果您的功能设置AdditionalConfigurationstatus为，ENABLED但您的功能配置status未设置为ENABLED，则在这种情况下 GuardDuty 不会采取任何操作。
 - 以下内容APIs会受到此影响：
 - [UpdateDetector](#)
 - [UpdateMemberDetectors](#)
 - [UpdateOrganizationConfiguration](#)

将 dataSources 映射到 features

下表显示保护类型、dataSources 和 features 的映射。

GuardDuty 保护类型	数据源名称*	特征名称
VPC 流日志	flowLogs (只读 ; 无法修改)	FLOW_LOGS (只读 ; 无法修改)
Route53 解析器DNS查询日志	dnsLogs (只读 ; 无法修改)	DNS_LOGS (只读 ; 无法修改)
CloudTrail 事件	ccloudTrail (只读 ; 无法修改)	CLOUD_TRAIL (只读 ; 无法修改)
S3	s3Logs	S3_DATA_EVENTS
EKS审计日志监控	kubernetes.auditlogs	EKS_AUDIT_LOGS

GuardDuty 保护类型	数据源名称 *	特征名称
恶意软件防护 EC2	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
RDS登录事件		RDS_LOGIN_EVENTS
EKS运行时监控		EKS_RUNTIME_MONITORING
运行时监控		RUNTIME_MONITORING
GuardDuty 适用于 Amazon EKS 集群的安全代理		EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
	GuardDuty 仅为这些保护类型提供功能激活支持。	RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT
GuardDuty 适用于 Amazon ECS-Fargate 集群的安全代理		RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT

GuardDuty 保护类型	数据源名称 *	特征名称
GuardDuty Amazon EC2 实例的安全代理		RUNTIME_MONITORING_additionalConfiguration.EC2_AGENT_MANAGEMENT
Lambda 保护		LAMBDA_NETWORK_LOGS

*GetUsageStatistics 使用自己的 dataSource 名称。有关更多信息，请参阅[估算成本 GuardDuty](#)或[GetUsageStatistics](#)。

GuardDuty S3 防护

S3 Protection 可帮助亚马逊 GuardDuty 监控亚马逊简单存储服务 (Amazon S3) AWS CloudTrail 的数据事件，其中包括API对象级操作，以识别您的 Amazon S3 存储桶中数据的潜在安全风险。

GuardDuty 监控 AWS CloudTrail 管理事件和 AWS CloudTrail S3 数据事件，以识别您的 Amazon S3 资源中的潜在威胁。这两个数据源监控不同类型的活动。S3 的 CloudTrail 管理事件示例包括列出或配置 Amazon S3 存储桶的操作 ListBuckets，例如 DeleteBuckets、和 PutBucketReplication。S3 CloudTrail 的数据事件示例包括对象级 API 操作，例如、GetObjectListObjectsDeleteObject、和 PutObject

当您 GuardDuty 为启用了 Amazon 时 AWS 账户，GuardDuty 就会开始监控 CloudTrail 管理事件。您无需明确启用或配置 S3 数据事件登录 AWS CloudTrail 即可使用 S3 保护。您可以随时为任何账户启用 S3 保护功能（用于监控 S3 CloudTrail 的数据事件）AWS 区域，只要该功能在 Amazon GuardDuty 中可用。已经启用的可以首次启用 GuardDuty S3 保护，免费试用期为 30 天。AWS 账户对于首次启用 AWS 账户 GuardDuty 的，S3 保护已启用并包含在这个 30 天的免费试用版中。有关更多信息，请参阅 [估算成本 GuardDuty](#)。

我们建议您在中启用 S3 保护 GuardDuty。如果未启用此功能，GuardDuty 将无法完全监控您的 Amazon S3 存储桶，也无法生成对存储在 S3 存储桶中的数据的可疑访问的发现。

如何 GuardDuty 使用 S3 数据事件

启用 S3 数据事件（S3 保护）后，GuardDuty 开始分析来自所有 S3 存储桶的 S3 数据事件，并监控它们是否存在恶意和可疑活动。有关更多信息，请参阅 [AWS CloudTrail S3 的数据事件](#)。

当未经身份验证的用户访问 S3 对象时，这意味着 S3 对象可以公开访问。因此，GuardDuty 不处理此类请求。GuardDuty 使用有效的 IAM (AWS Identity and Access Management) 或 AWS STS (AWS Security Token Service) 凭证处理对 S3 对象发出的请求。

备注

启用 S3 保护后，Amazon 会 GuardDuty 监控来自位于您启用的 GuardDuty 同一区域的 Amazon S3 存储桶的数据事件。

当基于 S3 数据事件监控 GuardDuty 检测到潜在威胁时，它会生成安全发现。有关 GuardDuty 可以为 Amazon S3 存储桶生成的调查结果类型的信息，请参阅 [GuardDuty S3 查找类型](#)。

如果您禁用 S3 保护，则 GuardDuty 会停止对存储在 S3 存储桶中的数据的 S3 数据事件监控。

S3 保护中的功能

AWS CloudTrail S3 的数据事件

数据事件也称为数据面板操作，提供对在资源上或资源内执行的资源操作的见解。数据事件通常是高容量活动。

以下是 GuardDuty 可以监控的 S3 CloudTrail 数据事件的示例：

- GetObjectAPI操作
- PutObjectAPI操作
- ListObjectsAPI操作
- DeleteObjectAPI操作

GuardDuty 首次启用时，S3 保护在默认情况下处于启用状态，并且还包含在 30 天免费试用期内。但是，此功能是可选的，您可以随时选择为任何账户或区域启用或禁用该功能。有关将 Amazon S3 配置为功能的更多信息，请参阅 [S3 防护](#)。

为独立账户配置 S3 保护

对于与之关联的账户 AWS Organizations，可以通过控制台设置自动执行此过程。有关更多信息，请参阅 [在多账户环境中配置 S3 保护](#)。

启用或禁用 S3 保护

选择您的首选访问方法，为独立账户配置 S3 保护。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择 S3 保护。
3. S3 保护页面提供您账户的 S3 保护的当前状态。选择启用或禁用，可随时启用或禁用 S3 保护。
4. 选择确认以确认您的选择。

API/CLI

1. 使用当前区域的有效检测器 ID，传递 features 对象 name，同时分别将 S3_DATA_EVENTS 设置为 DISABLED 或 ENABLED 以启用或禁用 S3 保护，来运行 [updateDetector](#)。

Note

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

2. 或者，您可以使用 AWS Command Line Interface。要启用 S3 保护，请运行以下命令并确保使用您自己的有效检测器 ID。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

要禁用 S3 保护，请将示例中的 ENABLED 替换为 DISABLED。

在多账户环境中配置 S3 保护

在多账户环境中，只有委派的 GuardDuty 管理员账户可以选择为其 AWS 组织中的成员账户配置（启用或禁用）S3 保护。GuardDuty 成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。委派的 GuardDuty 管理员账户可以选择在组织中的所有账户、仅限新账户或不启用任何账户上自动启用 S3 保护。有关更多信息，请参阅 [使用 AWS Organizations 管理账户](#)。

为委派的 GuardDuty 管理员账户配置 S3 保护

选择您的首选访问方法，为委派的 GuardDuty 管理员帐户配置 S3 保护。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

确保使用管理账户凭证。

2. 在导航窗格中，选择 S3 保护。
3. 在 S3 保护页面上，选择编辑。
4. 请执行以下操作之一：

使用对所有账户启用

- 选择为所有账户启用。这将为组织中的所有活跃 GuardDuty 账户（包括加入 AWS 组织的新账户）启用保护计划。
- 选择保存。

使用手动配置账户

- 要仅为委派 GuardDuty 管理员账户启用保护计划，请选择手动配置帐户。
- 在“委派 GuardDuty 管理员帐户（此帐户）”部分下选择“启用”。
- 选择保存。

API/CLI

使用当前区域 [updateDetector](#) 的委托 GuardDuty 管理员帐户的探测器 ID 运行，并将 `features` 对象 `namestatus` 作为 `S3_DATA_EVENTS` 和传递为 `ENABLED`。

或者，您可以使用配置 S3 保护 AWS Command Line Interface。运行以下命令，并确保替换 `12abc34d567e8fa901bc2d34e56789f0` 包含当前区域委派 GuardDuty 管理员帐户的探测器 ID。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。 `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

为组织中的所有成员账户自动启用 S3 保护

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用您的管理员帐户登录。

2. 请执行以下操作之一：

使用 S3 保护页面

1. 在导航窗格中，选择 S3 保护。
2. 选择为所有账户启用。此操作会自动为组织中的现有账户和新账户启用 S3 保护。
3. 选择保存。

Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在管理自动启用首选项窗口中，选择 S3 保护下的为所有账户启用。
4. 选择保存。

如果您无法使用为所有账户启用选项，请参阅 [有选择地在成员账户中启用或禁用 S3 保护](#)。

API/CLI

- 要有选择地为您的成员账户启用或禁用 S3 保护，请使用您自己的账户调用该 [updateMemberDetectors](#) API 操作 *detector ID*。
- 以下示例说明了如何为单个成员账户启用 S3 保护。一定要更换 *12abc34d567e8fa901bc2d34e56789f0* 使用 detector-id 委派 GuardDuty 管理员账户的，以及 *111122223333*。要禁用 S3 保护，请 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为所有现有活跃成员账户启用 S3 保护

选择您的首选访问方法，为组织中所有现有的活跃成员账户启用 S3 保护。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派的 GuardDuty 管理员账户凭据登录。

2. 在导航窗格中，选择 S3 保护。
3. 在 S3 保护页面上，您可以查看配置的当前状态。在活跃成员账户部分下，选择操作。
4. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
5. 选择确认。

API/CLI

- 要有选择地为您的成员账户启用或禁用 S3 保护，请使用您自己的账户调用该 [updateMemberDetectors](#) API 操作 *detector ID*。
- 以下示例说明了如何为单个成员账户启用 S3 保护。一定要更换 *12abc34d567e8fa901bc2d34e56789f0* 使用 detector-id 委派 GuardDuty 管理员账户的，以及 *111122223333*。要禁用 S3 保护，请 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为新成员账户自动启用 S3 保护

选择您的首选访问方法，为加入组织的新账户启用 S3 保护。

Console

委派的 GuardDuty 管理员账户可以使用 S3 保护或账户页面，通过控制台为组织中的新成员账户启用。

为新成员账户自动启用 S3 保护

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

- 使用 S3 保护页面：

1. 在导航窗格中，选择 S3 保护。
2. 在 S3 保护页面上，选择编辑。
3. 选择手动配置账户。
4. 选择为新成员账户自动启用。此步骤可确保每当有新账户加入您的组织时，系统都会自动为其账户启用 S3 保护。只有组织委派的 GuardDuty 管理员帐户才能修改此配置。
5. 选择保存。

- 使用账户页面：

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项。
3. 在管理自动启用首选项窗口中，选择 S3 保护下的为新账户启用。
4. 选择保存。

API/CLI

- 要有选择地为您的成员账户启用或禁用 S3 保护，请使用您自己的账户调用该 [UpdateOrganizationConfiguration](#) API 操作 *detector ID*。
- 以下示例说明了如何为单个成员账户启用 S3 保护。要将其禁用，请参阅 [有选择地在成员账户中启用或禁用 S3 保护](#)。将首选项设置为针对该区域中加入组织的新账户 (NEW)、组织中的所有账户 (ALL) 或组织中的无账户 (NONE) 自动启用或禁用保护计划。有关更多信息，请参阅 [autoEnableOrganization 成员](#)。根据您的首选项，可能需要将 NEW 替换为 ALL 或 NONE。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

有选择地在成员账户中启用或禁用 S3 保护

选择您的首选访问方法，有选择地为成员账户启用或禁用 S3 保护。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 在导航窗格中，选择账户。

在账户页面上，查看 S3 保护列，了解您的成员账户的状态。

3. 有选择地启用或禁用 S3 保护

选择您要为其配置 S3 保护的账户。您可以一次选择多个账户。在编辑保护计划下拉菜单中，选择 S3Pro，然后选择相应的选项。

API/CLI

要有选择地为您的成员账户启用或禁用 S3 保护，请使用您自己的检测器 ID 运行该 [updateMemberDetectors](#) API 操作。以下示例说明了如何为单个成员账户启用 S3 保护。要将其禁用，请将 `true` 替换为 `false`。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。 `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Note

您也可以传递用空格 IDs 分隔的账户列表。

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

Note

如果您使用脚本注册新帐户，并希望在新账户中禁用 S3 保护，则可以使用本主题中所述的可选 `dataSources` 对象修改 [createDetector](#) API 操作。

自动为新 GuardDuty 账户禁用 S3 保护

Important

默认情况下，首次为 AWS 账户 该联接 GuardDuty 自动启用 S3 保护。

如果您是首次启用新账户 GuardDuty 的 GuardDuty 管理员帐户，并且不希望默认启用 S3 保护，则可以通过使用可选 `features` 对象修改 [createDetector](#) API 操作来将其禁用。以下示例使用启用禁用 S3 保护的新 GuardDuty 检测器。 AWS CLI

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",  
"Status" : "DISABLED"}]'
```


GuardDuty EKS保护

EKS审计日志监控可帮助您检测亚马逊 Elastic Kubernetes Service (亚马逊) 中EKS集群中可能存在的可疑活动。EKS审计日志监控使用EKS审计日志来捕获用户、使用 Kubernetes API 的应用程序和控制平面按时间顺序排列的活动。有关更多信息，请参阅 [EKS审计日志监控](#)。

Note

EKS运行时监控作为运行时监控的一部分进行管理。有关更多信息，请参阅 [GuardDuty 运行时监控](#)。

EKS保护功能

EKS审计日志监控

EKS审计日志捕获您的 Amazon EKS 集群中的连续操作，包括来自用户、使用 Kubernetes 的应用程序和控制API平面的活动。审计日志记录是所有 Kubernetes 集群的一个组件。

有关更多信息，请参阅 Kubernetes 文档中的[审计](#)。

Amazon EKS 允许通过[EKS控制平面日志记录功能](#)将EKS审核 CloudWatch 日志作为 Amazon 日志提取。GuardDuty 不会管理您的 Amazon EKS 控制平面日志，如果您尚未为亚马逊启用EKS审核日志，也无法在您的账户中访问审核日志EKS。要管理对EKS审核日志的访问和保留，您必须配置 Amazon EKS 控制平面日志功能。有关更多信息，请参阅 Amazon EKS 用户指南中的[启用和禁用控制平面日志](#)。

有关配置EKS审计日志监控的信息，请参见[EKS审计日志监控](#)。

EKS审计日志监控

EKS审计日志监控可帮助您在 Amazon Elastic Kubernetes Service 中检测EKS集群中可能存在的可疑活动。启用EKS审计日志监控后，会 GuardDuty 立即开始[EKS审计日志监控](#)从您的 Amazon EKS 集群进行监控并分析这些集群中是否存在潜在的恶意和可疑活动。它通过独立且重复的审计日志流直接使用 Amazon EKS 控制平面日志功能中的 Kubernetes 审计日志事件。此过程不需要任何其他设置，也不影响您可能拥有的任何现有 Amazon EKS 控制平面日志配置。

禁用EKS审计日志监控后，会 GuardDuty 立即停止监控和分析您的 Amazon EKS 资源的EKS审计日志。

EKS审计日志监控可能并非在所有可用 AWS 区域 的地方都可 GuardDuty 用。有关更多信息，请参阅[特定于区域的功能可用性](#)。

30 天免费试用期如何影响账号 GuardDuty

- GuardDuty 首次启用时，EKS审计日志监控已包含在 30 天的免费试用期内。
- 现有 GuardDuty 账户（30 天免费试用期已经结束）可以首次启用“EKS审计日志监控”，免费试用期为 30 天。

为独立账户配置EKS审核日志监控

选择您的首选访问方式，为独立账户启用或禁用“EKS审核日志监控”。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“EKS保护”。
3. 在配置选项卡下，您可以查看EKS审计日志监控的当前配置状态。在“EKS审计日志监控”部分，选择“启用”以启用或选择“禁用”以禁用“EKS审核日志监控”功能。
4. 选择保存。

API/CLI

- 使用委派 GuardDuty 管理员账户的区域探测器 ID 运行[updateDetector](#)API操作，并将features对象名称传递为EKS_AUDIT_LOGS，状态为ENABLED或DISABLED。

或者，您也可以启用或禁用运行 AWS CLI 命令的EKS审计日志监控。以下示例代码启用 GuardDuty EKS审计日志监控。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
```

在多账户环境中配置EKS审计日志监控

在多账户环境中，只有委派的 GuardDuty 管理员帐户可以选择为其组织中的成员帐户启用或禁用“EKS 审核日志监控;”功能。GuardDuty 成员帐户无法通过其帐户修改此配置。委托 GuardDuty 管理员帐户使用管理其成员帐户 AWS Organizations。此委派的 GuardDuty 管理员帐户可以选择在所有新帐户加入组织时自动启用EKS审核日志监控。有关多账户环境的更多信息，请参阅在 [Amazon 中管理多个帐户](#)。GuardDuty

为委派的 GuardDuty 管理员帐户配置EKS审核日志监控

选择您的首选访问方法，为委派的 GuardDuty 管理员帐户配置“EKS审核日志监控”。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

确保使用管理帐户凭证。

2. 在导航窗格中，选择“EKS保护”。
3. 在“配置”选项卡下，您可以在相应部分中查看“EKS审计日志监控”的当前配置状态。要更新委派 GuardDuty 管理员帐户的配置，请在“EKS审计日志监控”窗格中选择“编辑”。
4. 请执行以下操作之一：

使用对所有帐户启用

- 选择为所有帐户启用。这将为组织中的所有活跃 GuardDuty 帐户（包括加入 AWS 组织的新帐户）启用保护计划。
- 选择保存。

使用手动配置帐户


- 要仅为委派 GuardDuty 管理员帐户启用保护计划，请选择手动配置帐户。
- 在“委派 GuardDuty 管理员帐户（此帐户）”部分下选择“启用”。
- 选择保存。

API/CLI

使用您自己的区域探测器 ID 运行 [updateDetector](#) API 操作，并以 ENABLED 或的 status 形式传递 features 对象 name DISABLED。EKS_AUDIT_LOGS

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectorsAPI](#)。

您可以通过运行以下 AWS CLI 命令来启用或禁用“EKS审计日志监控”。请务必使用有效的委托 GuardDuty 管理员账号 *detector ID*。

 Note

以下示例代码启用EKS审计日志监控。一定要更换

12abc34d567e8fa901bc2d34e56789f0 使用detector-id委派 GuardDuty 管理员账户的和 *555555555555* 使用 AWS 账户 委派 GuardDuty 管理员账户的。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectorsAPI](#)。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

要禁用“EKS审计日志监控”，请ENABLED替换为DISABLED。

为所有成员账户自动启用EKS审核日志监控

选择您的首选访问方式，为组织中的现有成员账户启用EKS审核日志监控。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。


2. 请执行以下操作之一：

使用“EKS保护”页面

1. 在导航窗格中，选择“EKS保护”。
2. 在“配置”选项卡下，您可以查看组织中活跃成员账户的EKS审核日志监控的当前状态。

要更新EKS审计日志监控配置，请选择编辑。

3. 选择为所有账户启用。此操作会自动为组织中的现有账户和新账户启用EKS审核日志监控。
4. 选择保存。

 Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在“管理自动启用首选项”窗口中，选择“EKS审计日志监控”下的“为所有帐户启用”。
4. 选择保存。


如果您无法使用“为所有账户启用”选项，并且想要为组织中的特定账户自定义EKS审核日志监控配置，请参阅[有选择地为成员账户启用或禁用“EKS审核日志监控”](#)。

API/CLI

- 要有选择地为您的成员账户启用或禁用“EKS审核日志监控”，请使用您自己的账户运行该[updateMemberDetectors](#)API操作 *detector ID*。
- 以下示例说明如何为单个成员账户启用“EKS审核日志监控”。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

 Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为所有现有活跃成员账户启用EKS审核日志监控

选择您的首选访问方式，为组织中所有现有活跃成员账户启用EKS审核日志监控。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派 GuardDuty 管理员账户凭证登录。

2. 在导航窗格中，选择“EKS保护”。
3. 在“EKS保护”页面上，您可以查看GuardDuty启动的恶意软件扫描配置的当前状态。在活跃成员账户部分下，选择操作。
4. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
5. 选择保存。

API/CLI

- 要有选择地为您的成员账户启用或禁用“EKS审核日志监控”，请使用您自己的账户运行该 [updateMemberDetectors](#) API 操作 *detector ID*。
- 以下示例说明如何为单个成员账户启用“EKS审核日志监控”。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区 detectorId 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为新成员账户自动启用EKS审核日志监控

在选择配置 GuardDuty启动的恶意软件扫描 GuardDuty 之前，必须启用新添加的成员帐户。通过邀请管理的成员帐户可以为其帐户手动配置 GuardDuty启动的恶意软件扫描。有关更多信息，请参阅 [Step 3 - Accept an invitation](#)。

选择您的首选访问方式，为加入您组织的新账户启用EKS审核日志监控。

Console

委派的 GuardDuty 管理员帐户可以使用“EKS审计日志监控”或“帐户”页面，为组织中的新成员帐户启用EKS审计日志监控。

为新成员账户自动启用“EKS审核日志监控”

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

- 使用“EKS保护”页面：

1. 在导航窗格中，选择“EKS保护”。
2. 在“EKS保护”页面上，在“EKS审计日志监控”中选择“编辑”。
3. 选择手动配置账户。
4. 选择为新成员账户自动启用。此步骤可确保每当有新账户加入您的组织时，系统都会自动为其账户启用“EKS审核日志监控”。只有组织委派的 GuardDuty 管理员帐户才能修改此配置。
5. 选择保存。

- 使用账户页面：

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项。
3. 在“管理自动启用首选项”窗口中，在“EKS审计日志监控”下选择“为新帐户启用”。
4. 选择保存。

API/CLI

- 要有选择地为新账户启用或禁用“EKS审核日志监控”，请使用您自己的账户运行该[UpdateOrganizationConfiguration](#)API操作 *detector ID*。
- 以下示例说明如何为加入组织的新成员启用“EKS审核日志监控”。您也可以传递用空格IDs分隔的账户列表。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

有选择地为成员账户启用或禁用“EKS审核日志监控”

选择您的首选访问方式，为组织中的选定成员帐户启用或禁用“EKS审核日志监控”。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 在导航窗格中，选择账户。

在“帐户”页面上，查看“EKS审计日志监控”列，了解您的成员账户的状态。

3. 启用或禁用“EKS审计日志监控”

选择要为EKS审计日志监控配置的帐户。您可以一次选择多个账户。在“编辑保护计划”下拉列表中，选择“EKS审计日志监控”，然后选择相应的选项。

API/CLI

要有选择地为您的成员账户启用或禁用“EKS审核日志监控”，请使用您自己的账户调用该[updateMemberDetectors](#)API操作 *detector ID*。

以下示例说明如何为单个成员账户启用“EKS审核日志监控”。要将其禁用，请将 ENABLED 替换为 DISABLED。您也可以传递用空格IDs分隔的账户列表。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行ListDetectorsAPI。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":  
"ENABLED"}]'
```

GuardDuty 运行时监控

运行时监控可观察和分析操作系统级别、网络 and 文件事件，以帮助检测环境中特定 AWS 工作负载中的潜在威胁。

运行时监控@@ 中支持的 AWS 资源 — GuardDuty 最初发布的运行时监控仅支持亚马逊 Elastic Kubernetes Service (亚马逊) 资源。EKS现在，您还可以使用运行时监控功能为您的 AWS Fargate 亚马逊弹性容器服务 (AmazonECS) 和亚马逊弹性计算云 (AmazonEC2) 资源提供威胁检测。

GuardDuty 不支持在上 AWS Fargate面运行的 Amazon EKS 集群。

在本文档以及与运行时监控相关的其他章节中，GuardDuty 使用资源类型的术语来指代亚马逊 EKS、Fargate Amazon ECS 和亚马逊EC2资源。

Runtime Monitoring 使用 GuardDuty 安全代理，该代理可增加运行时行为的可见性，例如文件访问、进程执行、命令行参数和网络连接。对于要监控潜在威胁的每种资源类型，您可以自动或手动管理该特定资源类型的安全代理 (Fargate (ECS仅限 Amazon) 除外)。自动管理安全代理意味着您 GuardDuty 允许代表您安装和更新安全客户端。另一方面，当您手动管理资源的安全代理时，您负责根据需要安装和更新安全代理。

借助此扩展功能，GuardDuty 可以帮助您识别和应对可能针对在您的个人工作负载和实例中运行的应用程序和数据的潜在威胁。例如，威胁可能会从破坏单个容器开始，而这种容器通常在运行易受攻击的 Web 应用程序。此 Web 应用程序可能拥有对底层容器和工作负载的访问权限。在这种情况下，错误配置的凭证可能会导致对账户及其所存储数据的访问权限扩大。

通过分析单个容器和工作负载的运行时事件，GuardDuty 有可能在初始阶段识别容器和相关 AWS 凭证的泄露情况，并检测到有人企图提升权限、可疑API请求以及对环境中数据的恶意访问。

内容

- [工作方式](#)
- [运行时监控中的 30 天免费试用是如何运作的](#)
- [关键概念-管理 GuardDuty 安全代理的方法](#)
- [启用 GuardDuty 运行时监控](#)
- [配置EKS运行时监控 \(API仅限 \)](#)
- [从EKS运行时监控迁移到运行时监控](#)
- [评估资源的运行时间覆盖率](#)

- [设置CPU和内存监控](#)
- [收集的 GuardDuty 使用运行时事件类型](#)
- [Amazon ECR 存储库托管 GuardDuty 代理](#)
- [GuardDuty 代理发布历史记录](#)
- [禁用和清理资源的影响](#)

工作方式

要使用运行时监控，必须启用运行时监控，然后管理 GuardDuty 安全代理。以下列表说明了这个两步过程：

1. 为您的账户@@ 启用运行时监控，这样它 GuardDuty 就可以接受从您的亚马逊EC2实例、亚马逊 ECS集群和亚马逊EKS工作负载收到的运行时事件。
2. 管理要监控其运行时行为的各个资源的 GuardDuty 代理。根据资源类型，您可以选择手动部署 GuardDuty 安全代理，也可以 GuardDuty 允许代表您管理安全代理，称为自动代理配置。

GuardDuty 使用[实例身份角色](#)对每种资源类型的安全代理进行身份验证，将关联的运行时事件发送到VPC终端节点。

Note

GuardDuty 不会让你访问运行时事件。

当您在“运行时监控”或“EKS运行时监控”中管理EC2实例的安全代理（手动或通过 GuardDuty），并且GuardDuty 目前部署在 Amazon EC2 实例上并[收集的运行时事件类型](#)从该实例接收时，GuardDuty 不会向您 AWS 账户 收取分析来自此 Amazon EC2 实例的VPC流日志的费用。这有助于 GuardDuty 避免账户中的双重使用成本。

以下主题说明了为每种资源类型启用运行时监控和管理 GuardDuty 安全代理的工作方式有何不同。

内容

- [运行时监控如何与 Amazon EC2 实例配合使用](#)
- [运行时监控如何与 Fargate 配合使用（仅限亚马逊ECS）](#)
- [运行时监控如何与 Amazon EKS 集群配合使用](#)

- [运行时监控配置后](#)

运行时监控如何与 Amazon EC2 实例配合使用

您的 Amazon EC2 实例可以在您的 AWS 环境中运行多种类型的应用程序和工作负载。启用运行时监控并管理 GuardDuty 安全代理后，GuardDuty 可帮助您检测现有 Amazon EC2 实例和可能的新实例中的威胁。此功能还支持亚马逊ECS托管的亚马逊EC2实例。

启用运行时监控可以 GuardDuty 随时使用当前正在运行的运行时事件和 Amazon EC2 实例中的新进程。GuardDuty 需要安全代理将运行时事件从您的EC2实例发送到 GuardDuty。

对于 Amazon EC2 实例，GuardDuty 安全代理在实例级别运行。您可以决定是要监控账户中的所有还是部分 Amazon EC2 实例。如果要管理选定实例，则只有这些实例才需要安全代理。

GuardDuty 还可以使用来自新任务和 Amazon ECS 集群内的 Amazon EC2 实例中运行的现有任务的运行时事件。

要安装 GuardDuty 安全代理，运行时监控提供了以下两个选项：

- [使用自动代理配置（推荐）](#)，或
- [手动管理安全代理](#)

通过以下方式使用自动代理配置 GuardDuty（推荐）

使用自动代理配置，GuardDuty 允许代表您在 Amazon EC2 实例上安装安全代理。GuardDuty 还管理安全客户端的更新。

默认情况下，GuardDuty 会在您账户中的所有实例上安装安全代理。如果您只 GuardDuty 想为选定 EC2实例安装和管理安全代理，请根据需要向您的EC2实例添加包含或排除标签。

有时，您可能不想监控属于您账户的所有 Amazon EC2 实例的运行时事件。如果您想监控有限数量的实例的运行时事件，请将包含标签添加为GuardDutyManaged:true到这些选定的实例。从可用于 Amazon 的自动代理配置开始EC2，如果您的EC2实例具有包含标签 (GuardDutyManaged:true)，即使您没有明确启用自动代理配置，也 GuardDuty将使用该标签并管理所选实例的安全代理。

另一方面，如果您不想监控运行时事件的EC2实例数量有限，请为这些选定的实例添加排除标签 (GuardDutyManaged:false)。GuardDuty 将通过既不安装也不管理这些EC2资源的安全代理来遵守排除标签。

影响

当您在 AWS 账户 或组织中使用自动代理配置时，您 GuardDuty 允许代表您执行以下步骤：

- GuardDuty 为您SSM管理的所有 Amazon EC2 实例创建一个SSM关联，这些实例在<https://console.aws.amazon.com/systems-manager/>控制台的 Fleet Manager 下方显示。
- 在禁用自动代理配置的情况下使用包含标签 — 启用运行时监控后，如果您不启用自动代理配置，而是向 Amazon EC2 实例添加包含标签，则表示 GuardDuty 允许您代表自己管理安全代理。SSM然后，协会将在每个带有包含标签 (GuardDutyManaged:true) 的实例中安装安全代理。
- 如果您启用自动代理配置，则该SSM协会将在属于您账户的所有EC2实例中安装安全代理。
- 使用带有自动代理配置的排除标签 — 在启用自动代理配置之前，当您向 Amazon EC2 实例添加排除标签时，这意味着 GuardDuty 允许您阻止为该选定实例安装和管理安全代理。

现在，当您启用自动代理配置时，该SSM协会将在所有EC2实例中安装和管理安全代理，但标有排除标签的实例除外。

- GuardDuty 只要至少有一个 Linux EC2 实例未处于已VPC终止或关闭实例状态的 Linux 实例VPC，就会在所有实例中创建终端节点，包括共享VPCs端点。VPCs这包括集中式VPC和分支式VPCs。GuardDuty 不支持仅为集中式创建VPC端点VPC。有关集中式VPC工作原理的更多信息，请参阅AWS 白皮书《构建可扩展且安全的多VPC AWS 网络基础架构》中的[接口VPC端点](#)。

有关不同实例状态的信息，请参阅 Amazon EC2 用户指南中的[实例生命周期](#)。

GuardDuty 还支持[使用VPC与自动安全代理共享](#)。当您的组织考虑了所有先决条件时 AWS 账户，GuardDuty 将使用共享VPC来接收运行时事件。

Note

使用VPC终端节点不会产生额外费用。

手动管理安全代理

有两种方法可以EC2手动管理 Amazon 的安全代理：

- 使用中的 GuardDuty 托管文档在 AWS Systems Manager 已托SSM管的 Amazon EC2 实例上安装安全代理。

每当您启动新的 Amazon EC2 实例时，请确保其SSM已启用。

- 使用RPM包管理器 (RPM) 脚本在您的 Amazon EC2 实例上安装安全代理，无论这些实例是否处于 SSM托管状态。

后续步骤

要开始使用运行时监控配置来监控您的 Amazon EC2 实例，请参阅[Amazon EC2 实例支持的先决条件](#)。

运行时监控如何与 Fargate 配合使用 (仅限亚马ECS逊)

启用运行时监控后 GuardDuty，即可使用任务中的运行时事件。这些任务在 Amazon ECS 集群中运行，而Amazon集群又在 AWS Fargate (Fargate) 实例上运行。GuardDuty 要接收这些运行时事件，必须使用完全托管的专用安全代理。

运行时监控仅支持通过管理您的 Amazon ECS 集群 (AWS Fargate) 的安全代理 GuardDuty。不支持在 Amazon ECS 集群上手动管理安全代理。

您可以通过使用 AWS 账户或组织的自动代理配置来允许 GuardDuty 代表您管理 GuardDuty 安全客户端。GuardDuty 将开始将安全代理部署到您的 Ama ECS zon 集群中启动的新 Fargate 任务。以下列表列出了启用 GuardDuty 安全代理时的预期情况。

启用 GuardDuty 安全代理的影响

GuardDuty 创建虚拟私有云 (VPC) 端点

部署 GuardDuty 安全代理时，GuardDuty 将创建一个VPC终端节点，安全代理通过该端点将运行时事件传送到该端点 GuardDuty。

注意

- 使用自动代理集中VPC使用——当你对某一资源类型使用 GuardDuty 自动代理配置时，GuardDuty 将代表你为所有资源类型创建一个VPC终端节点VPCs。这包括集中式VPC和分支式VPCs。GuardDuty 不支持仅为集中式创建VPC端点VPC。有关集中式VPC工作原理的更多信息，请参阅AWS 白皮书《构建可扩展且安全的多VPC AWS 网络基础架构》中的[接口VPC端点](#)。
- 使用VPC终端节点不会产生额外费用。

GuardDuty 添加一个边车容器

对于开始运行的新 Fargate 任务或服务，GuardDuty 容器（边车）将自身附加到 Amazon Fargate 任务中的每个容器。GuardDuty 安全代理在连接的 GuardDuty 容器内运行。这 GuardDuty 有助于收集在这些任务中运行的每个容器的运行时事件。

启动 Fargate 任务时，如果 GuardDuty 容器（sidecar）无法在正常状态下启动，则运行时监控的设计不会阻止任务运行。

默认情况下，Fargate 任务是不可变的。GuardDuty 当任务已经处于运行状态时，不会部署边车。如果要监控已在运行的任务中的容器，可以停止该任务并重新启动它。

运行时监控如何与 Amazon EKS 集群配合使用

运行时监控使用[EKS插件 `aws-guardduty-agent`](#)，也称为 GuardDuty 安全代理。在您的 EKS 集群上部署 GuardDuty 安全代理后，GuardDuty 就可以接收这些 EKS 集群的运行时事件了。

GuardDuty 仅支持在亚马逊 EC2 实例上运行的亚马逊 EKS 集群。GuardDuty 不支持在 AWS Fargate 面运行的 Amazon EKS 集群。

您可以在账户或集群级别监控 Amazon EKS 集群的运行时事件。您只能管理要监控以进行威胁检测的 Amazon EKS 集群 GuardDuty 的安全代理。您可以手动管理 GuardDuty 安全客户端，也可以使用自动代理配置来代表您管理安全客户端。GuardDuty

当您使用自动代理配置方法 GuardDuty 来允许代表您管理安全代理的部署时，它将自动创建一个 Amazon Virtual Private Cloud (Amazon VPC) 终端节点。安全代理使用此 Amazon VPC 终端节点将 GuardDuty 运行时事件传送到。

注意

- 使用 VPC 终端节点不会产生额外费用。
- 使用自动代理集中 VPC 使用——当你对某一资源类型使用 GuardDuty 自动代理配置时，GuardDuty 将代表你为所有资源类型创建一个 VPC 终端节点 VPCs。这包括集中式 VPC 和分支式 VPCs。GuardDuty 不支持仅为集中式创建 VPC 端点 VPC。有关集中式 VPC 工作原理的更多信息，请参阅 AWS 白皮书《构建可扩展且安全的多 VPC AWS 网络基础架构》中的[接口 VPC 端点](#)。

运行时监控配置后

评估运行时间覆盖率

启用运行时监控并部署 GuardDuty 安全代理后，我们建议您持续评估部署安全代理的资源的覆盖状态。保险状态可能为“健康”或“不健康”。健康覆盖状态表示当存在操作系统级活动时，GuardDuty 正在接收来自相应资源的运行时事件。

当资源的覆盖状态变为“健康”时，GuardDuty 可以接收运行时事件并对其进行分析以进行威胁检测。在容器工作负载和实例中运行的任务或应用程序中 GuardDuty 检测到潜在的安全威胁时，GuardDuty 会生成一个或多个运行时监控查找类型。

您还可以将 Amazon EventBridge (EventBridge) 配置为在保险状态从“不健康”变为“健康”等时收到通知。有关更多信息，请参阅 [评估资源的运行时间覆盖率](#)。

GuardDuty 安全代理CPU的设置和内存监控

在评估覆盖状态显示为“健康”之后，您可以针对您的资源类型评估安全代理的性能。对于安全代理 v1.5 或更高版本的 Amazon EKS 集群，GuardDuty 支持配置（附加组件）安全代理的参数。有关更多信息，请参阅 [设置CPU和内存监控](#)。

GuardDuty 检测潜在威胁

当 GuardDuty 开始接收资源的运行时事件时，它就会开始分析这些事件。当在您的任何 Amazon EC2 实例、Amazon 集群或 Amazon ECS 集群中 GuardDuty 检测到潜在的安全威胁时，它会生成一个或多个安全威胁[运行时监控查找类型](#)。EKS您可以访问调查结果详细信息以查看受影响的资源详细信息。

运行时监控中的 30 天免费试用是如何运作的

对于新 GuardDuty 账户和在运行时监控功能扩展到 Amazon EC2 实例和 AWS Fargate（ECS仅限 Amazon）之前已经启用EKS运行时监控的现有账户，30 天免费试用期的运作方式有所不同。

我正在使用 GuardDuty 试用期或者我从未启用过EKS运行时监控

以下列表说明了如果您使用的是 30 天试用期或从未启用EKS运行时监控，GuardDuty 30 天免费试用期是如何运作的：

- GuardDuty 首次启用时，默认情况下不会启用EKS运行时监控和运行时监控。

为您的账户或组织启用“运行时监控”时，请务必同时为要监控的资源配置 GuardDuty 安全代理，以进行威胁检测。例如，如果您想对您的 Amazon EC2 实例使用运行时监控，则在启用运行时监控后，还必须为 Amazon 配置安全代理 EC2。您可以选择手动或通过自动执行此操作 GuardDuty。

- 运行时监控保护计划已在账户级别启用。30 天免费试用期适用于资源级别。将 GuardDuty 安全代理部署到特定资源类型后，30 天免费试用将在 GuardDuty 收到与该资源类型关联的第一个运行时事件时开始。例如，您已在资源级别（适用于亚马逊 EC2 实例、Amazon 集群和亚马逊 ECS 集 EKS 群）部署了 GuardDuty 代理。当 GuardDuty 收到 Amazon EC2 实例的第一个运行时事件时，30 天免费试用将 EC2 仅适用于亚马逊。
- 当您只想启用 EKS 运行时监控时 — GuardDuty 首次启用运行 EKS 时监控时，默认情况下不启用运行时监控（在发布运行时监控之后）。您需要启用“EKS 运行时监控”。要以最佳方式使用它，请确保手动管理 GuardDuty 安全客户端，或者启用自动代理配置，以便代表您 GuardDuty 管理安全代理。EKS 运行时监控的 30 天免费试用期从 GuardDuty 收到 Amazon EKS 资源的第一个运行时事件时开始。

我在启动 EKS 运行时监控之前启用了运行时监控

- 对于已启用 EKS 运行时监控保护计划并使用 GuardDuty 控制台体验使用此保护计划的现有 GuardDuty 账户 — 随着运行时监控的发布，运行时监控控制台体验现已整合到运行时监控中。EKS 运行时监控的现有配置保持不变。您可以继续使用 API/CLI 支持来执行与 EKS 运行时监控相关的操作。
- 要使用 EKS 运行时监控作为运行时监控的一部分，您需要为您的账户或组织配置运行时监控。要保持运行时监控的相同配置，请参见 [从 EKS 运行时监控迁移到运行时监控](#)。但是，这不会影响您的 30 天免费试用 Amazon EKS 资源。
- 运行时监控保护计划在每个区域的账户级别启用。将 GuardDuty 安全代理部署到其中一种指定资源类型（Amazon EC2 实例和 Amazon ECS 集群）后，30 天免费试用将在 GuardDuty 收到与该资源关联的第一个运行时事件时开始。每种资源类型都有 30 天免费试用。

例如，启用运行时监控后，您选择仅在 Amazon EC2 实例上部署 GuardDuty 代理，此资源的 30 天免费试用期仅在 GuardDuty 收到 Amazon EC2 实例的第一个运行时事件时才会开始。稍后，当您为 Fargate（ECS 仅限亚马逊）部署 GuardDuty 代理时，只有在 GuardDuty 收到亚马逊集群的第一个运行时事件时，该资源的 30 天免费试用才会开始。ECS 考虑到您的账户已经启用了 EKS 运行时监控，请 GuardDuty 不要重置 Amazon EKS 资源的 30 天免费试用期。

关键概念-管理 GuardDuty 安全代理的方法

考虑一下可以帮助您管理 Amazon EKS 集群和 Amazon 集群上的安全代理的关键概念。ECS

内容

- [Fargate \(ECS仅限亚马逊 \) 资源-管理 GuardDuty 安全代理的方法](#)
- [Amazon EKS 集群-管理 GuardDuty 安全代理的方法](#)

Fargate (ECS仅限亚马逊) 资源-管理 GuardDuty 安全代理的方法

运行时监控为您提供了在账户中的所有 Amazon ECS 集群 (账户级别) 或部分集群 (集群级别) 上检测潜在安全威胁的选项。当您为将要运行的每个 Amazon ECS Fargate 任务启用自动代理配置时，GuardDuty 将为该任务中的每个容器工作负载添加一个边车容器。GuardDuty 安全代理被部署到这个 sidecar 容器上。通过这种方式 GuardDuty 可以了解 Amazon ECS 任务中容器的运行时行为。

运行时监控仅支持通过管理您的 Amazon ECS 集群 (AWS Fargate) 的安全代理 GuardDuty。不支持在 Amazon ECS 集群上手动管理安全代理。

在配置账户之前，请评估您希望如何管理 GuardDuty 安全代理，并有可能监控属于 Amazon ECS 任务的容器的运行时行为。考虑以下方法。

主题

- [管理所有 Amazon ECS 集群 GuardDuty 的安全代理](#)
- [管理大部分 Amazon ECS 集群 GuardDuty 的安全代理，但不包括一些 Amazon ECS 集群](#)
- [管理精选 Amazon ECS 集群 GuardDuty 的安全代理](#)

管理所有 Amazon ECS 集群 GuardDuty 的安全代理

这种方法将帮助您在账户层面检测潜在的安全威胁。如果您 GuardDuty 想检测属于您账户的所有 Amazon ECS 集群的潜在安全威胁，请使用此方法。

管理大部分 Amazon ECS 集群 GuardDuty 的安全代理，但不包括一些 Amazon ECS 集群

如果您 GuardDuty 想检测 AWS 环境中大多数 Amazon ECS 集群的潜在安全威胁，但不包括部分集群，请使用此方法。此方法可帮助您在集群级别监控 Amazon ECS 任务中容器的运行时行为。例如，属于您账户的亚马逊ECS集群数量为 1000。但是，您只想监控 930 个 Amazon ECS 集群。

此方法要求您向不想监控的 Amazon ECS 集群添加预定义 GuardDuty 标签。有关更多信息，请参阅 [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS\)](#)。

管理精选 Amazon ECS 集群 GuardDuty 的安全代理

当您想要 GuardDuty 检测某些 Amazon ECS 集群的潜在安全威胁时，请使用此方法。此方法可帮助您在集群级别监控 Amazon ECS 任务中容器的运行时行为。例如，属于您账户的亚马逊 ECS 集群数量为 1000。但是，您只想监控 230 个集群。

此方法要求您向要监控的 Amazon ECS 集群添加预定义 GuardDuty 标签。有关更多信息，请参阅 [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS\)](#)。

Amazon EKS 集群-管理 GuardDuty 安全代理的方法

GuardDuty 要在账户级别或 EKS 集群级别使用集群的运行时事件，需要管理相应集群 GuardDuty 的安全代理。

管理 GuardDuty 安全代理的方法

在 2023 年 9 月 13 日之前，您可以配置 GuardDuty 为在账户级别管理安全代理。此行为表明，默认情况下，GuardDuty 将在属于的所有 EKS 群集上管理安全代理 AWS 账户。现在，GuardDuty 提供了一种精细的功能来帮助您选择 GuardDuty 要管理安全代理的 EKS 集群。

选择后 [手动管理 GuardDuty 安全代理](#)，您仍然可以选择要监控的 EKS 集群。但是，要手动管理代理，先决条件 AWS 账户 是为您创建 Amazon VPC 终端节点。

Note

无论您使用哪种方法来管理 GuardDuty 安全代理，都始终在帐户级别启用 EKS 运行时监控。

主题

- [通过以下方式管理安全代理 GuardDuty](#)
- [手动管理 GuardDuty 安全代理](#)

通过以下方式管理安全代理 GuardDuty

GuardDuty 代表您部署和管理安全客户端。在任何时候，您都可以使用以下方法之一监控您账户中的 EKS 集群。

主题

- [监控所有集EKS群](#)
- [监控所有EKS集群并排除选择性EKS集群](#)
- [监控选择性EKS集群](#)

监控所有集EKS群

- 何时使用此方法-当您想要 GuardDuty 为账户中的所有EKS集群部署和管理安全代理时，请使用此方法。默认情况下，还 GuardDuty 会在您的账户中可能创建的新EKS集群上部署安全代理。
- 使用此方法的影响：
 - GuardDuty 创建一个 Amazon Virtual Private Cloud (AmazonVPC) 终端节点，GuardDuty 安全代理通过该终端节点将运行时事件传送到 GuardDuty。当您通过管理安全代理时，创建 Amazon VPC 终端节点不会产生额外费用 GuardDuty。
 - 您的工作节点必须具有通往活动guardduty-dataVPC终端节点的有效网络路径。GuardDuty 在您的EKS集群上部署安全代理。Amazon Elastic Kubernetes Service (EKS亚马逊) 将协调安全代理在集群内节点上的部署。EKS
 - 根据 IP 可用性，GuardDuty 选择要创建VPC端点的子网。如果您使用高级网络拓扑，则必须验证连接是否可行。
- 注意事项 — 目前，当您使用此选项时，EKS运行时监控不会创建共享VPC。

监控所有EKS集群并排除选择性EKS集群

- 何时使用此方法 — 如果您 GuardDuty 想管理账户中所有EKS集群的安全代理，但不包括部分群集，请使用此方法。EKS此方法使用基于标签的 [1](#) 方法，在这种方法中，您可以标记不想接收其运行时事件的EKS集群。预定义标签必须以 GuardDutyManaged-false 作为键值对。
- 使用此方法的影响：
 - 此方法要求只有在向要排除在监控范围之外的EKS集群添加标签后，才能启用 GuardDuty 代理自动管理。

因此，当 [通过以下方式管理安全代理 GuardDuty](#) 适用于此方法时，也会产生影响。在启用 GuardDuty 代理自动管理之前添加标签时，既 GuardDuty 不会为不受监控的EKS集群部署也不管理安全代理。

- 注意事项：

- 在启用自动代理配置之前，必须将标签键值对添加为GuardDutyManaged : false对于选定的EKS集群，否则，在使用标签之前，GuardDuty 安全代理将部署在所有EKS集群上。
- 您必须防止标签被修改，除非由可信身份修改。

Important

使用服务控制策略或IAM策略管理修改EKS集群GuardDutyManaged标签值的权限。有关更多信息，请参阅用户指南中的[服务控制策略 \(SCPs\)](#) 或AWS Organizations 用户指南中的[IAM控制 AWS 资源访问权限](#)。

- 对于您不想监控的潜在新EKS集群，请务必在创建此EKS集群时添加GuardDutyManaged-false 键值对。
- 此方法的注意事项与 [监控所有集EKS群](#) 的注意事项相同。

监控选择性EKS集群

- 何时使用此方法 — 如果您只 GuardDuty 想为账户中的部分EKS集群部署和管理安全代理更新，请使用此方法。此方法使用基于标签的 [1](#) 方法，在这种方法中，您可以标记要接收其运行时事件的EKS集群。
- 使用此方法的影响：
 - 通过使用包含标签，GuardDuty 将仅针对标有 GuardDutyManaged-true 作为键值对的选定EKS集群自动部署和管理安全代理。
 - 使用此方法的影响与 [监控所有集EKS群](#) 的影响相同。
- 注意事项：
 - 如果GuardDutyManaged标签的值未设置为true，则包含标签将无法按预期工作，这可能会影响对EKS集群的监控。
 - 为确保您选择的EKS集群受到监控，您需要防止修改标签，但可信身份除外。

Important

使用服务控制策略或IAM策略管理修改EKS集群GuardDutyManaged标签值的权限。有关更多信息，请参阅用户指南中的[服务控制策略 \(SCPs\)](#) 或AWS Organizations 用户指南中的[IAM控制 AWS 资源访问权限](#)。

- 对于您不想监控的潜在新EKS集群，请务必在创建此EKS集群时添加 GuardDutyManaged-false 键值对。
- 此方法的注意事项与 [监控所有集EKS群](#) 的注意事项相同。

¹ 有关为选定EKS集群添加标签的更多信息，请参阅《[亚马逊EKS用户指南](#)》中的[为EKS您的亚马逊资源添加标签](#)。

手动管理 GuardDuty 安全代理

- 何时使用此方法 — 如果您想在所有EKS集群上手动部署和管理 GuardDuty 安全代理，请使用此方法。确保您的账户已启用EKS运行时监控。如果您不启用EKS运行时监控，则 GuardDuty安全代理可能无法按预期运行。
- 使用这种方法的影响-您需要协调EKS集群中所有账户以及该功能可用区域 GuardDuty 的安全代理软件 AWS 区域 的部署。
- 注意事项：随着新集群和工作负载的不断部署，您必须支持安全的数据流，同时监控和消除覆盖缺口。

启用 GuardDuty 运行时监控

在您的账户中启用运行时监控之前，请确保您要监控运行时事件的资源类型支持平台要求。有关更多信息，请参阅 [先决条件](#)。

如果您在启动EKS运行时监控之前一直在使用运行时监控，则可以使用APIs来检查和更新EKS运行时监控的现有配置。您也可以将现有配置从“EKS运行时监控”迁移到“运行时监控”。有关更多信息，请参阅 [从EKS运行时监控迁移到运行时监控](#)。

Note

目前，本文档提供了仅通过控制台为您的账户和组织启用运行时监控的步骤。[也可以使用“API操作”或AWS CLI for 启用运行时监控 GuardDuty。](#)

您可以使用以下主题中的步骤配置运行时监控。

内容

- [启用运行时监控的先决条件](#)

- [为独立账户启用运行时监控](#)
- [为多账户环境启用运行时监控](#)
- [管理 GuardDuty 安全代理](#)

启用运行时监控的先决条件

要启用 Runtime Monitoring 并管理 GuardDuty 安全代理，您必须满足要监控的每种资源类型的先决条件，以进行威胁检测。

内容

- [Amazon EC2 实例支持的先决条件](#)
- [AWS Fargate \(ECS仅限 Amazon \) 支持的先决条件](#)
- [Amazon EKS 集群支持的先决条件](#)
- [将基础设施即代码 \(IaC\) 与 GuardDuty 自动安全代理一起使用](#)

Amazon EC2 实例支持的先决条件

SSM管理EC2实例

您 GuardDuty 要监控其运行时事件的 Amazon EC2 实例必须由 AWS Systems Manager (SSM) 托管。无论您是使用 GuardDuty 自动管理安全客户端还是手动管理安全客户端（除外[方法 2-使用 Linux Package Managers](#)），这都是如此。

要使用管理您的亚马逊EC2实例 AWS Systems Manager，请参阅AWS Systems Manager 用户指南中的[为亚马逊EC2实例设置 Systems Manager](#)。

验证架构要求

操作系统分发的架构可能会影响 GuardDuty 安全代理的行为。在对 Amazon EC2 实例使用运行时监控之前，您必须满足以下要求：

- 下表显示了经验证可支持 Amazon EC2 实例 GuardDuty 安全代理的操作系统分布。

操作系统发行版	内核版本	内核支持	CPU建筑
			x64 () AMD64
			Graviton () ARM64

- AL2还有 AL2 5.4、5.10、 e BPF、Trace 支持 支持
023 5.15、6.1、 points、Kpro
- Ubuntu 20.04 6.5、6.8
和 Ubuntu
22.04
- Debian 11 和
Debian 12
- 其他要求-仅当您拥有亚马逊 ECS /亚马逊时 EC2

对于亚马逊 ECS /亚马逊EC2，我们建议您使用最新的亚马逊ECS优化版AMIs（日期为 2023 年 9 月 29 日或更晚），或者使用亚马逊ECS代理版本 v1.77.0。

验证您的组织服务控制策略

如果您已设置服务控制策略 (SCP) 来管理组织中的权限，请验证权限边界是否没有限制 `guardduty:SendSecurityTelemetry`。它是支持跨不同资源类型的运行时监控所必需的。
GuardDuty

如果您是成员账户，请与关联的委托管理员建立联系。有关为您的组织 SCPs 进行管理的信息，请参阅 [服务控制策略 \(SCPs\)](#)。

使用自动代理配置时

为 [使用自动代理配置 \(推荐\)](#) 此，您 AWS 账户 必须满足以下先决条件：

- 在自动代理配置中使用包含标签时，GuardDuty 要为新实例创建 SSM 关联，请确保新实例已 SSM 被管理并显示在 <https://console.aws.amazon.com/systems-manager/> 控制台的 Fleet Manager 下。
- 在自动代理配置中使用排除标签时：
 - 在为您的账户配置 GuardDuty 自动代理之前，请添加 `GuardDutyManaged:false` 标签。

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后 EC2，任何在没有排除标签的情况下启动的 EC2 实例都将包含在 GuardDuty 自动代理配置中。

- 要使排除标签起作用，请更新实例配置，以便实例元数据服务 (IMDS) 中提供实例身份文档。执行此步骤的程序已经是您账户的一部分 [启用运行时监控](#)。

CPU和 GuardDuty 代理的内存限制

CPU限制

与 Amazon EC2 实例关联 GuardDuty 的安全代理的最大CPU限制为总数 v CPU 核心的 10%。例如，如果您的EC2实例具有 4 v CPU 内核，则安全代理最多可以使用 400% 的可用内核。

内存限制

从与您的 Amazon EC2 实例关联的内存中，GuardDuty 安全代理可以使用的内存有限。

下表显示了内存限制。

Amazon EC2 实例的内存	GuardDuty 代理的最大内存
小于 8 GB	128MB
小于 32 GB	256 MB
大于或等于 32 GB	1 GB

后续步骤

下一步是配置运行时监控并管理安全代理（自动或手动）。

AWS Fargate（ECS仅限 Amazon）支持的先决条件

验证架构要求

您使用的平台可能会影响 GuardDuty 安全代理支持 GuardDuty 从您的 Amazon ECS 集群接收运行时事件的方式。您必须验证自己使用的是其中一个经过验证的平台。

初步考虑因素：

您的亚马逊ECS集群的 AWS Fargate (Fargate) 平台必须是 Linux。相应的平台版本必须至少为1.4.0、或LATEST。有关平台版本的更多信息，请参阅《亚马逊弹性容器服务开发人员指南》中的 [Linux 平台版本](#)。

目前尚不支持 Windows 平台版本。

经过验证的平台

操作系统的分布和CPU架构会影响 GuardDuty安全代理提供的支持。下表显示了用于部署 GuardDuty安全代理和配置运行时监控的经过验证的配置。

操作系统发行版	内核支持	CPU建筑	
		x64 () AMD64	Graviton () ARM64
Linux	e BPF、Trace points、Kpro	支持	支持

提供ECR权限和子网详细信息

在启用运行时监控之前，必须提供以下详细信息：

为任务执行角色提供权限

任务执行角色要求您拥有某些亚马逊弹性容器注册表 (Amazon ECR) 权限。您可以使用 [AmazonECSTask ExecutionRolePolicy](#) 托管策略，也可以在TaskExecutionRole策略中添加以下权限：

```
...
    "ecr:GetAuthorizationToken",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage",
...

```

要进一步限制亚马逊ECR权限，您可以添加托管其 GuardDuty 安全代理URI的亚马逊ECR存储库 AWS Fargate (ECS仅限亚马逊)。有关更多信息，请参阅 [GuardDuty 代理存储库 AWS Fargate \(ECS仅限 Amazon \)](#)。

在任务定义中提供子网详细信息

您可以在任务定义中提供公有子网作为输入，也可以创建 Amazon ECR VPC 终端节点。

- 使用任务定义选项 — [UpdateServiceAPIs](#)在 Amazon 弹性容器服务API参考中运行[CreateService](#)和需要您传递子网信息。有关更多信息，请参阅《[亚马逊弹性容器服务开发者指南](#)》中的[亚马逊ECS任务定义](#)。

- 使用亚马逊ECRVPC终端节点选项-提供通往亚马逊的网络路径 ECR-URI 确保托管 GuardDuty 安全代理的亚马逊ECR存储库可通过网络访问。如果您的 Fargate 任务将在私有子网中运行，那么 Fargate 将需要网络路径来下载容器。 GuardDuty

有关启用 Fargate 下载容器的信息，请参阅[亚马逊弹性 GuardDuty 容器注册表用户指南ECS中的在亚马逊上使用亚马逊ECR镜像](#)。

验证您的组织服务控制策略

此步骤是支持运行时监控和评估不同资源类型的覆盖范围所必需的。 GuardDuty

如果您已设置服务控制策略 (SCP) 来管理组织中的权限，请验证您TaskExecutionRole及其策略guarddduty:SendSecurityTelemetry中的权限边界是否没有限制。

以下策略是允许该guarddduty:SendSecurityTelemetry策略的示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        ...,
        ...,
        "guarddduty:SendSecurityTelemetry"
      ],
      "Resource": "*"
    }
  ]
}
```

1. 使用以下步骤验证权限边界是否不受限制：guarddduty:SendSecurityTelemetry

1. 登录 AWS Management Console 并打开IAM控制台，网址为<https://console.aws.amazon.com/iam/>。
2. 在导航窗格的访问管理下，选择角色。
3. 为详细信息页面选择角色名称。
4. 展开“权限边界”部分。确保未guarddduty:SendSecurityTelemetry被拒绝或限制。

2. 使用以下步骤验证您的TaskExecutionRole策略的权限边界是否不受限制guarddduty:SendSecurityTelemetry：

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 <https://console.aws.amazon.com/iam/>。
2. 在导航窗格的访问管理下，选择策略。
3. 为详细信息页面选择策略名称。
4. 在“附加的实体”选项卡下，查看“作为权限边界附加”部分。确保未 `guardduty:SendSecurityTelemetry` 被拒绝或限制。

有关策略和权限的信息，请参阅《IAM 用户指南》中的 [权限边界](#)。

如果您是成员账户，请与关联的委托管理员建立联系。有关为您的组织 SCPs 进行管理的信息，请参阅 [服务控制策略 \(SCPs\)](#)。

CPU 和内存限制

在 Fargate 任务定义中，必须在任务级别指定 CPU 和内存值。下表显示了任务级别 CPU 和内存值的有效组合，以及相应 GuardDuty 的安全代理对容器的最大内存限制。 GuardDuty

CPU 价值	内存值	GuardDuty 代理最大内存限制
256 (.25 vCPU)	512 MiB、1 GB、2GB	128MB
512 (.5 vCPU)	1GB、2GB、3GB、4GB	
1024 (1 vCPU)	2 GB、3 GB、4 GB	
	5 GB、6 GB、7 GB、8 GB	
2048 (2 vCPU)	4GB 到 16GB 之间 (以 1GB 为增量)	
4096 (4 vCPU)	介于 8 GB 到 20 GB 之间，以 1 GB 为增量	
8192 (8 vCPU)	在 16 GB 到 28 GB 之间，以 4 GB 为增量	256 MB
	介于 32 GB 到 60 GB 之间，以 4 GB 为增量	512MB

CPU价值	内存值	GuardDuty 代理最大内存限制
16384 (16 v) CPU	32 GB 到 120 GB 之间 (以 8 GB 为增量)	1 GB

启用运行时监控并评估集群的覆盖状态是否为“正常”后，您可以设置和查看容器洞察指标。有关更多信息，请参阅 [在 Amazon ECS 集群上设置监控](#)。

下一步是配置运行时监控并配置安全代理。

Amazon EKS 集群支持的先决条件

验证架构要求

您使用的平台可能会影响 GuardDuty 安全代理支持 GuardDuty 从您的EKS集群接收运行时事件的方式。您必须验证自己使用的是其中一个经过验证的平台。如果您要手动管理 GuardDuty 代理，请确保 Kubernetes 版本支持当前正在使用的 GuardDuty 代理版本。

经过验证的平台

操作系统分布、内核版本和CPU架构会影响 GuardDuty 安全代理提供的支持。下表显示了用于部署 GuardDuty 安全代理和配置EKS运行时监控的经过验证的配置。

操作系统发行版	内核版本	内核支持	CPU建筑	支持的 Kubernetes 版本
			x64 () AMD64 Graviton () ARM64 (Graviton2 及以上) ¹	
Ubuntu AL2 AL2023 ³	5.4、5.10、 5.15、6.1 ²	e BPF Tracepoints , Kp	支持	支持 v1.21-v1.30
Bottlerocket				v1.23-v1.30

1. Amazon EKS 集群的运行时监控不支持第一代 Graviton 实例，例如 A1 实例类型。
2. 目前，在内核版本6.1中，GuardDuty无法生成[运行时监控查找类型](#)与之相关的内容[DNS事件](#)。
3. 随着 GuardDuty 安全代理 v1.6. AL2 0 及更高版本的发布，运行时监控支持 023。有关更多信息，请参阅 [GuardDuty 适用于 Amazon EKS 集群的安全代理](#)。

安全代理支持的 Kubernetes 版本 GuardDuty

下表显示了安全代理支持的EKS集群的 Kubernetes 版本。 GuardDuty

Kubernetes 版本	Amazon EKS 附加 GuardDuty 安全代理版本
1.28-1.30	v1.4.1 及更高版本
1.27	v1.3.0、v1.3.1
1.26	v1.2.0
1.21-1.25	所有版本

某些 GuardDuty 安全代理版本将终止标准支持。有关代理版本的信息，请参见[GuardDuty 适用于 Amazon EKS 集群的安全代理](#)。

CPU和内存限制

下表显示了 GuardDuty (aws-guardduty-agent) 的 Amazon EKS 附加组件CPU和内存限制。

参数	最小限制	最大限制
CPU	200m	1000m
内存	256Mi	1024Mi

当您使用 Amazon EKS 插件版本 1.5.0 或更高版本时，GuardDuty 可以根据您的CPU和内存值配置插件架构。有关可配置范围的信息，请参见[可配置的参数和值](#)。

启用EKS运行时监控并评估EKS集群的覆盖状态后，您可以设置和查看容器洞察指标。有关更多信息，请参阅 [设置CPU和内存监控](#)。

后续步骤

下一步是配置运行时监控，并通过手动或自动管理安全代理 GuardDuty。

将基础设施即代码 (IaC) 与 GuardDuty 自动安全代理一起使用

仅当以下列表适用于您的用例时，才使用此部分：

- 您可以使用基础设施即代码 (IaC) 工具（例如 AWS Cloud Development Kit (AWS CDK) 和 Terraform）来管理您的 AWS 资源，以及
- 您需要为一种或多种资源类型（亚马逊EKS、亚马逊或亚马逊 ECS-FargateEC2）启用 GuardDuty 自动代理配置。

IaC 资源依赖关系图概述

当您为资源类型启用 GuardDuty 自动代理配置时，GuardDuty 会自动创建与该VPC终端节点关联的VPC终端节点和安全组，并为该资源类型安装安全代理。默认情况下，只有在您禁用“运行时监控”后，才 GuardDuty 会删除VPC终端节点和关联的安全组。有关更多信息，请参阅 [禁用和清理资源的影响](#)。

当您使用 IaC 工具时，它会维护资源的依赖关系图。在使用 IaC 工具删除资源时，它只会删除可以作为资源依赖关系图的一部分进行跟踪的资源。IaC 工具可能不知道在其指定配置之外创建的资源。例如，您可以使用 I VPC aC 工具创建，然后使用 AWS 控制台或API操作向其中添加安全组。VPC在资源依赖关系图中，您创建的VPC资源取决于关联的安全组。如果您使用 IaC 工具删除此VPC资源，则会出现错误。解决此错误的方法是手动删除关联的安全组，或者更新 IaC 配置以包含此添加的资源。

常见问题-删除 IaC 中的资源

使用 GuardDuty 自动代理配置时，您可能需要删除使用 IaC 工具创建的资源（亚马逊EKSEC2、亚马逊或 Amazon ECS-Fargate）。但是，此资源依赖于 GuardDuty 创建的VPC端点。这可以防止 IaC 工具自行删除资源，并要求您禁用“运行时监控”，这会进一步自动删除VPC端点。

例如，当您尝试删除以您的名义 GuardDuty 创建的VPC终端节点时，您将收到与以下示例类似的错误。

Example

使用时的错误示例 CDK

The following resource(s) failed to delete:

```
[mycdkvpccapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpccapplicationprivatesubnet1Subnet1SubnetEXAMPLE1]
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPLE)
HandlerErrorCode: InvalidRequest)
```

Example

使用 Terraform 时的错误示例

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE, 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE, 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

解决方案-防止资源删除问题

本节可帮助您管理独立于的VPC终端节点和安全组 GuardDuty。

要获得使用 IaC 工具配置的资源完全所有权，请按所列顺序执行以下步骤：

1. 创建一个VPC. 要允许进入权限，请将 GuardDuty VPC终端节点与安全组相关联。VPC
2. 为您的资源类型启用 GuardDuty自动代理配置

完成上述步骤后，GuardDuty将不会创建自己的VPC终端节点，而是会重复使用您使用 IaC 工具创建的终端节点。

有关创建自己的网关的信息VPC，请参阅VPC仅在 Amazon T VPC ran [sit Gat](#) eways 中创建。有关创建VPC终端节点的信息，请参阅以下与您的资源类型对应的部分：

- 有关亚马逊的信息EC2，请参阅[手动创建亚马逊VPC终端节点](#)。
- 有关亚马逊的信息EKS，请参阅[部署 GuardDuty 安全代理的先决条件](#)。

为独立账户启用运行时监控

使用以下步骤在您的账户中启用运行时监控。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“运行时监控”。
3. 在“配置”选项卡下，选择“启用”，为您的账户启用运行时监控。
4. GuardDuty 要接收来自一种或多种资源类型（Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群）的运行时效事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理（仅限亚马逊 ECS 实例）](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

为多账户环境启用运行时监控

在多账户环境中，只有委派的 GuardDuty 管理员帐户才能为成员账户启用或禁用 Runtime Monitoring，并管理属于其组织中成员账户的资源类型的自动代理配置。GuardDuty 成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。有关多账户环境的更多信息，请参阅[管理多个账户](#)。

适用于委派 GuardDuty 管理员账号

为委派的 GuardDuty 管理员帐户启用运行时监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“运行时监控”。
3. 在“配置”选项卡下，在“运行时监视配置”部分中选择“编辑”。

4. 使用对所有账户启用

如果要为属于该组织的所有帐户（包括委派的 GuardDuty 管理员帐户）启用运行时监控，请为所有帐户选择启用。

5. 使用手动配置账户

如果要单独为每个成员帐户启用运行时监控，请选择手动配置帐户。

- 在委托管理员（此帐户）部分选择启用。

6. GuardDuty 要接收来自一种或多种资源类型（Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群）的运行时效事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理（仅限亚马逊 ECS）](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

适用于所有成员账户

为组织中的所有成员账户启用运行时监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派 GuardDuty 管理员账号登录。

2. 在导航窗格中，选择“运行时监控”。
3. 在“运行时监控”页面的“配置”选项卡下，选择“运行时监视配置”部分中的“编辑”。
4. 选择为所有账户启用。
5. GuardDuty 要接收来自一种或多种资源类型（Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群）的运行时效事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)

- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS 实例 \)](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

对于所有现有的活跃会员账户

为组织中的现有成员账户启用运行时监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用组织的委派 GuardDuty 管理员帐户登录。

2. 在导航窗格中，选择“运行时监控”。
3. 在“运行时监控”页面的“配置”选项卡下，您可以查看运行时监控配置的当前状态。
4. 在“运行时监控”窗格的“活跃成员帐户”部分下，选择“操作”。
5. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
6. 选择确认。
7. GuardDuty 要接收来自一种或多种资源类型 (Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群) 的运行时间事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS 实例 \)](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

Note

更新成员账户的配置可能最长需要 24 小时。

仅为新成员账户自动启用运行时监控

为组织中的新成员帐户启用运行时监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用组织指定的委派 GuardDuty 管理员帐户登录。

2. 在导航窗格中，选择“运行时监控”
3. 在“配置”选项卡下，在“运行时监视配置”部分中选择“编辑”。
4. 选择手动配置账户。
5. 选择为新成员账户自动启用。
6. GuardDuty 要接收来自一种或多种资源类型（Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群）的运行时效事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理（仅限亚马逊 ECS 实例）](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

仅适用于精选活跃会员账户

为单个活跃成员账户启用运行时监控

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派的 GuardDuty 管理员账户凭据登录。

2. 在导航窗格中，选择账户。
3. 在“帐户”页面上，查看“运行时监控”和“自动管理代理”列中的值。这些值表示相应帐户的运行时效监控和 GuardDuty 代理管理是启用还是未启用。
4. 从“帐户”表中，选择要为其启用运行时监控的帐户。您可以一次选择多个账户。
5. 选择确认。
6. 选择编辑保护计划。选择适当的操作。

7. 选择确认。
8. GuardDuty 要接收来自一种或多种资源类型 (Amazon EC2 实例、Amazon ECS 集群或 Amazon EKS 集群) 的运行时事件，请使用以下选项来管理这些资源的安全代理：

启用 GuardDuty 安全代理

- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS \)](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

管理 GuardDuty 安全代理

您可以管理要监控的资源 GuardDuty 的安全代理。如果要监控多种资源类型，请务必管理该资源的 GuardDuty 代理。

Important

使用 Amazon EC2 实例 GuardDuty 的安全代理时，您可以在 Amazon EKS 集群中的底层主机上安装和使用该代理。如果您已经在该 EKS 群集上部署了安全代理，则同一台主机上可能同时运行两个安全代理。有关在这种情况下 GuardDuty 的工作原理的信息，请参阅[处理双重安全代理](#)。

以下主题将帮助您完成管理安全代理的后续步骤。

内容

- [使用 VPC 与自动安全代理共享](#)
- [处理安装在主机上的双重安全代理](#)
- [管理 Amazon EC2 实例的自动安全代理](#)
- [手动管理 Amazon EC2 实例的安全代理](#)
- [管理 Fargate 的自动安全代理 \(仅限亚马逊 ECS \)](#)
- [自动管理 Amazon EKS 集群的安全代理](#)
- [手动管理 Amazon EKS 集群的安全代理](#)

使用VPC与自动安全代理共享

当您选择 GuardDuty 自动管理安全代理时，Runtime Monitorin VPC g 支持在中 AWS 账户 属于同一组织的共享客户端 AWS Organizations。GuardDuty 可以代表您根据与您的组织共享VPC内容相关的详细信息设置 Amazon VPC 终端节点政策。

在此版本之前，VPCs仅当您选择手动管理 GuardDuty 安全客户端时，才 GuardDuty 支持使用共享。

内容

- [工作方式](#)
- [使用共享的先决条件 VPC](#)
- [常见问题 \(FAQs\)](#)

工作方式

当共享的所有者账户为任何资源（Amazon EKS 或 AWS Fargate（ECS仅限 Amazon））VPC启用运行时监控和自动代理配置时，所有共享资源都有VPCs资格在共享所有VPC者账户中自动安装共享的亚马逊VPC终端节点和关联的安全组。GuardDuty 检索与共享的 Amazon VPC 关联的组织 ID。

现在，与共享的亚马逊VPC所有者账户属于同一组织的用户也可以共享相同的亚马逊VPC终端节点。AWS 账户 GuardDuty VPC当共享VPC所有者账户或参与账户需要 Amazon VPC 终端节点时创建共享。需要亚马逊VPC终端节点的示例包括启用 GuardDuty、运行时监控、EKS运行时监控或启动新的 Amazon ECS-Fargate 任务。当这些账户为任何资源类型启用运行时监控和自动代理配置时，GuardDuty 会创建一个 Amazon VPC 终端节点，并使用与共享VPC所有者账户相同的组织 ID 设置终端节点策略。GuardDuty 为 GuardDuty 创建的 Amazon VPC 终端节点添加GuardDutyManaged标签并将其设置为。true如果共享的 Amazon VPC 所有者账户尚未为任何资源启用运行时监控或自动代理配置，则 GuardDuty 不会设置亚马逊VPC终端节点策略。有关在共享VPC所有者帐户中配置运行时监控和自动管理安全代理的信息，请参阅[启用 GuardDuty 运行时监控](#)。

使用相同亚马逊VPC终端节点策略的每个账户都被称为关联共享亚马逊的参与者 AWS 账户VPC。

以下示例显示了共享VPC所有者账户和参与者账户的默认VPC终端节点策略。aws:PrincipalOrgID将显示与共享VPC资源关联的组织 ID。本政策仅限于所有者账户组织中存在的参与者账户。

Example

```
{
```

```
"Version": "2012-10-17",
"Statement": [{
  "Action": "*",
  "Resource": "*",
  "Effect": "Allow",
  "Principal": "*"
},
{
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalOrgID": "o-abcdef0123"
    }
  },
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Principal": "*"
}
]
```

使用共享的先决条件 VPC

初始设置的先决条件

要成为共享的所有者 AWS 账户，请在中执行以下步骤VPC：

1. 创建组织-按照《AWS Organizations 用户指南》中[创建和管理组织](#)中的步骤创建组织。

有关添加或删除成员账户的信息，请参阅在[组织 AWS 账户 中管理](#)。

2. 创建共享VPC资源-您可以通过所有者账户创建共享VPC资源。有关更多信息，请参阅 Amazon VPC 用户指南中的[VPC与其他账户共享您的账户](#)。

特定于 GuardDuty运行时监控的先决条件

以下列表提供了特定于以下各项的先决条件 GuardDuty：

- 共享账户VPC和参与账户的所有者账户可以来自不同的组织 GuardDuty。但是，他们必须属于同一个组织 AWS Organizations。这是 GuardDuty 为共享端点创建 Amazon VPC 终端节点和安全组所必需的VPC。有关共享VPCs工作方式的信息，请参阅 Amazon VPC 用户指南中的[VPC与其他账户共享您的账户](#)。

- 为共享VPC所有者账户和参与者账户中的任何资源启用EKS运行时监控或运行时监控，以及 GuardDuty 自动代理配置。有关更多信息，请参阅 [启用运行时监控](#)。

如果您已经完成了这些配置，请继续下一步。

- 在处理 Amazon EKS 或 Amazon ECS (AWS Fargate 仅限) 任务时，请务必选择与所有者账户关联的共享VPC资源并选择其子网。

常见问题 (FAQs)

以下列表提供了在运行时监控中使用启用了 GuardDuty 自动代理配置的共享VPC资源时常见问题的故障排除步骤：

我已经在使用运行时监控 (或EKS运行时监控)。如何启用共享VPC？

有关创建共享的先决条件的信息VPC，请参阅[先决条件](#)。

当共享VPC所有者账户和参与者账户都满足先决条件时，GuardDuty 将尝试自动设置 Amazon VPC 终端节点策略。

如果在此版本之前，您 AWS 账户 遇到了VPC不支持共享内容的覆盖问题，请遵循先决条件。当您的资源类型 (仅限 Amazon EKS 或 Amazon ECS (AWS Fargate 仅限) 任务) 调用共享VPC终端节点要求时，GuardDuty 将尝试设置新的VPC终端节点策略。

作为共享VPC所有者账户，我希望共享VPC终端节点策略仅限于我组织中的一部分参与者账户。我该怎么办？

如果您有GuardDutyManaged:true标签与终端节点关联，请将其删除。这样可以 GuardDuty 防止尝试修改或覆盖共享VPC的VPC端点策略。

有关更多信息，请参阅[使用VPC终端节点策略控制对终端节点的访问](#)。

为什么共享VPC端节点从修改aws:PrincipalAccount为aws:PrincipalOrgId？我怎样才能防止这种情况发生？

当 GuardDuty 检测到由同一组织的多个账户共享时 AWS Organizations，GuardDuty 会尝试修改策略以指定组织 ID。VPC

为防止出现这种情况，请从共享VPC终端节点中删除GuardDutyManaged:true标签。这样可以 GuardDuty 防止尝试修改或覆盖共享VPC的VPC端点策略。

当共享VPC所有者账户或其中一个参与者账户禁用运行时监控 (GuardDuty 或EKS运行时监控) 时会发生什么？

当共享VPC所有者账户禁用 GuardDuty 或运行时监控 (或EKS运行时监控) 时， GuardDuty会检查属于参与者账户的任何资源类型是否使用过共享VPC端点，或者任何参与者账户是否曾经为任何资源类型启用 GuardDuty 代理管理。如果是，则 GuardDuty 不会删除共享VPC端节点和安全组。

如果共享VPC参与者帐户禁用 GuardDuty 或运行时监控 (或EKS运行时监控) ，则不会对共享VPC所有者帐户产生任何影响，所有者帐户既不会删除共享VPC资源，也不会删除安全组。

如何删除共享VPC资源？它将产生什么影响？

作为共享VPC所有者账户，即使您的账户或运行时监控中的任何参与账户正在使用共享VPC资源，您也可以将其删除。有关删除共享内容VPC和了解其影响的信息，请参阅[To delete a VPC endpoint](#)。

处理安装在主机上的双重安全代理

Amazon EC2 实例可以支持多种类型的工作负载。当您在 Amazon EC2 实例上配置自动安全代理时，同一个EC2实例可能会通过另一个安全代理EKS。

概述

假设您启用了运行时监控的场景。现在，您可以EKS通过为 Amazon 启用自动代理 GuardDuty。您还为 Amazon 启用了自动代理EC2。可能会发生这样的情况：同一台底层主机安装了两个安全代理，一个用于亚马逊EKS，另一个用于亚马逊EC2。这可能导致两个安全代理在同一主机内运行，收集运行时事件并将其发送到 GuardDuty，并可能生成重复的发现。

影响

- 当在同一台主机上运行多个安全代理时，您的账户可能会遇到双倍的内存处理量CPU和内存处理需求。有关每种资源类型的CPU和内存限制的信息，[先决条件](#) 请参见该资源的相关信息。
- GuardDuty 在设计运行时监控功能时，即使两个安全代理从同一底层主机收集运行时事件存在重叠，也只会向您的账户收取一个运行时事件流的费用。

如何 GuardDuty 处理多个代理

GuardDuty 检测两个安全客户端何时在同一台主机上运行，并仅将其中一个指定为主动收集运行时事件的安全代理。第二个代理将消耗最少的系统资源，以防止对应用程序性能产生任何影响。

GuardDuty 考虑了以下场景：

- 当EC2实例同时属于 Amazon EKS 和 Amazon EC2 安全代理的范围时，EKS安全代理优先。这仅适用于您使用适用于 Amazon 的安全代理 v1.1.0 或更高版本。EC2较旧的代理版本将继续运行并收集运行时事件，因为较旧的代理版本不受优先级的影响。
- 当 Amazon EKS 和 Amazon EC2 都 GuardDuty 托管安全代理并且您的亚马逊EC2实例也处于SSM托管状态时，两个安全代理都将安装在主机级别。安装代理后，GuardDuty 决定哪个安全代理将继续运行。当两个安全代理都在运行时，最终只有一个会收集运行时事件。
- 当EC2与两者关联的安全代理同时EKS运行时，GuardDuty 可能仅在重叠期间生成重复的发现结果。

这种情况可能在以下情况下发生：

- 两者的安全代理EC2EKS均通过 GuardDuty（自动）进行配置，或者
- 您的 Amazon EKS 资源有自动安全代理。
- 当EKS安全代理已在运行时，如果您在同一台底层主机上手动部署EC2安全代理并满足所有先决条件，则 GuardDuty 可能无法安装第二个安全代理。

管理 Amazon EC2 实例的自动安全代理

Note

在继续之前，请务必遵循所有内容[Amazon EC2 实例支持的先决条件](#)。

从 Amazon EC2 手动代理迁移到自动代理

AWS 账户 如果您以前手动管理安全客户端，现在想要使用 GuardDuty 自动代理配置，则本节适用于您。如果这不适用于您，请继续为您的账户配置安全代理。

启用 GuardDuty 自动代理后，将代表您 GuardDuty 管理安全客户端。有关 GuardDuty 采取了哪些步骤的信息，请参阅[使用自动代理配置（推荐）](#)。

清理资源

删除SSM关联

- 删除您在EC2手动管理 Amazon 安全代理时可能创建的任何SSM关联。有关更多信息，请参阅[删除关联](#)。

- 这样做是为了让无论您是在账户级别还是实例级别使用自动代理（通过使用包含或排除标签），GuardDuty 都可以接管SSM操作的管理。有关可以SSM执行哪些操作的更多信息 GuardDuty，请参阅[的服务相关角色权限 GuardDuty](#)。
- 删除先前为手动管理安全代理而创建的SSM关联时，在创建用于自动管理安全客户端的SSM关联时 GuardDuty，可能会有短暂的重叠期。在此期间，您可能会遇到基于日SSM程安排的冲突。有关更多信息，请参阅 [Amazon EC2 SSM 日程安排](#)。

管理您的 Amazon EC2 实例的包含和排除标签

- 包含标签 — 如果您不启用 GuardDuty 自动代理配置，但使用包含标签 (GuardDutyManaged:true) 标记您的任何 Amazon EC2 实例，则会 GuardDuty 创建一个SSM 关联，该关联将在选定EC2实例上安装和管理安全代理。这是一种预期行为，可帮助您仅在选定 EC2实例上管理安全代理。有关更多信息，请参阅 [运行时监控如何与 Amazon EC2 实例配合使用](#)。

要防止 GuardDuty 安装和管理安全客户端，请从这些EC2实例中移除包含标签。有关更多信息，请参阅 Amazon EC2 用户指南中的[添加和删除标签](#)。

- 排除标签 — 当您想要为账户中的所有EC2实例启用 GuardDuty 自动代理配置时，请确保没有 EC2实例使用排除标签 (GuardDutyManaged:false) 进行标记。

为独立账户配置 GuardDuty 代理

Configure for all instances

为独立账户中的所有实例配置运行时监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“运行时监控”。
3. 在配置选项卡下，选择编辑。
4. 在该EC2部分中，选择启用。
5. 选择保存。
6. 您可以验证 GuardDuty 创建的SSM关联是否会在属于您账户的所有EC2资源上安装和管理安全代理。
 - a. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。

- b. 打开SSM关联的“目标”选项卡 (GuardDutyRuntimeMonitoring-do-not-delete)。请注意，Tag 键显示为InstanceIds。

Using inclusion tag in selected instances

为选定的 Amazon EC2 实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开亚马逊EC2控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:true标签添加到 GuardDuty 要监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。
3. 您可以验证 GuardDuty 创建的SSM关联是否仅在标有包含标签的EC2资源上安装和管理安全代理。

打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。

- 打开已创建的SSM关联的“目标”选项卡 (GuardDutyRuntimeMonitoring-do-not-delete)。标签键显示为标签:GuardDutyManaged。

Using exclusion tag in selected instances

Note

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后EC2，任何在没有排除标签的情况下启动的EC2实例都将包含在 GuardDuty 自动代理配置中。

为选定的 Amazon EC2 实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开亚马逊EC2控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:false标签添加到您不 GuardDuty 想监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。

3. [要使排除标签在实例元数据中可用](#)，请执行以下步骤：
 - a. 在实例的详细信息选项卡下，查看允许在实例元数据中添加标签的状态。

如果当前已禁用，请使用以下步骤将其状态更改为“已启用”。否则，请跳过此步骤。
 - b. 选择您要允许为其添加标签的实例。
 - c. 在“操作”菜单下，选择“实例设置”。
 - d. 选择允许在实例元数据中添加标签。
 - e. 在“访问实例元数据中的标签”下，选择“允许”。
 - f. 选择保存。
4. 添加排除标签后，执行与为所有实例配置选项卡中指定的相同步骤。

现在，您可以评估运行时间[Amazon EC2 实例的覆盖范围](#)。

在多 GuardDuty 账户环境中配置代理

适用于委派 GuardDuty 管理员账号

Configure for all instances

如果您选择“为所有帐户启用运行时监控”，则为委派的 GuardDuty 管理员帐户选择以下选项之一：

- 选项 1

在“自动代理配置”下，在“为所有账户启用” EC2部分中，选择“为所有账户启用”。

- 选项 2

- 在“自动代理配置”下，在“手动配置帐户” EC2部分中，选择“手动配置帐户”。

- 在“委派管理员（此帐户）”下，选择“启用”。

- 选择保存。

如果您为运行时监控选择了手动配置帐户，请执行以下步骤：

- 在“自动代理配置”下，在“手动配置帐户” EC2部分中，选择“手动配置帐户”。

- 在“委派管理员（此帐户）”下，选择“启用”。

- 选择保存。

无论您选择哪个选项为委派 GuardDuty 管理员帐户启用自动代理配置，您都可以验证 GuardDuty 创建的SSM关联是否将在属于该账户的所有EC2资源上安装和管理安全客户端。

1. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
2. 打开SSM关联的“目标”选项卡 (GuardDutyRuntimeMonitoring-do-not-delete)。请注意，Tag 键显示为InstanceIds。

Using inclusion tag in selected instances

为选定的 Amazon EC2 实例配置 GuardDuty 代理

1. 登录 AWS Management Console 并打开亚马逊EC2控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:true标签添加到 GuardDuty 要监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。

添加此标签将 GuardDuty 允许为这些选定EC2实例安装和管理安全代理。您无需明确启用自动代理配置。

3. 您可以验证 GuardDuty 创建的SSM关联是否仅在标有包含标签的EC2资源上安装和管理安全代理。

打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。

- 打开已创建的SSM关联的“目标”选项卡 (GuardDutyRuntimeMonitoring-do-not-delete)。标签键显示为标签:GuardDutyManaged。

Using exclusion tag in selected instances

Note

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后EC2，任何在没有排除标签的情况下启动的EC2实例都将包含在 GuardDuty 自动代理配置中。

为选定的 Amazon EC2 实例配置 GuardDuty 代理

1. 登录 AWS Management Console 并打开亚马逊EC2控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:false标签添加到您不 GuardDuty 想监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。
3. [要使排除标签在实例元数据中可用](#)，请执行以下步骤：
 - a. 在实例的详细信息选项卡下，查看允许在实例元数据中添加标签的状态。

如果当前已禁用，请使用以下步骤将其状态更改为“已启用”。否则，请跳过此步骤。
 - b. 在“操作”菜单下，选择“实例设置”。
 - c. 选择允许在实例元数据中添加标签。
4. 添加排除标签后，执行与为所有实例配置选项卡中指定的相同步骤。

现在，您可以评估运行时间[Amazon EC2 实例的覆盖范围](#)。

为所有成员账户自动启用

Note

更新成员账户的配置可能最长需要 24 小时。

Configure for all instances

以下步骤假设您在“运行时监控”部分为所有账户选择了“启用”：

1. 在 Amazon 的自动代理配置部分中，为所有账户选择“启用” EC2。
2. 您可以验证 GuardDuty 创建 (GuardDutyRuntimeMonitoring-do-not-delete) 的SSM 关联是否将在属于该账户的所有EC2资源上安装和管理安全代理。
 - a. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
 - b. 打开SSM关联的“目标”选项卡。请注意，T ag 键显示为InstanceIds。

Using inclusion tag in selected instances

为选定的 Amazon EC2 实例配置 GuardDuty 代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:true标签添加到 GuardDuty 要监控和检测潜在威胁的EC2实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。

添加此标签将 GuardDuty 允许为这些选定EC2实例安装和管理安全代理。您无需明确启用自动代理配置。

3. 您可以验证 GuardDuty 创建的SSM关联是否会在属于您账户的所有EC2资源上安装和管理安全代理。
 - a. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
 - b. 打开SSM关联的“目标”选项卡 (GuardDutyRuntimeMonitoring-do-not-delete)。请注意，Tag 键显示为InstanceIds。

Using exclusion tag in selected instances

Note

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后EC2，任何在没有排除标签的情况下启动的EC2实例都将包含在 GuardDuty 自动代理配置中。

为选定的 Amazon EC2 实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:false标签添加到您不 GuardDuty 想监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。
3. [要使排除标签在实例元数据中可用](#)，请执行以下步骤：
 - a. 在实例的详细信息选项卡下，查看允许在实例元数据中添加标签的状态。

如果当前已禁用，请使用以下步骤将其状态更改为“已启用”。否则，请跳过此步骤。

- b. 在“操作”菜单下，选择“实例设置”。
 - c. 选择允许在实例元数据中添加标签。
4. 添加排除标签后，执行与为所有实例配置选项卡中指定的相同步骤。

现在，您可以评估运行时间[Amazon EC2 实例的覆盖范围](#)。

仅限新成员账户自动启用

委托 GuardDuty 管理员账户可以将 Amazon EC2 资源的自动代理配置设置为在新成员账户加入组织时自动启用。

Configure for all instances

以下步骤假设您在“运行时监控”部分下选择了“自动为新成员帐户启用”：

1. 在导航窗格中，选择“运行时监控”。
2. 在“运行时监控”页面上，选择“编辑”。
3. 选择为新成员账户自动启用。此步骤可确保每当有新账户加入您的组织时，系统EC2都会自动为其账户启用 Amazon 的自动代理配置。只有组织的委派 GuardDuty 管理员帐户可以修改此选择。
4. 选择保存。

当新的成员账户加入组织时，将自动为他们启用此配置。GuardDuty 要管理属于此新成员账户的 Amazon EC2 实例的安全代理，请确保满足[EC2例如](#)所有先决条件。

创建SSM关联后 (GuardDutyRuntimeMonitoring-do-not-delete)，您可以验证该SSM协会是否将在属于新成员账户的所有EC2实例上安装和管理安全代理。

- 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
- 打开SSM关联的“目标”选项卡。请注意，Tag 键显示为Instancelds。

Using inclusion tag in selected instances

为账户中的选定实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:true标签添加到 GuardDuty 要监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。

添加此标签将 GuardDuty 允许为这些选定实例安装和管理安全代理。您无需明确启用自动代理配置。

3. 您可以验证 GuardDuty 创建的SSM关联是否仅在标有包含标签的EC2资源上安装和管理安全代理。
 - a. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
 - b. 打开已创建的SSM关联的“目标”选项卡。标签键显示为标签:GuardDutyManaged。

Using exclusion tag in selected instances

Note

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后EC2，任何在没有排除标签的情况下启动的EC2实例都将包含在 GuardDuty 自动代理配置中。

为独立账户中的特定实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:false标签添加到您不 GuardDuty 想监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。
3. [要使排除标签在实例元数据中可用](#)，请执行以下步骤：
 - a. 在实例的详细信息选项卡下，查看允许在实例元数据中添加标签的状态。

如果当前已禁用，请使用以下步骤将其状态更改为“已启用”。否则，请跳过此步骤。

- b. 在“操作”菜单下，选择“实例设置”。
 - c. 选择允许在实例元数据中添加标签。
4. 添加排除标签后，执行与为所有实例配置选项卡中指定的相同步骤。

现在，您可以评估运行时间[Amazon EC2 实例的覆盖范围](#)。

仅限精选成员账户

Configure for all instances

1. 在账户页面上，选择要为其启用运行时监控-自动代理配置 (Amazon EC2 zon) 的一个或多个账户。确保您在此步骤中选择的帐户已启用运行时监控。
2. 在编辑保护计划中，选择相应的选项以启用运行时监控-自动代理配置 (Amazon EC2 zon)。
3. 选择确认。


Using inclusion tag in selected instances

为选定实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 将GuardDutyManaged:true标签添加到 GuardDuty 要监控和检测潜在威胁的实例。有关添加此标签的信息，请参阅[为单个资源添加标签](#)。

添加此标签将 GuardDuty 允许您管理已标记的 Amazon EC2 实例的安全代理。您无需明确启用自动代理配置 (运行时监控-自动代理配置 (EC2))。

Using exclusion tag in selected instances

 Note

在启动 Amazon EC2 实例之前，请务必将排除标签添加到这些实例。在您为 Amazon 启用自动代理配置后EC2，任何在没有排除标签的情况下启动的EC2实例都将包含在 GuardDuty 自动代理配置中。

为选定实例配置 GuardDuty 安全代理

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为 <https://console.aws.amazon.com/ec2/>。
2. 将 GuardDutyManaged:false 标签添加到您不 GuardDuty 想监控或检测潜在威胁的 EC2 实例。有关添加此标签的信息，请参阅 [为单个资源添加标签](#)。
3. [要使排除标签在实例元数据中可用](#)，请执行以下步骤：
 - a. 在实例的详细信息选项卡下，查看允许在实例元数据中添加标签的状态。
如果当前已禁用，请使用以下步骤将其状态更改为“已启用”。否则，请跳过此步骤。
 - b. 在“操作”菜单下，选择“实例设置”。
 - c. 选择允许在实例元数据中添加标签。
4. 添加排除标签后，执行与为所有实例配置选项卡中指定的相同步骤。

你现在可以评估了 [Amazon EC2 实例的覆盖范围](#)。

手动管理 Amazon EC2 实例的安全代理

启用运行时监控后，您需要手动安装 GuardDuty 安全代理。安装代理后，GuardDuty 将接收来自 Amazon EC2 实例的运行时事件。

要管理 GuardDuty 安全代理，您必须创建一个 Amazon VPC 终端节点，然后按照步骤手动安装安全代理。

手动创建亚马逊VPC终端节点

在安装 GuardDuty 安全代理之前，必须先创建亚马逊虚拟私有云 (AmazonVPC) 终端节点。这将有助于 GuardDuty 接收您的 Amazon EC2 实例的运行时事件。

Note

使用VPC终端节点不会产生额外费用。

创建 Amazon VPC 终端节点

1. 登录 AWS Management Console 并打开 Amazon VPC 控制台，网址为 <https://console.aws.amazon.com/vpc/>。

2. 在导航窗格的VPC私有云下，选择终端节点。
3. 选择 Create Endpoint (创建端点) 。
4. 在创建端点页面上，对于服务类别，选择其他端点服务。
5. 对于服务名称，输入 **com.amazonaws.us-east-1.guardduty-data**。

请务必更换 *us-east-1* 和你的 AWS 区域. 该区域必须与属于您的 AWS 账户 ID 的 Amazon EC2 实例位于同一区域。

6. 选择验证服务。
7. 成功验证服务名称后，选择您的实例所在VPC的位置。添加以下政策，仅限指定账户使用亚马逊 VPC终端节点。使用此策略下面提供的组织 Condition，您可以更新以下策略来限制对端点的访问。要向组织IDs中的特定账户提供 Amazon VPC 终端节点支持，请参阅[Organization condition to restrict access to your endpoint](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

aws:PrincipalAccount 账户 ID 必须与包含VPC和VPC端点的账户相匹配。以下列表显示了如何与其他 AWS 账户共享VPC终端节点IDs：

- 要指定多个账户来访问VPC终端节点，请"aws:PrincipalAccount: "111122223333"替换为以下方块：

```
"aws:PrincipalAccount": [  
    "666666666666",  
    "555555555555"  
]
```

请务必将该 AWS 账户IDs替换为需要访问VPC终端节点的账户的账户。IDs

- 要允许组织中的所有成员访问VPC终端节点，请"aws:PrincipalAccount: "111122223333"替换为以下行：

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

一定要更换组织 *o-abcdef0123* 使用您的组织 ID。

- 要限制通过组织 ID 访问资源，请将您的ResourceOrgID添加到策略中。有关更多信息，请参阅[aws:ResourceOrgID](#) 《IAM用户指南》。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 在“其他设置”下，选择“启用DNS名称”。
9. 在子网下，选择您的实例所在的子网。
10. 在安全组下，选择一个已从您的VPC（或您的 Amazon EC2 实例）启用入站端口 443 的安全组。如果您还没有启用入站端口 443 的安全组，请参阅 Amazon EC2 用户指南中的[创建安全组](#)。

如果在限制您的VPC（或实例）的入站权限时出现问题，请为来自任何 IP 地址的入站 443 端口提供支持。（0.0.0.0/0）

手动安装安全客户端

GuardDuty 提供了以下两种在您的 Amazon EC2 实例上安装 GuardDuty 安全代理的方法：

- 方法 1-通过使用 AWS Systems Manager -此方法需要 AWS Systems Manager 管理您的 Amazon EC2 实例。
- 方法 2-使用 Linux Package Managers — 无论您的亚马逊EC2实例是否处于 AWS Systems Manager 托管状态，您都可以使用此方法。

方法 1-通过使用 AWS Systems Manager

要使用此方法，请确保您的 Amazon EC2 实例处于 AWS Systems Manager 托管状态，然后安装代理。

AWS Systems Manager 托管亚马逊EC2实例

使用以下步骤 AWS Systems Manager 管理您的 Amazon EC2 实例。

- [AWS Systems Manager](#)帮助您管理 AWS 应用程序和资源 end-to-end 并实现大规模的安全运营。

要使用管理您的亚马逊EC2实例 AWS Systems Manager，请参阅AWS Systems Manager 用户指南中的[为亚马逊EC2实例设置 Systems Manager](#)。

- 下表显示了新的 GuardDuty 托管 AWS Systems Manager 文档：

文档名称	文档类型	用途
AmazonGuardDuty-RunTimeMonitoringSsmPlugin	Distributor	打包 GuardDuty 安全客户端。
AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin	命令	运行安装/卸载脚本来安装安全客户端。 GuardDuty

有关更多信息 AWS Systems Manager，请参阅《AWS Systems Manager 用户指南》中的 [Amazon EC2 Systems Manager 文档](#)。

适用于 Debian 服务器

提供的适用于 Debian 服务器的 Amazon 机器映像 (AMIs) AWS 要求您安装 AWS Systems Manager 代理 (代SSM理)。您需要执行额外的步骤来安装SSM代理，以便SSM管理您的 Amazon EC2 Debian 服务器实例。有关您需要采取的步骤的信息，请参阅《AWS Systems Manager 用户指南》中的“[在 Debian Server 实例上手动安装SSM代理](#)”。

使用以下方法为 Amazon EC2 实例安装 GuardDuty 代理 AWS Systems Manager

1. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
2. 在导航窗格中，选择“文档”
3. 在 Owned by Amazon 中，选择 AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin。
4. 选择 Run Command。
5. 输入以下“运行命令”参数
 - 操作：选择“安装”。
 - 安装类型：选择“安装”或“卸载”。
 - 名称: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
 - 版本：如果此处仍为空，您将获得最新版本 GuardDuty 的安全客户端。有关发行版本的更多信息，请参阅[GuardDuty Amazon EC2 实例的安全代理](#)。
6. 选择目标的 Amazon EC2 实例。您可以选择一个或多个 Amazon EC2 实例。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的[从控制台 AWS Systems Manager 运行命令](#)
7. 验证 GuardDuty 代理安装是否正常。有关更多信息，请参阅[正在验证 GuardDuty 安全代理安装状态](#)。

方法 2-使用 Linux Package Managers

使用此方法，您可以通过运行 RPM 脚本或 Debian 脚本来安装 GuardDuty 安全代理。根据操作系统，您可以选择首选方法：

- 使用 RPM 脚本在操作系统发行版 AL2 或 AL2 023 上安装安全代理。
- 使用 Debian 脚本在操作系统发行版 Ubuntu 或 Debian 上安装安全代理。有关支持的 Ubuntu 和 Debian 操作系统发行版的信息，请参阅[验证架构要求](#)

RPM installation

Important

我们建议先验证 GuardDuty 安全代理 RPM 签名，然后再将其安装到您的计算机上。

1. 验证 GuardDuty 安全代理RPM签名

a. 准备模板

使用适当的公钥、x86_64 的签名、arm64 RPM RPM 4 的签名以及指向 Amazon S3 存储桶中托管的RPM脚本的相应访问链接来准备命令。替换 AWS 区域、AWS 账户 ID 和 GuardDuty 代理版本的值以访问RPM脚本。

- 公钥：

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem
```

- GuardDuty 安全代理RPM签名：

x86_64 的签名 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig
```

arm64 的签名 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- 访问 Amazon S3 存储桶中RPM脚本的链接：

x86_64 的访问链接 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm
```

arm64 的访问链接 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.rpm
```

AWS 区域	区域名称	AWS 账号
eu-west-1	欧洲地区 (爱尔兰)	694911143906

us-east-1	美国东部 (弗吉尼亚州北部)	593207742271
us-west-2	美国西部 (俄勒冈州)	733349766148
eu-west-3	欧洲地区 (巴黎)	665651866788
us-east-2	美国东部 (俄亥俄州)	307168627858
eu-central-1	欧洲地区 (法兰克福)	323658145986
ap-northeast-2	亚太地区 (首尔)	914738172881
eu-north-1	欧洲地区 (斯德哥尔摩)	591436053604
ap-east-1	亚太地区 (香港)	258348409381
me-south-1	中东 (巴林)	536382113932
eu-west-2	欧洲地区 (伦敦)	892757235363
ap-northeast-1	Asia Pacific (Tokyo)	533107202818
ap-southeast-1	亚太地区 (新加坡)	174946120834
ap-south-1	亚太地区 (孟买)	251508486986
ap-southeast-3	亚太地区 (雅加达)	510637619217
sa-east-1	南美洲 (圣保罗)	758426053663
ap-northeast-3	亚太地区 (大阪)	273192626886
eu-south-1	欧洲地区 (米兰)	266869475730
af-south-1	非洲 (开普敦)	197869348890
ap-southeast-2	亚太地区 (悉尼)	005257825471
me-central-1	中东 (UAE)	000014521398

us-west-1	美国西部 (加利福尼亚北部)	684579721401
ca-central-1	加拿大 (中部)	354763396469
ca-west-1	加拿大西部 (卡尔加里)	339712888787
ap-south-2	亚太地区 (海得拉巴)	950823858135
eu-south-2	欧洲 (西班牙)	919611009337
eu-central-2	欧洲 (苏黎世)	529164026651
ap-southeast-4	亚太地区 (墨尔本)	251357961535
il-central-1	以色列 (特拉维夫)	870907303882

b. 下载模板

在以下命令中，要下载相应的公钥、x86_64 的签名RPM、arm64 RPM 4 的签名以及 Amazon S3 存储桶中托管的RPM脚本的相应访问链接，请务必将账户 ID 替换为相应 AWS 账户 的 ID，将区域替换为您当前的区域。

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm ./amazon-guardduty-agent-1.3.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig ./amazon-guardduty-agent-1.3.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem ./publickey.pem
```

c. 导入公钥

使用以下命令将公钥导入数据库：

```
gpg --import publickey.pem
```

gpg 显示导入成功

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
```

```
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. 验证签名

使用以下命令验证签名

```
gpg --verify amazon-guardduty-agent-1.3.0.x86_64.sig amazon-guardduty-agent-1.3.0.x86_64.rpm
```

如果验证通过，您将看到一条类似于以下结果的消息。现在，您可以使用继续安装 GuardDuty 安全客户端RPM。

输出示例：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

如果验证失败，则意味着签名可能RPM已被篡改。您必须从数据库中删除公钥并重试验证过程。

例如：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

使用以下命令从数据库中删除公钥：

```
gpg --delete-keys AwsGuardDuty
```

现在，再次尝试验证过程。

2. [SSH从 Linux 或 macOS 上连接](#)。
3. 使用以下命令安装 GuardDuty 安全代理：

```
sudo rpm -ivh amazon-guardduty-agent-1.3.0.x86_64.rpm
```

4. 验证 GuardDuty 代理安装是否正常。有关这些步骤的更多信息，请参阅[正在验证 GuardDuty 安全代理安装状态](#)。

Debian installation

Important

我们建议先验证 GuardDuty 安全代理 Debian 签名，然后再将其安装到您的计算机上。

1. 验证 GuardDuty 安全代理 Debian 签名

- a. 为相应的公钥、amd64 Debian 软件包的签名、arm64 Debian 软件包的签名以及 Amazon S3 存储桶中托管的 Debian 脚本的相应访问链接准备模板

在以下模板中，替换 AWS 账户 ID 和 GuardDuty 代理版本的值以访问 Debian 软件包脚本。AWS 区域

- 公钥：

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/  
publickey.pem
```

- GuardDuty 安全代理 Debian 签名：

amd64 的签名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/  
amazon-guardduty-agent-1.3.0.amd64.sig
```

arm64 的签名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/  
amazon-guardduty-agent-1.3.0.arm64.sig
```

- 访问 Amazon S3 存储桶中 Debian 脚本的链接：

amd64 的访问链接

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/  
amazon-guardduty-agent-1.3.0.amd64.deb
```

arm64 的访问链接

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.deb
```

AWS 区域	区域名称	AWS 账号
eu-west-1	欧洲地区 (爱尔兰)	694911143906
us-east-1	美国东部 (弗吉尼亚州北部)	593207742271
us-west-2	美国西部 (俄勒冈州)	733349766148
eu-west-3	欧洲地区 (巴黎)	665651866788
us-east-2	美国东部 (俄亥俄州)	307168627858
eu-central-1	欧洲地区 (法兰克福)	323658145986
ap-northeast-2	亚太地区 (首尔)	914738172881
eu-north-1	欧洲地区 (斯德哥尔摩)	591436053604
ap-east-1	亚太地区 (香港)	258348409381
me-south-1	中东 (巴林)	536382113932
eu-west-2	欧洲地区 (伦敦)	892757235363
ap-northeast-1	Asia Pacific (Tokyo)	533107202818
ap-southeast-1	亚太地区 (新加坡)	174946120834
ap-south-1	亚太地区 (孟买)	251508486986
ap-southeast-3	亚太地区 (雅加达)	510637619217
sa-east-1	南美洲 (圣保罗)	758426053663

ap-northeast-3	亚太地区 (大阪)	273192626886
eu-south-1	欧洲地区 (米兰)	266869475730
af-south-1	非洲 (开普敦)	197869348890
ap-southeast-2	亚太地区 (悉尼)	005257825471
me-central-1	中东 (UAE)	000014521398
us-west-1	美国西部 (加利福尼亚北部)	684579721401
ca-central-1	加拿大 (中部)	354763396469
ca-west-1	加拿大西部 (卡尔加里)	339712888787
ap-south-2	亚太地区 (海得拉巴)	950823858135
eu-south-2	欧洲 (西班牙)	919611009337
eu-central-2	欧洲 (苏黎世)	529164026651
ap-southeast-4	亚太地区 (墨尔本)	251357961535
il-central-1	以色列 (特拉维夫)	870907303882

- b. 下载相应的公钥、amd64 的签名、arm64 的签名，以及指向 Amazon S3 存储桶中托管的 Debian 脚本的相应访问链接

在以下命令中，将账户 ID 替换为相应的 AWS 账户 ID，将地区替换为您当前的区域。

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.deb ./amazon-guardduty-
agent-1.3.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.sig ./amazon-guardduty-
agent-1.3.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

- c. 将公钥导入数据库

```
gpg --import publickey.pem
```

gpg 显示导入成功

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. 验证签名

```
gpg --verify amazon-guardduty-agent-1.3.0.amd64.sig amazon-guardduty-
agent-1.3.0.amd64.deb
```

成功验证后，您将看到一条类似于以下结果的消息：

输出示例：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

现在，您可以继续使用 Debian 安装 GuardDuty 安全代理。

但是，如果验证失败，则意味着 Debian 软件包中的签名可能已被篡改。

例如：

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

使用以下命令从数据库中删除公钥：

```
gpg --delete-keys AwsGuardDuty
```

现在，重试验证过程。

2. [SSH从 Linux 或 macOS 上连接](#)。
3. 使用以下命令安装 GuardDuty 安全代理：

```
sudo dpkg -i amazon-guardduty-agent-1.3.0.amd64.deb
```

4. 验证 GuardDuty 代理安装是否正常。有关这些步骤的更多信息，请参阅[正在验证 GuardDuty 安全代理安装状态](#)。

内存不足错误

如果您在EC2手动安装或更新 Amazon GuardDuty 安全代理时out-of-memory遇到错误，请参阅[排除内存不足错误](#)。

正在验证 GuardDuty 安全代理安装状态

验证 GuardDuty 安全代理是否正常

1. [SSH从 Linux 或 macOS 上连接](#)。
2. 运行以下命令以检查 GuardDuty 安全代理的状态：

```
sudo systemctl status amazon-guardduty-agent
```

如果要查看安全代理安装日志，可以在下方查看这些日志/var/log/amzn-guardduty-agent/。

要查看日志，请执行此操作sudo journalctl -u amazon-guardduty-agent。

手动更新 GuardDuty 安全客户端

您可以使用 R un 命令更新 GuardDuty 安全客户端。您可以按照与安装 GuardDuty 安全客户端相同的步骤进行操作。

手动卸载安全代理

本节提供从您的 Amazon EC2 资源中卸载 GuardDuty 安全代理的方法。如果您进一步计划禁用运行时监控，请参阅[禁用的影响](#)。

方法 1-使用“运行”命令

使用“运行”命令卸载 GuardDuty 安全代理

1. 您可以按照AWS Systems Manager 用户指南的 [AWS Systems Manager Run Command](#) 中指定的步骤卸载 GuardDuty 安全代理。使用参数中的“卸载”操作卸载 GuardDuty 安全客户端。

在“目标”部分中，确保仅影响您要从中卸载安全代理的 Amazon EC2 实例。

使用以下 GuardDuty 文档和发行商：

- 文件名：AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
 - 分销商：AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. 提供所有详细信息后，当您选择“运行”时，它在目标 Amazon EC2 实例上部署的安全代理将被删除。

要移除亚马逊VPC终端节点配置，您必须同时禁用运行时监控和亚马逊EKS运行时监控。

方法 2-使用 Linux Package Managers

1. [SSH从 Linux 或 macOS 上连接](#)。
2. 卸载命令

以下命令将从您连接的 Amazon EC2 实例中卸载 GuardDuty 安全代理：

- 对于RPM：

```
sudo rpm -e amazon-guardduty-agent
```

- 对于 Debian 来说：

```
sudo dpkg --purge amazon-guardduty-agent
```

运行命令后，您还可以查看与该命令相关的日志。

删除亚马逊终VPC端节点

当您想要禁用运行时监控或卸载账户 GuardDuty 的安全代理时，也可以选择删除手动创建的 Amazon VPC 终端节点（[手动创建亚马逊VPC终端节点](#)）。

使用控制台删除 Amazon VPC 终端节点

1. 打开 Amazon VPC 控制台，网址为 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择端点。
3. 选择在启用运行时监控时手动创建的端点。
4. 选择操作，删除VPC端点。
5. 当系统提示进行确认时，输入 **delete**。
6. 选择删除。

要删除 Amazon VPC 终端节点，请使用以下方法 AWS CLI

- [delete-vpc-endpoints](#) (AWS Command Line Interface)
- [Remove-EC2VpcEndpointCmdlet](#) (适用于 Windows 的工具) PowerShell

管理 Fargate 的自动安全代理 (仅限亚马逊 ECS)

运行时监控仅支持通过管理您的 Amazon ECS 集群 (AWS Fargate) 的安全代理 GuardDuty。不支持在 Amazon ECS 集群上手动管理安全代理。

GuardDuty要启用管理您的 ECS-Fargate 资源的安全代理，请按照以下各节中提供的步骤进行操作。

内容

- [为独立账户配置 GuardDuty 代理](#)
- [为多账户环境配置 GuardDuty 代理](#)

为独立账户配置 GuardDuty 代理

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“运行时监控”。
3. 在“配置”选项卡下：

a. 管理所有 Amazon ECS 集群的自动代理配置 (账户级别)

在“自动代理配置”部分中选择“启用”AWS Fargate (ECS仅限)。当新的 Fargate Amazon ECS 任务启动时，GuardDuty 将管理安全代理的部署。

- 选择保存。

b. 通过排除某些 Amazon ECS 集群来管理自动代理配置 (集群级别)

- 向要排除其所有任务的 Amazon ECS 集群添加标签。键值对必须是 GuardDutyManaged-。false
- 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
```

```

    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

- iii. 在“配置”选项卡下，在“自动代理配置”部分中选择“启用”。

 Note

在为您的账户启用 GuardDuty 代理自动管理之前，请务必将排除标签添加到您的 Amazon ECS 集群；否则，将在相应的 Amazon ECS 集群内启动的所有任务中部署安全代理。

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

- iv. 选择保存。
- c. 通过包含一些 Amazon ECS 集群来管理自动代理配置（集群级别）
 - i. 向要包含其所有任务的 Amazon ECS 集群添加标签。键值对必须是 GuardDutyManaged-。true
 - ii. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
```

```

        "ecs:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {

```

```
    "aws:PrincipalTag/GuardDutyManaged": true
  }
}
]
```

4. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- 命令参考中的 [update-service](#)。AWS CLI

为多账户环境配置 GuardDuty 代理

在多账户环境中，只有委派的 GuardDuty 管理员账户才能启用或禁用成员账户的自动代理配置，以及管理属于其组织中成员账户的 Amazon ECS 集群的自动代理配置。GuardDuty 成员账户无法修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。有关多账户环境的更多信息，请参阅 [中的管理多个账户。GuardDuty](#)

为委派的 GuardDuty 管理员账户启用自动代理配置

Manage for all Amazon ECS clusters (account level)

如果您选择“为所有帐户启用运行时监控”，则有以下选项：

- 在“自动代理配置”部分为所有账户选择“启用”。GuardDuty 将为所有已启动的 Amazon ECS 任务部署和管理安全代理。
- 选择手动配置账户。

如果您在“运行时监控”部分选择了“手动配置帐户”，请执行以下操作：

1. 在“自动代理配置”部分中选择“手动配置帐户”。
2. 在“委派 GuardDuty 管理员账户（此账户）”部分选择“启用”。

选择保存。

如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务](#)。
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- 命令参考中的 [update-service](#)。AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 向此 Amazon ECS 集群添加一个标签，键值对为 `GuardDutyManaged-。false`
2. 禁止修改标签，但可信实体除外。《AWS Organizations 用户指南》中 [除授权原则外，禁止修改标签](#) 中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```


```
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}
```

```

    }
  }
]
}

```

3. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。
- 5.

 Note

在为您的账户启用自动代理配置之前，请务必将排除标签添加到您的亚马逊ECS集群；否则，s GuardDuty idecar 容器将附加到已启动的 Amazon ECS 任务中的所有容器上。

在“配置”选项卡下，在“自动代理配置”中选择“启用”。

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

6. 选择保存。
7. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务](#)。
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- 命令参考中的 [update-service](#)。AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 向要包含其所有任务的 Amazon ECS 集群添加标签。键值对必须是 GuardDutyManaged-。 true
2. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    }
  ]
}

```

```
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}
```

Note

在 Amazon ECS 集群中使用包含标签时，您无需通过自动 GuardDuty 代理配置明确启用代理。

3. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- 命令参考中的 [update-service](#)。AWS CLI

为所有成员账户自动启用

Manage for all Amazon ECS clusters (account level)

以下步骤假设您在“运行时监控”部分为所有帐户选择了“启用”。

1. 在“自动代理配置”部分为所有账户选择“启用”。GuardDuty 将为所有已启动的 Amazon ECS 任务部署和管理安全代理。
2. 选择保存。
3. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- 命令参考中的 [update-service](#)。AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 向此 Amazon ECS 集群添加一个标签，键值对为 `GuardDutyManaged-: false`
2. 禁止修改标签，但可信实体除外。《AWS Organizations 用户指南》中 [除授权原则外，禁止修改标签](#) 中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```


```

        "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ]
},

```

```
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    ]
}
```

3. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。
- 5.

 Note

在为您的账户启用自动代理配置之前，请务必将排除标签添加到您的亚马逊ECS集群；否则，s GuardDuty idecar 容器将附加到已启动的 Amazon ECS 任务中的所有容器上。

在配置选项卡下，选择编辑。

6. 在“自动代理配置”部分为所有账户选择“启用”

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

7. 选择保存。
8. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

无论您选择如何启用运行时监控，以下步骤都将帮助您监控组织中所有成员账户的精选 Amazon ECS Fargate 任务。

1. 请勿在“自动代理配置”部分启用任何配置。保持运行时监控配置与您在上一步中选择的配置相同。
2. 选择保存。
3. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

Note

在 Amazon ECS 集群中使用包含标签时，您无需明确启用GuardDuty 代理自动管理。

4. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

为现有活跃成员账户启用自动代理配置

Manage for all Amazon ECS clusters (account level)

1. 在“运行时监控”页面的“配置”选项卡下，您可以查看自动代理配置的当前状态。
2. 在自动代理配置窗格中，在“活跃成员帐户”部分下，选择操作。
3. 在操作中，选择为所有现有活跃成员账户启用。
4. 选择确认。
5. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 向此 Amazon ECS 集群添加一个标签，键值对为 GuardDutyManaged-。false

2. 禁止修改标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

3. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。
- 5.

 Note

在为您的账户启用自动代理配置之前，请务必将排除标签添加到您的亚马逊ECS集群；否则，s GuardDuty idecar 容器将附加到已启动的 Amazon ECS 任务中的所有容器上。

在“配置”选项卡下的“自动代理配置”部分的“活跃成员帐户”下，选择“操作”。

6. 在操作中，选择为所有活跃成员账户启用。

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

7. 选择确认。
8. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 向要包含其所有任务的 Amazon ECS 集群添加标签。键值对必须是 `GuardDutyManaged-: true`
2. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```

```

        "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ]
},

```

```
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    ]
}
```

Note

在 Amazon ECS 集群中使用包含标签时，您无需明确启用自动代理配置。

3. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

自动启用新成员的自动代理配置

Manage for all Amazon ECS clusters (account level)

1. 在“运行时监控”页面上，选择“编辑”以更新现有配置。
2. 在“自动代理配置”部分，选择“为新成员账户自动启用”。
3. 选择保存。
4. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 向此 Amazon ECS 集群添加一个标签，键值对为 GuardDutyManaged-。false
2. 禁止修改标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
```

```

        "ecs:DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs:DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

3. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

4. 在导航窗格中，选择“运行时监控”。

5.

Note

在为您的账户启用自动代理配置之前，请务必将排除标签添加到您的亚马逊ECS集群；否则，s GuardDuty idecar 容器将附加到已启动的 Amazon ECS 任务中的所有容器上。

在“配置”选项卡下，在“自动代理配置”部分中，选择“自动为新成员帐户启用”。

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

6. 选择保存。

7. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 向要包含其所有任务的 Amazon ECS 集群添加标签。键值对必须是 GuardDutyManaged-。 true
2. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "ecs:ResourceTag/GuardDutyManaged": false
        }
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [

```

```

        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

Note

在 Amazon ECS 集群中使用包含标签时，您无需明确启用自动代理配置。

3. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- [命令参考中的更新服务](#)。AWS CLI

有选择地为活跃成员账户启用自动代理配置

Manage for all Amazon ECS (account level)

1. 在“帐户”页面上，选择要为其启用运行时监控-自动代理配置 (ECS-Fargate) 的帐户。您可以选择多个帐户。确保您在此步骤中选择的帐户已启用运行时监控。
2. 从编辑保护计划中，选择相应的选项以启用运行时监控-自动代理配置 (ECS-F argate)。

3. 选择确认。
4. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定ECS服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务forceNewDeployment。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务。](#) AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. 向此 Amazon ECS 集群添加一个标签，键值对为 GuardDutyManaged-。 false
2. 禁止修改标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```


```
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}
```

```

    }
  }
]
}

```

3. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。
- 5.

 Note

在为您的账户启用 GuardDuty 代理自动管理之前，请务必将排除标签添加到您的 Amazon ECS 集群；否则，GuardDuty 代理容器将附加到已启动的 Amazon ECS 任务中的所有容器上。

在“帐户”页面上，选择要为其启用运行时监控-自动代理配置 (ECS-Fargate) 的帐户。您可以选择多个帐户。确保您在此步骤中选择的帐户已启用运行时监控。

对于尚未排除的 Amazon ECS 集群，GuardDuty 将管理安全代理在 sidecar 容器中的部署。

6. 从编辑保护计划中，选择相应的选项以启用运行时监控-自动代理配置 (ECS-F argate)。
7. 选择保存。
8. 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器 ECS 服务开发者指南中的控制台更新亚马逊服务](#)。
- [UpdateService](#) 在《亚马逊弹性容器服务 API 参考》中。
- [命令参考中的更新服务](#)。AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. 确保不要为拥有要监控的 Amazon ECS 集群的选定账户启用自动代理配置（或运行时监控 ECS-自动代理配置 (-Fargate)）。
2. 向要包含其所有任务的 Amazon ECS 集群添加标签。键值对必须是 `GuardDutyManaged: true`

3. 禁止修改这些标签，但可信实体除外。《AWS Organizations 用户指南》中[除授权原则外，禁止修改标签](#)中提供的政策已修改为适用于此处。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

Note

在 Amazon ECS 集群中使用包含标签时，您无需明确启用自动代理配置。

- 如果 GuardDuty 要监控属于服务一部分的任务，则需要在启用运行时监控后部署新的服务。如果特定 ECS 服务的上次部署是在启用运行时监控之前启动的，则可以重新启动该服务，也可以使用更新服务 `forceNewDeployment`。

有关更新服务的步骤，请参阅以下资源：

- [使用亚马逊弹性容器ECS服务开发者指南中的控制台更新亚马逊服务。](#)
- [UpdateService](#)在《亚马逊弹性容器服务API参考》中。
- [命令参考中的更新服务。](#) AWS CLI

自动管理 Amazon EKS 集群的安全代理

为独立账户配置自动代理

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“运行时监控”。
3. 在“配置”选项卡下，选择“启用”，为您的账户启用自动代理配置。

部署 GuardDuty 安全代理的首选方法	步骤
通过以下方式管理安全代理 GuardDuty (监控所有EKS集群)	<ol style="list-style-type: none"> 1. 在“自动代理配置”部分中选择“启用”。 GuardDuty 将管理您账户中所有现有集群和潜在新EKS集群的安全代理的部署和更新。 2. 选择保存。
监控所有EKS集群，但排除其中一些集群 (使用排除标签)	从以下过程中，选择一种适合您的场景。 在未在该EKS群集上部署 GuardDuty 安全代理时将该群集排除在监控范围之外 <ol style="list-style-type: none"> 1. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed ，其值为false。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。 2. 要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：

部署 GuardDuty 安全代理的首选方法

步骤

- Replace (替换) `ec2:CreateTags` 和 `eks:TagResource` 。
- Replace (替换) `ec2>DeleteTags` 和 `eks:UntagResource` 。
- Replace (替换) `access-project` 与 `GuardDutyManaged`
- Replace (替换) `123456789012` 使用可信实体的 AWS 账户 ID。

如果您有多个可信实体，请使用以下示例添加多个 `PrincipalArn`：

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

3. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。

Note

在为您的账户启用 GuardDuty 代理自动管理之前，请务必向 EKS 集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有 EKS 集群上。

5. 在配置选项卡下，在 GuardDuty 代理管理部分中选择启用。

部署 GuardDuty 安全代理的首选方法	步骤
	<p>对于未被排除在监控范围之外的EKS集群，GuardDuty 将管理 GuardDuty 安全代理的部署和更新。</p> <p>6. 选择保存。</p> <p>在已在该EKS群集上部署 GuardDuty 安全代理后，将该群集排除在监控范围之外</p> <ol style="list-style-type: none">1. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed ，其值为false。 <p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。</p> <p>完成此步骤后，GuardDuty 将不会更新此群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时事件。这可能会影响您的使用情况统计数据。</p> <ol style="list-style-type: none">2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none">• Replace（替换）<i>ec2:CreateTags</i> 和<i>eks:TagResource</i> 。• Replace（替换）<i>ec2>DeleteTags</i> 和<i>eks:UntagResource</i> 。• Replace（替换）<i>access-project</i> 与 GuardDutyManaged• Replace（替换）<i>123456789012</i> 使用可信实体的 AWS 账户 ID。

部署 GuardDuty 安全代理的首选方法	步骤
	<p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre data-bbox="792 380 1507 655">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="691 674 1487 852">3. 要停止接收来自该集群的运行时事件，必须从该集 EKS 群中移除已部署的安全代理。有关删除已部署的安全代理的更多信息，请参阅 禁用和清理资源的影响。

部署 GuardDuty 安全代理的首选方法	步骤
使用包含标签监控选择性EKS集群	<ol style="list-style-type: none"> 1. 确保在“自动代理配置”部分中选择“禁用”。保持运行时监控处于启用状态。 2. 选择保存 3. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed，其值为true。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。 <p>GuardDuty 将为您要监控的选定EKS群集管理安全代理的部署和更新。</p> <ol style="list-style-type: none"> 4. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none"> • Replace（替换）<i>ec2:CreateTags</i> 和 <i>eks:TagResource</i>。 • Replace（替换）<i>ec2>DeleteTags</i> 和 <i>eks:UntagResource</i>。 • Replace（替换）<i>access-project</i> 与 <i>GuardDutyManaged</i> • Replace（替换）<i>123456789012</i> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:</pre>

部署 GuardDuty 安全代理的首选方法	步骤
	<pre>iam::123456789012:role/org-admins/iam-admin"]</pre>
手动管理代理	<ol style="list-style-type: none"> 1. 确保在“自动代理配置”部分中选择“禁用”。保持运行时监控处于启用状态。 2. 选择保存。 3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

为多账户环境配置自动代理

在多账户环境中，只有委派的 GuardDuty 管理员账户才能启用或禁用成员账户的自动代理配置，以及管理属于其组织中成员账户的 EKS 集群的自动代理。GuardDuty 成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。有关多账户环境的更多信息，请参阅 [管理多个账户](#)。

为委派的 GuardDuty 管理员账户配置自动代理配置

管理 GuardDuty 安全代理的首选方法	步骤
通过以下方式管理安全代理 GuardDuty (监控所有 EKS 集群)	<p>如果您在“运行时监控”部分为所有帐户选择“启用”，则有以下选项：</p> <ul style="list-style-type: none"> • 在“自动代理配置”部分为所有账户选择“启用”。GuardDuty 将为属于委派 GuardDuty 管理员账户的所有 EKS 集群以及属于组织中所有现有和可能的新成员账户的所有 EKS 集群部署和管理安全代理。 • 选择手动配置账户。 <p>如果您在“运行时监控”部分选择了“手动配置帐户”，请执行以下操作：</p> <ol style="list-style-type: none"> 1. 在“自动代理配置”部分中选择“手动配置帐户”。 2. 在“委派 GuardDuty 管理员账户（此账户）”部分选择“启用”。

管理 GuardDuty安全代理
的首选方法

步骤

选择保存。

管理 GuardDuty安全代理的首选方法	步骤
监控所有EKS集群，但排除其中一些集群（使用排除标签）	<p>从以下过程中，选择一种适合您的场景。</p> <p>在未在该EKS群集上部署 GuardDuty安全代理时将该群集排除在监控范围之外</p> <ol style="list-style-type: none">1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。• Replace（替换）<code>ec2>DeleteTags</code> 和<code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 GuardDuty Managed• Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>3. 打开 GuardDuty 控制台，网址为https://console.aws.amazon.com/guardduty/。4. 在导航窗格中，选择“运行时监控”。

管理 GuardDuty安全代理的首选方法

步骤

Note

在为您的账户启用 GuardDuty 代理自动管理之前，请务必向EKS集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。

5. 在配置选项卡下，在GuardDuty 代理管理部分中选择启用。

对于未被排除在监控范围之外的EKS集群，GuardDuty 将管理 GuardDuty 安全代理的部署和更新。

6. 选择保存。

在EKS集群上部署 GuardDuty安全代理后，将该集群排除在监控范围之外

1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。

有关为 Amazon EKS 集群添加标签的更多信息，请参阅 [《亚马逊 EKS用户指南》中的使用控制台处理标签](#)。

2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中[防止标签被修改，除非由授权主体修改](#)中的策略。在该策略中，替换以下详细信息：

- Replace（替换）`ec2:CreateTags` 和`eks:TagResource`。
- Replace（替换）`ec2:DeleteTags` 和`eks:UntagResource`。
- Replace（替换）`access-project` 与 GuardDuty Managed
- Replace（替换）`123456789012` 使用可信实体的 AWS 账户 ID。

管理 GuardDuty安全代理的首选方法	步骤
	<p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p> <pre data-bbox="618 380 1507 575">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. 如果您为此EKS群集启用了自动代理，则在此步骤之后，GuardDuty 将不会更新该群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时代事件。这可能会影响您的使用情况统计数据。</p> <p>要停止接收来自该集群的运行时代事件，必须从该集EKS群中移除已部署的安全代理。有关删除已部署的安全代理的更多信息，请参阅 禁用和清理资源的影响</p> <p>4. 如果您是手动管理此EKS集群 GuardDuty 的安全代理，请参阅 禁用和清理资源的影响。</p>

管理 GuardDuty安全代理的首选方法	步骤
使用包含标签监控选择性 EKS 集群	<p>无论您选择如何启用运行时监控，以下步骤都将帮助您监控账户中的部分 EKS 集群：</p> <ol style="list-style-type: none">1. 确保在“自动代理配置”部分为委派 GuardDuty 管理员帐户（此帐户）选择“禁用”。保持运行时监控配置与上一步中的配置相同。2. 选择保存。3. 向 EKS 集群添加一个标签，其密钥为 <code>GuardDutyManaged</code>，其值为 <code>true</code>。 <p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊 EKS 用户指南》中的使用控制台处理标签。</p> <p>GuardDuty 将为您要监控的选定 EKS 群集管理安全代理的部署和更新。</p> <ol style="list-style-type: none">4. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中 防止标签被修改，除非由授权主体修改 中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。• Replace（替换）<code>ec2:DeleteTags</code> 和 <code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 GuardDuty Managed• Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 帐户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

管理 GuardDuty安全代理的首选方法	步骤
手动管理 GuardDuty 安全代理	<p>无论您选择如何启用运行时监控，都可以手动管理EKS集群的安全代理。</p> <ol style="list-style-type: none"> 1. 确保在“自动代理配置”部分为委派 GuardDuty 管理员帐户（此帐户）选择“禁用”。保持运行时监控配置与上一步中的配置相同。 2. 选择保存。 3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

自动启用所有成员账户的自动代理

Note

更新成员账户的配置可能最长需要 24 小时。

管理 GuardDuty安全代理的首选方法	步骤
<p>通过以下方式管理安全代理 GuardDuty</p> <p>（监控所有EKS集群）</p>	<p>本主题旨在为所有成员账户启用运行时监控，因此，以下步骤假设您必须在“运行时监控”部分为所有账户选择“启用”。</p> <ol style="list-style-type: none"> 1. 在“自动代理配置”部分为所有账户选择“启用”。GuardDuty 将为属于委派 GuardDuty 管理员账户的所有EKS集群以及属于组织中所有现有和可能的新成员账户的所有EKS集群部署和管理安全代理。 2. 选择保存。
<p>监控所有EKS集群，但排除其中一些集群（使用排除标签）</p>	<p>从以下过程中，选择一种适合您的场景。</p>

管理 GuardDuty安全代理的首选方法	步骤
	<p>在未在该EKS群集上部署 GuardDuty安全代理时将该群集排除在监控范围之外</p> <ol style="list-style-type: none">1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊 EKS用户指南》中的使用控制台处理标签。2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。• Replace（替换）<code>ec2>DeleteTags</code> 和<code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 GuardDuty Managed• Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。<p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>3. 打开 GuardDuty 控制台，网址为https://console.aws.amazon.com/guardduty/。4. 在导航窗格中，选择“运行时监控”。

管理 GuardDuty安全代理的首选方法

步骤

Note

在为您的账户启用自动代理之前，请务必向EKS集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。

5. 在“配置”选项卡下，在“运行时监视配置”部分中选择“编辑”。
6. 在“自动代理配置”部分为所有账户选择“启用”。对于未被排除在监控范围之外的EKS集群，GuardDuty 将管理 GuardDuty 安全代理的部署和更新。
7. 选择保存。

在EKS集群上部署 GuardDuty安全代理后，将该集群排除在监控范围之外

1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。

有关为 Amazon EKS 集群添加标签的更多信息，请参阅 [《亚马逊 EKS用户指南》中的使用控制台处理标签](#)。

2. 如果您为此EKS群集启用了自动代理配置，则在此步骤之后，GuardDuty 将不会更新该群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时事件。这可能会影响您的使用情况统计数据。

要停止接收来自该集群的运行时事件，必须从该集EKS群中移除已部署的安全代理。有关删除已部署的安全代理的更多信息，请参阅 [禁用和清理资源的影响](#)

3. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中[防止标签被修改，除非由授权主体修改](#)中的策略。在该策略中，替换以下详细信息：

管理 GuardDuty安全代理的首选方法	步骤
	<ul style="list-style-type: none">• Replace (替换) <i>ec2:CreateTags</i> 和 <i>eks:TagResource</i> 。• Replace (替换) <i>ec2>DeleteTags</i> 和 <i>eks:UntagResource</i> 。• Replace (替换) <i>access-project</i> 与 GuardDuty Managed• Replace (替换) <i>123456789012</i> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>4. 如果您是手动管理此EKS集群 GuardDuty 的安全代理，请参阅禁用和清理资源的影响。</p>

管理 GuardDuty安全代理的首选方法

步骤

使用包含标签监控选择性 EKS 集群

无论您选择如何启用 Runtime Monitoring，以下步骤都将帮助您监控组织中所有成员账户的精选 EKS 集群：

1. 请勿在“自动代理配置”部分启用任何配置。保持运行时监控配置与上一步中的配置相同。
2. 选择保存。
3. 向 EKS 集群添加一个标签，其密钥为 `GuardDutyManaged`，其值为 `true`。

有关为 Amazon EKS 集群添加标签的更多信息，请参阅 [《亚马逊 EKS 用户指南》中的使用控制台处理标签](#)。

GuardDuty 将为您要监控的选定 EKS 群集管理安全代理的部署和更新。

4. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中[防止标签被修改，除非由授权主体修改](#)中的策略。在该策略中，替换以下详细信息：

- Replace（替换）`ec2:CreateTags` 和 `eks:TagResource`。
- Replace（替换）`ec2:DeleteTags` 和 `eks:UntagResource`。
- Replace（替换）`access-project` 与 GuardDuty Managed
- Replace（替换）`123456789012` 使用可信实体的 AWS 账户 ID。

如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

管理 GuardDuty安全代理的首选方法	步骤
手动管理 GuardDuty 安全代理	<p>无论您选择如何启用运行时监控，都可以手动管理EKS集群的安全代理。</p> <ol style="list-style-type: none"> 1. 请勿在“自动代理配置”部分启用任何配置。保持运行时监控配置与上一步中的配置相同。 2. 选择保存。 3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

为所有现有活跃成员账户启用自动代理

Note

更新成员账户的配置可能最长需要 24 小时。

管理组织中现有活跃成员账户 GuardDuty 的安全代理

- GuardDuty 要从属于组织中现有活跃成员账户的EKS集群接收运行时事件，必须选择首选方法来管理这些EKS集群 GuardDuty 的安全代理。有关每种方法的更多信息，请参阅 [管理 GuardDuty安全代理的方法](#)。

管理 GuardDuty 安全代理的首选方法	步骤
<p>通过以下方式管理安全代理 GuardDuty</p> <p>(监控所有EKS集群)</p>	<p>监控所有EKS集群中所有现有活跃成员账户</p> <ol style="list-style-type: none"> 1. 在“运行时监控”页面的“配置”选项卡下，您可以查看自动代理配置的当前状态。 2. 在自动代理配置窗格中，在“活跃成员帐户”部分下，选择操作。 3. 在操作中，选择为所有现有活跃成员账户启用。 4. 选择确认。

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控所有EKS集群，但排除其中一些集群（使用排除标签）</p>	<p>从以下过程中，选择一种适合您的场景。</p> <p>在未在该EKS群集上部署 GuardDuty 安全代理时将该群集排除在监控范围之外</p> <ol style="list-style-type: none"> 1. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed ，其值为false。 <p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。</p> 2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none"> • Replace（替换） <i>ec2:CreateTags</i> 和eks:TagResource 。 • Replace（替换） <i>ec2>DeleteTags</i> 和eks:UntagResource 。 • Replace（替换） <i>access-project</i> 与 GuardDutyManaged • Replace（替换） <i>123456789012</i> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

管理 GuardDuty 安全代理的首选方法

步骤

3. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
4. 在导航窗格中，选择“运行时监控”。

Note

在为您的账户启用自动代理配置之前，请务必向EKS集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。

5. 在“配置”选项卡下，在“自动代理配置”窗格的“活跃成员帐户”下，选择“操作”。
6. 在操作中，选择为所有活跃成员账户启用。
7. 选择确认。

在已在该EKS群集上部署 GuardDuty 安全代理后，将该群集排除在监控范围之外

1. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed，其值为false。

有关为 Amazon EKS 集群添加标签的更多信息，请参阅 [《亚马逊EKS用户指南》中的使用控制台处理标签](#)。

完成此步骤后，GuardDuty 将不会更新此群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时效事件。这可能会影响您的使用情况统计数据。

2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中[防止标签被修改，除非由授权主体修改](#)中的策略。在该策略中，替换以下详细信息：

管理 GuardDuty 安全代理的首选方法	步骤
	<ul style="list-style-type: none">• Replace (替换) <i>ec2:CreateTags</i> 和 <i>eks:TagResource</i> 。• Replace (替换) <i>ec2>DeleteTags</i> 和 <i>eks:UntagResource</i> 。• Replace (替换) <i>access-project</i> 与 <i>GuardDutyManaged</i>• Replace (替换) <i>123456789012</i> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. 无论您如何管理安全代理（通过 GuardDuty 还是手动），要停止接收来自该集群的运行时代事件，都必须从该集群中移除已部署的安全代理。EKS有关删除已部署的安全代理的更多信息，请参阅 禁用和清理资源的影响。</p>

管理 GuardDuty 安全代理的首选方法

步骤

使用包含标签监控选择性EKS集群

1. 在“帐户”页面上，启用运行时监控后，不要启用“运行时监控-自动代理配置”。
2. 向属于您要监控的选定账户的EKS集群添加标签。标签的键值对必须是 GuardDutyManaged -true。

有关为 Amazon EKS 集群添加标签的更多信息，请参阅 [《亚马逊EKS用户指南》中的使用控制台处理标签](#)。

GuardDuty 将为您要监控的选定EKS群集管理安全代理的部署和更新。

3. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中[防止标签被修改，除非由授权主体修改](#)中的策略。在该策略中，替换以下详细信息：

- Replace（替换）*ec2:CreateTags* 和 *eks:TagResource*。
- Replace（替换）*ec2>DeleteTags* 和 *eks:UntagResource*。
- Replace（替换）*access-project* 与 GuardDutyManaged
- Replace（替换）*123456789012* 使用可信实体的 AWS 账户 ID。

如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：

```
"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]
```

管理 GuardDuty 安全代理的首选方法	步骤
手动管理 GuardDuty 安全代理	<ol style="list-style-type: none"> 1. 确保没有在“自动代理配置”部分中选择“启用”。保持运行时监控处于启用状态。 2. 选择保存。 3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

为新成员自动启用代理配置

管理 GuardDuty安全代理的首选方法	步骤
通过以下方式管理安全代理 GuardDuty (监控所有EKS集群)	<ol style="list-style-type: none"> 1. 在“运行时监控”页面上，选择“编辑”以更新现有配置。 2. 在“自动代理配置”部分，选择“为新成员账户自动启用”。 3. 选择保存。
监控所有EKS集群，但排除其中一些集群（使用排除标签）	<p>从以下过程中，选择一种适合您的场景。</p> <p>在未在该EKS群集上部署 GuardDuty安全代理时将该群集排除在监控范围之外</p> <ol style="list-style-type: none"> 1. 向该EKS集群添加一个标签，其密钥为GuardDuty Managed ，其值为false。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。 2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none"> • Replace（替换） <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code> 。

管理 GuardDuty安全代理的首选方法	步骤
	<ul style="list-style-type: none">• Replace (替换) <code>ec2:DeleteTags</code> 和 <code>eks:UntagResource</code> 。• Replace (替换) <code>access-project</code> 与 <code>GuardDutyManaged</code>• Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none">3. 打开 GuardDuty 控制台，网址为 https://console.aws.amazon.com/guardduty/。4. 在导航窗格中，选择“运行时监控”。 <div data-bbox="716 1157 1507 1419"><p>Note</p><p>在为您的账户启用自动代理配置之前，请务必向 EKS 集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有 EKS 集群上。</p></div> <ol style="list-style-type: none">5. 在“配置”选项卡下，在“GuardDuty 代理管理”部分中，选择“自动为新成员帐户启用”。 <p>对于未被排除在监控范围之外的 EKS 集群，GuardDuty 将管理 GuardDuty 安全代理的部署和更新。</p> <ol style="list-style-type: none">6. 选择保存。

管理 GuardDuty安全代理的首选方法	步骤
	<p>在EKS集群上部署 GuardDuty安全代理后，将该集群排除在监控范围之外</p> <ol style="list-style-type: none">1. 无论您是通过 GuardDuty 还是手动管理 GuardDuty 安全代理，都要向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。 如果您为此EKS群集启用了自动代理，则在此步骤之后，GuardDuty 将不会更新该群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时事件。这可能会影响您的使用情况统计数据。 要停止接收来自该集群的运行时事件，必须从该集EKS群中移除已部署的安全代理。有关删除已部署的安全代理的更多信息，请参阅 禁用和清理资源的影响2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。• Replace（替换）<code>ec2>DeleteTags</code> 和<code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 <code>GuardDutyManaged</code>• Replace（替换）<code>123456789012</code> 使用可信实体的AWS 账户 ID。 如果您有多个可信实体，请使用以下示例添加多个PrincipalArn：

管理 GuardDuty安全代理的首选方法	步骤
	<pre data-bbox="748 256 1507 495">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="651 506 1484 590">3. 如果您是手动管理此EKS集群 GuardDuty 的安全代理，请参阅禁用和清理资源的影响。

管理 GuardDuty安全代理的首选方法	步骤
使用包含标签监控选择性EKS集群	<p>无论您选择如何启用 Runtime Monitoring ，以下步骤都将帮助您监控组织中新成员帐户的选定EKS集群。</p> <ol style="list-style-type: none">1. 确保在“自动代理配置”部分中清除“自动为新成员账户启用”。保持运行时监控配置与上一步中的配置相同。2. 选择保存。3. 向EKS集群添加一个标签，其密钥为GuardDuty Managed ，其值为true。 <p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。</p> <p>GuardDuty 将为您要监控的选定EKS群集管理安全代理的部署和更新。</p> <ol style="list-style-type: none">4. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。• Replace（替换）<code>ec2>DeleteTags</code> 和<code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 <code>GuardDutyManaged</code>• Replace（替换）<code>123456789012</code> 使用可信实体的AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-</pre>

管理 GuardDuty安全代理的首选方法	步骤
	<pre>admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>
手动管理 GuardDuty 安全代理	<p>无论您选择如何启用运行时监控，都可以手动管理EKS集群的安全代理。</p> <ol style="list-style-type: none"> 1. 确保清除“自动代理配置”部分中的“自动为新成员帐户启用”复选框。保持运行时监控配置与上一步中的配置相同。 2. 选择保存。 3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

有选择地为活跃成员账户配置自动代理

管理 GuardDuty安全代理的首选方法	步骤
通过以下方式管理安全代理 GuardDuty (监控所有EKS集群)	<ol style="list-style-type: none"> 1. 在“帐户”页面上，选择要为其启用自动代理配置的帐户。您可以一次选择多个帐户。确保您在此步骤中选择的帐户已启用EKS运行时监控。 2. 从编辑保护计划中选择相应的选项以启用“运行时监控-自动代理配置”。 3. 选择确认。
监控所有EKS集群，但排除其中一些集群（使用排除标签）	<p>从以下过程中，选择一种适合您的场景。</p> <p>在未在该EKS群集上部署 GuardDuty安全代理时将该群集排除在监控范围之外</p> <ol style="list-style-type: none"> 1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。

管理 GuardDuty安全代理的首选方法	步骤
	<p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊 EKS用户指南》中的使用控制台处理标签。</p> <ol style="list-style-type: none">要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。Replace（替换）<code>ec2>DeleteTags</code> 和<code>eks:UntagResource</code>。Replace（替换）<code>access-project</code> 与 GuardDuty ManagedReplace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。<p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>打开 GuardDuty 控制台，网址为https://console.aws.amazon.com/guardduty/。 <div data-bbox="586 1444 1507 1709" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px;"><p>Note</p><p>在为您的账户启用自动代理配置之前，请务必向EKS集群添加排除标签；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。</p></div> <ol style="list-style-type: none">在“账户”页面上，选择要为其启用自动管理代理的账户。您可以一次选择多个账户。

管理 GuardDuty安全代理的首选方法	步骤
	<p>5. 在编辑保护计划中，选择相应的选项，为所选帐户启用运行时监控-自动代理配置。</p> <p>对于未被排除在监控范围之外的EKS集群，GuardDuty 将管理 GuardDuty 安全代理的部署和更新。</p> <p>6. 选择保存。</p> <p>在EKS集群上部署 GuardDuty安全代理后，将该集群排除在监控范围之外</p> <p>1. 向该EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为false。</p> <p>有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊 EKS用户指南》中的使用控制台处理标签。</p> <p>如果您之前已为此EKS群集启用了自动代理配置，则在此步骤之后，GuardDuty 将不会更新该群集的安全代理。但是，安全代理将保持部署状态，GuardDuty 并将继续接收来自该EKS集群的运行时效事件。这可能会影响您的使用情况统计数据。</p> <p>要停止接收来自该集群的运行时效事件，必须从该集EKS群中移除已部署的安全代理。有关删除已部署的安全代理的更多信息，请参阅 禁用和清理资源的影响</p> <p>2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> • Replace（替换）<i>ec2:CreateTags</i> 和eks:TagResource。 • Replace（替换）<i>ec2:DeleteTags</i> 和eks:UntagResource。 • Replace（替换）<i>access-project</i> 与 GuardDuty Managed

管理 GuardDuty安全代理的首选方法	步骤
	<ul style="list-style-type: none">• Replace (替换) 123456789012 使用可信实体的 AWS 账户 ID。 如果您有多个可信实体，请使用以下示例添加多个 Principal Arn ： <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. 如果您是手动管理此EKS集群 GuardDuty 的安全代理，则必须将其删除。有关更多信息，请参阅 禁用和清理资源的影响。</p>

管理 GuardDuty安全代理的首选方法	步骤
使用包含标签监控选择性EKS集群	<p>无论您选择如何启用运行时监控，以下步骤都将帮助您监控属于所选账户的精选EKS集群：</p> <ol style="list-style-type: none">1. 确保不要为拥有要监控的EKS集群的选定账户启用运行时监控-自动代理配置。2. 向EKS集群添加一个标签，其密钥为GuardDutyManaged，其值为true。 有关为 Amazon EKS 集群添加标签的更多信息，请参阅 《亚马逊EKS用户指南》中的使用控制台处理标签。 添加标签后，GuardDuty 将为您要监控的选定EKS集群管理安全代理的部署和更新。3. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">• Replace（替换）<code>ec2:CreateTags</code> 和<code>eks:TagResource</code>。• Replace（替换）<code>ec2:DeleteTags</code> 和<code>eks:UntagResource</code>。• Replace（替换）<code>access-project</code> 与 GuardDuty Managed• Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。<p>如果您有多个可信实体，请使用以下示例添加多个 Principal Arn：</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>

管理 GuardDuty安全代理的首选方法	步骤
手动管理 GuardDuty 安全代理	<ol style="list-style-type: none">1. 保持运行时监控配置与上一步中的配置相同。确保未为任何选定帐户启用“运行时监控-自动代理配置”。2. 选择确认。3. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

手动管理 Amazon EKS 集群的安全代理

本节介绍如何在启用运行时监控后管理您EKS的 Amazon 插件GuardDuty 代理（代理）。要使用运行时监控，您必须启用运行时监控并配置 Amazon EKS 附加组件aws-guardduty-agent。仅执行这两个步骤中的一个步骤无助于 GuardDuty 检测潜在威胁或生成调查结果。

部署 GuardDuty 安全代理的先决条件

本节介绍手动为EKS集群部署 GuardDuty 安全代理的先决条件。在继续操作之前，请确保您已经为帐户配置了运行时监控。如果您不配置运行时监控，则 GuardDuty 安全代理（EKS附加组件）将无法运行。有关更多信息，请参阅 [启用 GuardDuty 运行时监控](#)。完成下列步骤后，请参阅 [部署 GuardDuty 安全代理](#)。

选择您的首选访问方法来创建 Amazon VPC 终端节点。

Console

创建VPC终端节点

1. 打开 Amazon VPC 控制台，网址为<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中的虚拟私有云下，选择端点。
3. 选择 Create Endpoint（创建端点）。
4. 在创建端点页面上，对于服务类别，选择其他端点服务。
5. 对于服务名称，输入 **com.amazonaws.us-east-1.guardduty-data**。

请务必更换 **us-east-1** 使用正确的区域。该区域必须与属于您 AWS 帐户 ID 的EKS集群位于同一区域。

6. 选择验证服务。

- 成功验证服务名称后，选择您的集群所在VPC的位置。添加以下政策，仅限指定账户使用VPC终端节点。使用此策略下面提供的组织 Condition，您可以更新以下策略来限制对端点的访问。要向组织IDs中的特定账户提供VPC终端节点支持，请参阅[Organization condition to restrict access to your endpoint](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

aws:PrincipalAccount 账户 ID 必须与包含VPC和VPC端点的账户相匹配。以下列表显示了如何与其他人共享VPC端节点 AWS 账户 IDs：

限制访问端点的组织条件

- 要指定多个帐户来访问VPC终端节点，请"aws:PrincipalAccount": "**111122223333**" 替换为以下内容：

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

- 要允许组织中的所有成员访问VPC终端节点，请"aws:PrincipalAccount": "**111122223333**"替换为以下内容：

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- 要限制组织 ID 的访问资源，请将您的 ResourceOrgID 添加到策略中。

有关更多信息，请参阅 [ResourceOrgID](#)。

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. 在“其他设置”下，选择“启用DNS名称”。
9. 在子网下，选择集群所在的子网。
10. 在“安全组”下，选择已从您的VPC（或您的EKS集群）启用入站端口 443 的安全组。如果您还没有启用入站端口 443 的安全组，请[创建安全组](#)。

如果在限制您的VPC（或集群）的入站权限时出现问题，请为来自任何 IP 地址的入站 443 端口提供支持（ ）。0.0.0.0/0

API/CLI

- 调用[CreateVpcEndpoint](#)。
- 为参数使用以下值：
 - 对于服务名称，输入 **com.amazonaws.us-east-1.guardduty-data**。

请务必更换 **us-east-1** 使用正确的区域。该区域必须与属于您 AWS 账户 ID 的EKS集群位于同一区域。

- 对于 [DNSOptions](#)，通过将其设置为来启用私密DNS选项true。
- 有关信息 AWS Command Line Interface，请参阅[create-vpc-endpoint](#)。

为 Amazon 配置 GuardDuty 安全代理（附加组件）参数 EKS

您可以为 Amazon 配置 GuardDuty 安全代理的特定参数EKS。此支持适用于 GuardDuty 安全代理版本 1.5.0 及更高版本。有关最新插件版本的信息，请参阅[GuardDuty 适用于 Amazon EKS 集群的安全代理](#)。

我为什么要更新安全代理配置架构

GuardDuty 安全代理的配置架构在您的 Amazon 集EKS群内的所有容器中都是相同的。当默认值与关联的工作负载和实例大小不一致时，可以考虑配置CPU设置PriorityClass、内存设置和dnsPolicy设置。无论您如何管理 Amazon EKS 集群的 GuardDuty 代理，都可以配置或更新这些参数的现有配置。

使用已配置参数自动配置代理的行为

代表您 GuardDuty 管理安全代理（EKS附加组件）时，它会根据需要更新附加组件。GuardDuty 会将可配置参数的值设置为默认值。但是，您仍然可以将参数更新为所需的值。如果这导致冲突，则默认选项[resolveConflicts](#)为None。

可配置的参数和值

有关配置插件参数的步骤的信息，请参阅：

- [部署 GuardDuty 安全代理](#) 或
- [手动更新安全代理](#)

下表提供了可用于手动部署 Amazon EKS 附加组件或更新现有插件设置的范围和值。

CPU设置

参数	默认值	可配置范围
请求	200m	介于 200 米到 10000 米之间，两者兼而有之
限制	1000m	

内存设置

参数	默认值	可配置范围
请求	256Mi	介于 256 英里和 200000 英里之间，两者兼而有之
限制	1024 Mi	

PriorityClass 设置

GuardDuty 为您创建 Amazon EKS 加载项时，分配的 PriorityClass 为 `aws-guardduty-agent.priorityclass`。这意味着不会根据代理窗格的优先级采取任何操作。您可以通过选择以下 PriorityClass 选项之一来配置此插件参数：

可配置 PriorityClass	preemptionPolicy 值	preemptionPolicy 描述	Pod 值
<code>aws-guardduty-agent.priorityclass</code>	Never	无需操作	1000000
<code>aws-guardduty-agent.priorityclass-high</code>	PreemptLowerPriority	分配此值将抢占优先级值低于代理 pod 值的 Pod 运行。	100000000
<code>system-cluster-critical</code> ¹	PreemptLowerPriority		2000000000
<code>system-node-critical</code> ¹	PreemptLowerPriority		2000001000

¹ Kubernetes 提供了这两个 PriorityClass 选项——和 `system-cluster-critical` `system-node-critical` 有关更多信息，请参阅 Kubernetes 文档 [PriorityClass](#) 中的。

dnsPolicy 设置

选择 Kubernetes 支持的以下 DNS 策略选项之一。如果未指定任何配置，ClusterFirst 则用作默认值。

- ClusterFirst
- ClusterFirstWithHostNet
- Default

有关这些策略的信息，请参阅 Kubernetes DNS [文档中的 Pod 策略](#)。

部署 GuardDuty 安全代理

本节介绍如何首次为特定EKS集群部署 GuardDuty 安全代理。在继续本节之前，请确保您已经为账户设置了先决条件并启用了运行时监控。如果您不启用运行时监控，则 GuardDuty安全代理 (EKS附加组件) 将无法运行。

选择您的首选访问方法以首次部署 GuardDuty 安全代理。

Console

1. 在 <https://console.aws.amazon.com/eks/home#/clusters> 中打开 Amazon EKS 控制台。
2. 选择集群名称。
3. 选择附加组件选项卡。
4. 选择获取更多附加组件。
5. 在选择插件页面上，选择 Amazon GuardDuty 运行时监控。
6. 在配置选定插件设置页面上，使用默认设置。如果您的EKS附加组件的状态为需要激活，请选择激活 GuardDuty。此操作将打开 GuardDuty 控制台，为您的账户配置运行时监控。
7. 为账户配置运行时监控后，切换回 Amazon EKS 控制台。您的EKS附加组件的状态应该已更改为“准备安装”。
8. (可选) 提供EKS插件配置架构


对于附加版本，如果您选择 v1.5.0 及更高版本，则运行时监控支持配置代理的 GuardDuty 特定参数。有关参数范围的信息，请参见[配置EKS插件参数](#)。

- a. 展开可选配置设置以查看可配置参数及其预期值和格式。
 - b. 设置参数。这些值必须在中提供的范围内[配置EKS插件参数](#)。
 - c. 选择保存更改以根据高级配置创建插件。
 - d. 对于冲突解决方法，当您将参数的值更新为非默认值时，将使用您选择的选项来解决冲突。有关所列选项的更多信息，请参阅 Amazon EKS API 参考[resolveConflicts](#)中的。
9. 选择下一步。
 10. 在查看和创建页面上，验证所有详细信息，然后选择创建。
 11. 导航回集群详细信息，然后选择资源选项卡。
 12. 您可以查看带有前缀的新窗格aws-guardduty-agent。

API/CLI

您可以使用以下任一选项配置 Amazon EKS 插件代理 (aws-guardduty-agent) :

- [CreateAddon](#)为你的账户跑步。

 Note

对于附加组件version，如果您选择 v1.5.0 及更高版本，则运行时监控支持配置代理的 GuardDuty 特定参数。有关更多信息，请参阅 [配置EKS插件参数](#)。

对请求参数使用以下值：

- 对于 addonName，输入 aws-guardduty-agent。

使用插件版本 1.5.0 及更高版本支持的可配置值时，可以使用以下 AWS CLI 示例。确保替换以红色突出显示的占位符值以及Example.json与配置值关联的占位符值。

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-values 'file://example.json'
```

Example example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- 有关支持的 addonVersion 的信息，请参阅 [安全代理支持的 Kubernetes 版本 GuardDuty](#)。
- 或者，你可以使用 AWS CLI。有关更多信息，请参阅[创建插件](#)。

手动更新安全代理

当你手动管理 GuardDuty 安全代理时，你有责任为你的账户更新安全代理。要获得有关新代理版本的通知，您可以订阅 RSS Feed 到[GuardDuty 代理发布历史记录](#)。

您可以将安全代理更新到最新版本，以受益于新增的支持和改进。如果您当前的代理版本已接近标准支持的终止，则要继续使用运行时监控（或EKS运行时监控），则必须更新当前的代理版本。有关发行版本的信息，请参阅[GuardDuty 适用于 Amazon EKS 集群的安全代理](#)。

先决条件

在更新安全代理版本之前，请确保你现在计划使用的代理版本与你的 Kubernetes 版本兼容。有关更多信息，请参阅 [安全代理支持的 Kubernetes 版本 GuardDuty](#)。

Console

1. 在 <https://console.aws.amazon.com/eks/home#/clusters> 中打开 Amazon EKS 控制台。
2. 选择集群名称。
3. 选择“附加组件”。
4. 在“插件”下，选择“GuardDuty运行时监控”。
5. 选择“编辑”以更新代理详细信息。
6. 在“配置 GuardDuty 运行时监控”页面上，更新详细信息。
7. （可选）更新插件配置参数

如果您的EKS附加组件版本为 1.5.0 或更高版本，您也可以更新插件配置设置。

- a. 展开可选配置设置以查看配置架构。
- b. 根据中提供的范围更新参数值[配置EKS插件参数](#)。
- c. 选择保存更改以开始更新。
- d. 对于冲突解决方法，当您将参数的值更新为非默认值时，将使用您选择的选项来解决冲突。有关所列选项的更多信息，请参阅 Amazon EKS API 参考[resolveConflicts](#)中的。

API/CLI

要更新您的 Amazon EKS 集群 GuardDuty 的安全代理，请参阅[更新插件](#)。

Note

对于附加组件 version，如果您选择 v1.5.0 及更高版本，则运行时监控支持配置代理的 GuardDuty 特定参数。有关参数范围的信息，请参见[配置EKS插件参数](#)。

使用插件版本 1.5.0 及更高版本支持的可配置值时，可以使用以下 AWS CLI 示例。确保替换以红色突出显示的占位符值以及 Example.json 与配置值关联的占位符值。

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-values 'file://example.json'
```

Example example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

如果您的 Amazon EKS 插件版本为 1.5.0 或更高版本，并且您已经配置了插件架构，则可以验证集群的值显示是否正确。有关更多信息，请参阅[验证配置架构更新](#)。

验证配置架构更新

配置完参数后，请执行以下步骤以验证配置架构是否已更新：

1. 在 <https://console.aws.amazon.com/eks/home#/clusters> 中打开 Amazon EKS 控制台。
2. 在导航窗格中，选择集群。

3. 在集群页面上，选择要验证更新的集群名称。
4. 选择资源选项卡。
5. 从“资源类型”窗格的“工作负载”下选择DaemonSets。
6. 选择aws-guardduty-agent。
7. 在该aws-guardduty-agent页面上，选择 Raw view 以查看未格式化的JSON响应。验证可配置参数是否显示您提供的值。

验证后，切换到 GuardDuty 控制台。选择相应的，AWS 区域 然后查看您的 Amazon EKS 集群的覆盖状态。有关更多信息，请参阅 [Amazon EKS 集群的覆盖范围](#)。

配置EKS运行时监控 (API仅限)

在您的账户中配置EKS运行时监控之前，请确保您使用的是支持当前正在使用的 Kubernetes 版本的经过验证的平台。有关更多信息，请参阅[验证架构要求](#)。

GuardDuty 已将EKS运行时监控的控制台体验整合到运行时监控中。GuardDuty 推荐[检查EKS运行时监控配置状态](#)和[从EKS运行时监控迁移到运行时监控](#)。

作为迁移到运行时监控的一部分，请确保[禁用EKS运行时监控](#)。这一点很重要，因为如果您稍后选择禁用“运行时监控”，但未禁用“EKS运行时监控”，则将继续产生EKS运行时监控的使用成本。

为独立账户配置EKS运行时监控

有关与 [AWS Organizations](#) 关联的账户，请参阅 [为多EKS账户环境配置运行时监控](#)。

选择您的首选访问方式，为您的账户启用EKS运行时监控。

API/CLI

根据 [管理 GuardDuty安全代理的方法](#)，您可以选择首选方法，并按照下表中所述的步骤进行操作。

管理 GuardDuty 安全代理的首选方法	步骤
通过管理安全代理 GuardDuty (监控所有EKS集群)	1. 使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。 updateDetectorAPI

管理 GuardDuty 安全代理的首选方法

步骤

将 `EKS_ADDON_MANAGEMENT` 的状态设为 `ENABLED`。

GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。

2. 或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectorsAPI`。 `detectorId`

以下示例同时启用了 `EKS_RUNTIME_MONITORING` 和 `EKS_ADDON_MANAGEMENT`：

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'
```

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控所有EKS集群，但排除其中一些集群（使用排除标签）</p>	<ol style="list-style-type: none"> <p>为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -false</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。</p> <p>要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 Replace（替换）<code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code>。 Replace（替换）<code>access-project</code> 与 <code>GuardDutyManaged</code> Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控选择性EKS聚类 (使用包含标签)</p>	<ol style="list-style-type: none"> <p>为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -true</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户 指南中的使用CLI API、或 eksctl 处理标签。</p> <p>要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中 防止标签被修改，除非由授权主体修改 中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> Replace (替换) <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code> 。 Replace (替换) <code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code> 。 Replace (替换) <code>access-project</code> 与 <code>GuardDutyManaged</code> Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>使用您自己的区域探测器 ID 运行，并将 <code>features</code> 对象名称传递为，将 <code>EKS_RUNTIME_MONITORING</code> 状态传递为 <code>ENABLED</code>。 updateDetectorAPI</p> <p>将 <code>EKS_ADDON_MANAGEMENT</code> 的状态设为 <code>DISABLED</code>。</p>

管理 GuardDuty 安全代理的首选方法

步骤

GuardDuty 将管理所有标有 GuardDuty Managed -true 对的 Amazon EKS 集群的安全代理的部署和更新。

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```


管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<p>1. 使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}]]'</pre> <p>2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。</p>

为多EKS账户环境配置运行时监控

在多账户环境中，只有委派的 GuardDuty 管理员账户才能为成员账户启用或禁用 EKS Runtime Monitoring，并管理属于其组织中成员账户的EKS集群的 GuardDuty 代理管理。GuardDuty 成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。有关多账户环境的更多信息，请参阅[管理多个账户](#)。

为委派的 GuardDuty 管理员账户配置EKS运行时监控

选择您的首选访问方法以启用EKS运行时监控并管理属于委派 GuardDuty 管理员帐户的EKS集群 GuardDuty的安全代理。

API/CLI

根据 [管理 GuardDuty安全代理的方法](#)，您可以选择首选方法，并按照下表中所述的步骤进行操作。

管理 GuardDuty 安全代理的首选方法	步骤
通过管理安全代理 GuardDuty (监控所有EKS集群)	<p>使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ：</p> <pre data-bbox="683 1381 1507 1661">aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>
监控所有EKS集群，但排除其中一些集群（使用排除标签）	<ol style="list-style-type: none"> 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -false。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。

管理 GuardDuty 安全代理的首选方法	步骤
	<p>2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> • Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 • Replace（替换）<code>ec2:DeleteTags</code> 和 <code>eks:UntagResource</code>。 • Replace（替换）<code>access-project</code> 与 <code>GuardDutyManaged</code> • Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3.</p> <div data-bbox="743 1297 1507 1612" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p>Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p> </div> <p>使用您自己的区域探测器 ID 运行，并将 <code>features</code> 对象名称传递为，将 <code>EKS_RUNTIME_MONITORING</code> 状态传递为 <code>ENABLED</code>。updateDetectorAPI</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre>

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控选择性EKS聚类 (使用包含标签)</p>	<ol style="list-style-type: none"> <p>为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -true</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。</p> <p>要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> Replace (替换) <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code> 。 Replace (替换) <code>ec2:DeleteTags</code> 和 <code>eks:UntagResource</code> 。 Replace (替换) <code>access-project</code> 与 <code>GuardDutyManaged</code> Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>使用您自己的区域探测器 ID 运行，并将 <code>features</code> 对象名称传递为，将 <code>EKS_RUNTIME_MONITORING</code> 状态传递为 <code>ENABLED</code>。updateDetectorAPI</p> <p>将 <code>EKS_ADDON_MANAGEMENT</code> 的状态设为 <code>DISABLED</code>。</p>

管理 GuardDuty 安全代理的首选方法

步骤

GuardDuty 将管理所有标有 GuardDuty Managed -true 对的 Amazon EKS 集群的安全代理的部署和更新。

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}]'
```

管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<p>1. 使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <p>2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。</p>


为所有成员账户自动启用EKS运行时监控


选择您的首选访问方式，为所有成员账户启用EKS运行时监控。这包括委派 GuardDuty 管理员账户、现有成员账户和加入组织的新账户。选择您首选的方法来管理属于这些成员账户的EKS集群 GuardDuty 的安全代理。

API/CLI

根据 [管理 GuardDuty安全代理的方法](#)，您可以选择首选方法，并按照下表中所述的步骤进行操作。

<p>管理 GuardDuty 安全代理的首选方法</p>	<p>步骤</p>
<p>通过管理安全代理 GuardDuty (监控所有 EKS 集群)</p>	<p>要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>您也可以传递用空格IDs分隔的账户列表。</p> </div> <p>成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>
<p>监控所有EKS集群，但排除其中一些集群 (使用排除标签)</p>	<ol style="list-style-type: none"> 1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -false。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLIAPI、或 eksctl 处理标签。

管理 GuardDuty 安全代理的首选方法	步骤
	<p>2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> • Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 • Replace（替换）<code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code>。 • Replace（替换）<code>access-project</code> 与 GuardDuty Managed • Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3.</p> <div data-bbox="621 1251 1507 1564" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p> </div> <p>使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行 <code>ListDetectors</code> API。 <code>detectorId</code></p> <p>以下示例同时启用了 <code>EKS_RUNTIME_MONITORING</code> 和 <code>EKS_ADDON_MANAGEMENT</code>：</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div data-bbox="621 1045 1507 1213"><p> Note</p><p>您也可以传递用空格IDs分隔的账户列表。</p></div> <p>成功执行代码后，会返回 <code>UnprocessedAccounts</code> 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>

管理 GuardDuty 安全代理的首选方法	步骤
监控选择性EKS聚类 (使用包含标签)	<ol style="list-style-type: none"><li data-bbox="558 275 1484 453">1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -true。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLIAPI、或 eksctl 处理标签。<li data-bbox="558 474 1484 1050">2. 要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none"><li data-bbox="621 653 1406 730">• Replace (替换) <i>ec2:CreateTags</i> 和eks:TagResource 。<li data-bbox="621 751 1406 829">• Replace (替换) <i>ec2>DeleteTags</i> 和eks:UntagResource 。<li data-bbox="621 850 1406 928">• Replace (替换) <i>access-project</i> 与 GuardDutyManaged<li data-bbox="621 949 1471 1026">• Replace (替换) <i>123456789012</i> 使用可信实体的 AWS 账户 ID。<p data-bbox="654 1089 1354 1167">如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn ：</p><pre data-bbox="672 1236 1406 1423">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre><li data-bbox="558 1467 1427 1598">3. 使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI <p data-bbox="621 1644 1427 1680">将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p data-bbox="621 1726 1500 1803">GuardDuty 将管理所有标有 GuardDutyManaged -true 对的 Amazon EKS 集群的安全代理的部署和更新。</p>

管理 GuardDuty 安全代理的首选方法

步骤

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectors` API。 `detectorId`

以下示例启用了 `EKS_RUNTIME_MONITORING` ，并禁用了 `EKS_ADDON_MANAGEMENT` ：

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的探测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<p>1. 使用您自己的区域探测器 ID 运行，并将features对象名称传递为，将EKS_RUNTIME_MONITORING 状态传递为ENABLED。updateDetectorAPI</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] }]'</pre> <p>2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。</p>


为所有现有活跃成员账户配置EKS运行时监控

选择您的首选访问方法以启用EKS运行时监控并管理组织中现有活跃成员帐户 GuardDuty 的安全代理。

API/CLI

根据 [管理 GuardDuty安全代理的方法](#)，您可以选择首选方法，并按照下表中所述的步骤进行操作。

<p>管理 GuardDuty 安全代理的首选方法</p>	<p>步骤</p>
<p>通过管理安全代理 GuardDuty (监控所有 EKS 集群)</p>	<p>要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>您也可以传递用空格IDs分隔的账户列表。</p> </div> <p>成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>
<p>监控所有EKS集群，但排除其中一些集群 (使用排除标签)</p>	<ol style="list-style-type: none"> 1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -false。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLIAPI、或 eksctl 处理标签。

管理 GuardDuty 安全代理的首选方法	步骤
	<p>2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> • Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 • Replace（替换）<code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code>。 • Replace（替换）<code>access-project</code> 与 GuardDuty Managed • Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3.</p> <div data-bbox="621 1251 1507 1564" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty 安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p> </div> <p>要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <code>detector ID</code>。</p> <p>将 <code>EKS_ADDON_MANAGEMENT</code> 的状态设为 <code>ENABLED</code>。</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行 <code>ListDetectors</code> API。 <code>detectorId</code></p> <p>以下示例同时启用了 <code>EKS_RUNTIME_MONITORING</code> 和 <code>EKS_ADDON_MANAGEMENT</code>：</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}]]'</pre> <div data-bbox="621 1045 1507 1213"><p> Note</p><p>您也可以传递用空格IDs分隔的账户列表。</p></div> <p>成功执行代码后，会返回 <code>UnprocessedAccounts</code> 的空列表。如果更改账户的探测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>

管理 GuardDuty 安全代理的首选方法	步骤
监控选择性EKS聚类 (使用包含标签)	<ol style="list-style-type: none"><li data-bbox="558 275 1484 457">1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -true。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。<ol style="list-style-type: none"><li data-bbox="558 478 1484 604">2. 要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none"><li data-bbox="623 646 1406 730">• Replace (替换) <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code> 。<li data-bbox="623 751 1406 835">• Replace (替换) <code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code> 。<li data-bbox="623 856 1406 940">• Replace (替换) <code>access-project</code> 与 GuardDuty Managed<li data-bbox="623 961 1471 1045">• Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。<p data-bbox="656 1087 1354 1171">如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p><pre data-bbox="672 1234 1406 1423">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre><li data-bbox="558 1472 1484 1598">3. 要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectors API操作 <code>detector ID</code>。<p data-bbox="623 1640 1430 1682">将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p><p data-bbox="623 1724 1500 1808">GuardDuty 将管理所有标有 GuardDutyManaged -true 对的 Amazon EKS 集群的安全代理的部署和更新。</p>

管理 GuardDuty 安全代理的首选方法

步骤

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectors` API。 `detectorId`

以下示例启用了 `EKS_RUNTIME_MONITORING` ，并禁用了 `EKS_ADDON_MANAGEMENT` ：

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的探测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<p>1. 要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] }]'</pre> <p>2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。</p>

为新成员自动启用EKS运行时监控

委派的 GuardDuty 管理员帐户可以自动启用 EKS Runtime Monitoring ，并选择一种方法来管理加入组织的新账户 GuardDuty 的安全代理。

API/CLI

根据 [管理 GuardDuty安全代理的方法](#) ，您可以选择首选方法，并按照下表中所述的步骤进行操作。

管理 GuardDuty 安全代理的首选方法	步骤
<p>通过管理安全代理 GuardDuty (监控所有EKS集群)</p>	<p>要有选择地为新账户启用EKS运行时监控，请使用自己的账户调用该UpdateOrganizationConfigurationAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例为单个账户同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT 。您也可以传递用空格IDs分隔的账户列表。</p> <p>要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <pre data-bbox="683 1249 1507 1566">aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name": "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> <p>成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>
<p>监控所有EKS集群，但排除其中一些集群 (使用排除标签)</p>	<ol style="list-style-type: none"> 1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 GuardDutyManaged -false。有关添加标签

管理 GuardDuty 安全代理的首选方法	步骤
	<p>的更多信息，请参阅亚马逊EKS用户 指南中的使用CLI API、或 eksctl 处理标签。</p> <p>2. 要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none">• Replace（替换）<i>ec2:CreateTags</i> 和 <i>eks:TagResource</i> 。• Replace（替换）<i>ec2>DeleteTags</i> 和 <i>eks:UntagResource</i> 。• Replace（替换）<i>access-project</i> 与 <i>GuardDutyManaged</i>• Replace（替换）<i>123456789012</i> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 PrincipalArn：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3.  Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>要有选择地为新账户启用EKS运行时监控，请使用自己的账户调用该UpdateOrganizationConfigurationAPI 操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例为单个账户同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT 。您也可以传递用空格IDs分隔的账户列表。</p> <p>要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name": "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre> <p>成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p>

管理 GuardDuty 安全代理的首选方法	步骤
监控选择性EKS聚类 (使用包含标签)	<ol style="list-style-type: none">1. 为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -true</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。2. 要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：<ul style="list-style-type: none">• Replace (替换) <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code> 。• Replace (替换) <code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code> 。• Replace (替换) <code>access-project</code> 与 <code>GuardDutyManaged</code>• Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。<p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>3. 要有选择地为新账户启用EKS运行时监控，请使用自己的账户调用该UpdateOrganizationConfigurationAPI 操作 <code>detector ID</code>。 <p>将 <code>EKS_ADDON_MANAGEMENT</code> 的状态设为 <code>DISABLED</code>。</p>

管理 GuardDuty 安全代理的首选方法

步骤

GuardDuty 将管理所有标有 GuardDuty Managed -true 对的 Amazon EKS 集群的安全代理的部署和更新。

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectorsAPI`。detectorId

以下示例为单个账户启用了 EKS_RUNTIME_MONITORING，并禁用了 EKS_ADDON_MANAGEMENT。您也可以传递用空格IDs分隔的账户列表。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectorsAPI`。detectorId

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name": "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'
```

成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<ol style="list-style-type: none"><li data-bbox="678 275 1507 1780"><p data-bbox="678 275 1507 405">1. 要有选择地为新账户启用EKS运行时监控，请使用自己的账户调用该UpdateOrganizationConfigurationAPI操作 <i>detector ID</i>。</p><p data-bbox="678 447 1507 531">将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p><p data-bbox="678 573 1507 804">或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p><p data-bbox="678 846 1507 976">以下示例为单个账户启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT 。您也可以传递用空格IDs分隔的账户列表。</p><p data-bbox="678 1018 1507 1148">要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p><pre data-bbox="760 1190 1507 1507">aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]'</pre><p data-bbox="678 1549 1507 1675">成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。</p><li data-bbox="678 1696 1507 1780">2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。

为单个活跃成员账户启用EKS运行时监控

API/CLI

根据 [管理 GuardDuty 安全代理的方法](#)，您可以选择首选方法，并按照下表中所述的步骤进行操作。

管理 GuardDuty 安全代理的首选方法	步骤
通过管理安全代理 GuardDuty (监控所有EKS集群)	<p>要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理您账户中所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT：</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}]]'</pre> <div data-bbox="678 1623 1507 1789"> <p>Note</p> <p>您也可以传递用空格IDs分隔的账户列表。</p> </div>

管理 GuardDuty 安全代理的首选方法

步骤

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控所有EKS集群，但排除其中一些集群（使用排除标签）</p>	<ol style="list-style-type: none"> <p>为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -false</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户指南中的使用CLI API、或 eksctl 处理标签。</p> <p>要防止修改标签（可信实体除外），请使用《AWS Organizations 用户指南》中防止标签被修改，除非由授权主体修改中的策略。在该策略中，替换以下详细信息：</p> <ul style="list-style-type: none"> Replace（替换）<code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 Replace（替换）<code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code>。 Replace（替换）<code>access-project</code> 与 <code>GuardDutyManaged</code> Replace（替换）<code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>Note</p> <p>在将设置为之前，请务必将排除标签添加到您的EKS集群ENABLED；否则，GuardDuty安全代理将部署在您账户中的所有EKS集群上。STATUS EKS_RUNTIME_MONITORING</p>

管理 GuardDuty 安全代理的首选方法	步骤
	<p>要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 ENABLED。</p> <p>GuardDuty 将管理尚未排除在监控范围之外的所有 Amazon EKS 集群的安全代理的部署和更新。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例同时启用了 EKS_RUNTIME_MONITORING 和 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "Status" : " ENABLED"}]]'</pre> <p>Note 您也可以传递用空格IDs分隔的账户列表。</p>

管理 GuardDuty 安全代理的首选方法	步骤
	成功执行代码后，会返回 <code>UnprocessedAccounts</code> 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
<p>监控选择性EKS聚类 (使用包含标签)</p>	<ol style="list-style-type: none"> 为要排除在监控范围之外的EKS集群添加标签。键值对是 <code>GuardDutyManaged -true</code>。有关添加标签的更多信息，请参阅亚马逊EKS用户 指南中的使用CLI API、或 eksctl 处理标签。 要防止修改标签 (可信实体除外)，请使用《AWS Organizations 用户指南》中 防止标签被修改，除非由授权主体修改 中的策略。在该策略中，替换以下详细信息： <ul style="list-style-type: none"> Replace (替换) <code>ec2:CreateTags</code> 和 <code>eks:TagResource</code>。 Replace (替换) <code>ec2>DeleteTags</code> 和 <code>eks:UntagResource</code>。 Replace (替换) <code>access-project</code> 与 <code>GuardDutyManaged</code> Replace (替换) <code>123456789012</code> 使用可信实体的 AWS 账户 ID。 <p>如果您有多个可信实体，请使用以下示例添加多个 <code>PrincipalArn</code>：</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该 updateMemberDetectorsAPI 操作 <code>detector ID</code>。 <p>将 <code>EKS_ADDON_MANAGEMENT</code> 的状态设为 <code>DISABLED</code>。</p>

管理 GuardDuty 安全代理的首选方法

步骤

GuardDuty 将管理所有标有 GuardDuty Managed -true 对的 Amazon EKS 集群的安全代理的部署和更新。

或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectorsAPI`。detectorId

以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：

```
aws guardduty update-member-detectors --
detector-id 12abc34d567e8fa901bc2d34e56
789f0 --account-ids 111122223333 --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : "DISABLED"}] ]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

管理 GuardDuty 安全代理的首选方法	步骤
手动管理安全代理	<p>1. 要有选择地为您的成员账户启用EKS运行时监控，请使用您自己的账户运行该updateMemberDetectorsAPI操作 <i>detector ID</i>。</p> <p>将 EKS_ADDON_MANAGEMENT 的状态设为 DISABLED。</p> <p>或者，您可以使用自己的区域探测器 ID 来使用该 AWS CLI 命令。要查找您的账户和当前区域的，请参阅https://console.aws.amazon.com/guardduty/控制台中的“设置”页面，或者运行ListDetectorsAPI。detectorId</p> <p>以下示例启用了 EKS_RUNTIME_MONITORING ，并禁用了 EKS_ADDON_MANAGEMENT ：</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 5555555555 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "Status" : " ENABLED"}]]'</pre> <p>2. 要管理安全代理，请参阅 手动管理 Amazon EKS 集群的安全代理。</p>

从EKS运行时监控迁移到运行时监控

随着 GuardDuty 运行时监控的推出，威胁检测范围已扩展到亚马逊ECS容器和亚马逊EC2实例。EKS 运行时监控体验现已整合到运行时监控中。您可以为要监控运行时行为的每种资源类型（Amazon EC2 实例、Amazon ECS 集群和 Amazon EKS 集群）启用运行时监控并管理单独 GuardDuty 的安全代理。

GuardDuty 已将EKS运行时监控的控制台体验整合到运行时监控中。GuardDuty 推荐[检查EKS运行时监控配置状态](#)和[从EKS运行时监控迁移到运行时监控](#)。

作为迁移到运行时监控的一部分，请确保[禁用EKS运行时监控](#)。这一点很重要，因为如果您稍后选择禁用“运行时监控”，但未禁用“EKS运行时监控”，则将继续产生EKS运行时监控的使用成本。

从EKS运行时监控迁移到运行时监控

1. GuardDuty 控制台支持EKS运行时监控作为运行时监控的一部分。

您可以通过[检查EKS运行时监控配置状态](#)您的组织和帐户开始使用运行时监控。

在启用“EKS运行时监控”之前，请确保不要禁用“运行时监控”。如果您禁用EKS运行时监控，Amazon EKS 插件管理也将被禁用。按所列顺序继续执行以下步骤。

2. 确保您满足所有要求[启用运行时监控的先决条件](#)。

3. 通过复制运行时监控的组织配置设置与运行时监控相同的组织配置设置来启用EKS运行时监控。有关更多信息，请参阅[启用运行时监控](#)。

- 如果您有独立帐户，则需要启用运行时监控。

如果您的 GuardDuty 安全代理已经部署，则会自动复制相应的设置，您无需再次配置设置。

- 如果您的组织具有自动启用设置，请确保为运行时监控复制相同的自动启用设置。
- 如果您的组织单独为现有活跃成员帐户配置了设置，请确保启用运行时监控并为这些成员单独配置 GuardDuty 安全代理。

4. 在确保“运行时监控”和“GuardDuty 安全代理”设置正确后，使用API或 AWS CLI 命令[禁用“EKS运行时监控”](#)。

5. (可选) 如果要清理与 GuardDuty 安全代理关联的任何资源，请参阅[禁用和清理资源的影响](#)。

如果您想在不启用EKS运行时监控的情况下继续使用运行时监控，请参阅[配置EKS运行时监控 \(API仅限 \)](#)。

检查EKS运行时监控配置状态

使用以下APIs或 AWS CLI 命令检查EKS运行时监控的现有配置状态。

查看您账户中现有的EKS运行时监控配置状态

- 运行[GetDetector](#)以检查您自己账户的配置状态。
- 或者，您可以使用以下命令运行以下命令 AWS CLI :

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

请务必替换您 AWS 账户 和当前地区的探测器 ID。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 [ListDetectors](#) API。 `detectorId`

检查您组织的现有 EKS 运行时监控配置状态（仅限作为委派 GuardDuty 管理员帐户）

- 运行 [DescribeOrganizationConfiguration](#) 以检查组织的配置状态。

或者，您可以使用以下命令运行以下命令 AWS CLI：

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

请务必将探测器 ID 替换为您委派的 GuardDuty 管理员账户的探测器 ID，将区域替换为您当前的区域。要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 [ListDetectors](#) API。 `detectorId`

迁移到 EKS 运行时监控后禁用运行时监控

在确保您的账户或组织的现有设置已复制到运行时监控后，您可以禁用 EKS 运行时监控。

禁用 EKS 运行时监控

- 在自己的账户中禁用 EKS 运行时监控

[UpdateDetector](#) API 用你自己的区域跑步 *detector-id*。

或者，您可以使用以下 AWS CLI 命令。Replace（替换）

12abc34d567e8fa901bc2d34e56789f0 用你自己的区域 *detector-id*。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "DISABLED"}]'
```

- 对组织中的成员帐户禁用 EKS 运行时监控

在区域赛中 [UpdateMemberDetectors](#) API 大放异彩 *detector-id* 该组织的委派 GuardDuty 管理员帐户。

或者，您可以使用以下 AWS CLI 命令。Replace (替换)

12abc34d567e8fa901bc2d34e56789f0 与区域 *detector-id* 该组织的委派 GuardDuty 管理员账户和 *111122223333* 使用您要禁用此功能的成员帐户的 AWS 账户 ID。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "DISABLED"}]'
```

- 更新组织的EKS运行时监控自动启用设置

只有在将EKS运行时监控自动启用设置配置为组织中的新 (NEW) 或全部 (ALL) 成员帐户时，才执行以下步骤。如果您已经将其配置为NONE，则可以跳过此步骤。

Note

将EKS运行时监控自动启用配置设置为NONE意味着不会为任何现有成员帐户自动启用EKS运行时监控，也不会在新成员帐户加入您的组织时自动启用运行时监控。

在区域赛中[UpdateOrganizationConfiguration](#)API大放异彩 *detector-id* 该组织的委派 GuardDuty 管理员账户。

或者，您可以使用以下 AWS CLI 命令。Replace (替换)

12abc34d567e8fa901bc2d34e56789f0 与区域 *detector-id* 该组织的委派 GuardDuty 管理员账户。更换 *EXISTING_VALUE* 使用您当前的自动启用 GuardDuty配置。

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
--features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

评估资源的运行时间覆盖率

在您启用 Runtime Monitoring 并且 GuardDuty 安全代理部署到您的资源后，会 GuardDuty提供相应资源类型的覆盖率统计信息以及属于您账户的资源的各个覆盖状态的覆盖率统计信息。确定覆盖状态的方法是确保您已启用运行时监控、已创建您的 Amazon VPC 终端节点并已部署相应资源 GuardDuty的安全代理。健康覆盖状态表示当有与您的资源相关的运行时事件时，GuardDuty 能够通过 Amazon VPC 终端节点接收上述运行时事件并监控行为。如果在配置运行时监控、创建 Amazon VPC 终端节

点或部署 GuardDuty安全代理时出现问题，则覆盖状态将显示为“不健康”。当覆盖状态为不健康时，GuardDuty 将无法接收或监视相应资源的运行时行为，也无法生成任何运行时监控结果。

以下主题将帮助您查看覆盖率统计信息、配置 EventBridge 通知以及解决特定资源类型的覆盖率问题。

内容

- [Amazon EC2 实例的覆盖范围](#)
- [Amazon ECS 集群的覆盖范围](#)
- [Amazon EKS 集群的覆盖范围](#)
- [常见问题 \(FAQs\)](#)

Amazon EC2 实例的覆盖范围

对于 Amazon EC2 资源，运行时间覆盖率是在实例级别进行评估的。您的 Amazon EC2 实例可以在您的 AWS 环境中运行多种类型的应用程序和工作负载。此功能还支持亚马逊ECS托管的亚马逊EC2实例，如果您在亚马逊实例上运行亚马逊ECS集群，则EC2实例级别的覆盖问题将显示在亚马逊EC2运行时覆盖范围下。

主题

- [查看覆盖率统计数据](#)
- [配置覆盖状态变更通知](#)
- [排查覆盖问题](#)

查看覆盖率统计数据

与您自己的账户或成员账户关联的 Amazon EC2 实例的覆盖率统计数据是健康EC2实例占所选实例中所有EC2实例的百分比 AWS 区域。下式将其表示为：

$$(\text{运行正常的实例} / \text{所有实例}) * 100$$

如果您还为 Amazon ECS 集群部署了 GuardDuty 安全代理，则与在亚马逊实例上运行的 Amazon ECS 集群相关的任何EC2实例级别覆盖问题都将显示为亚马逊EC2实例运行时覆盖率问题。

选择一种访问方法来查看您账户的覆盖率统计数据。

Console

- 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
- 在导航窗格中，选择“运行时监控”。
- 选择“运行时覆盖范围”选项卡。
- 在EC2实例运行时覆盖率选项卡下，您可以查看按实例列表表中每个可用的 Amazon EC2 实例的覆盖状态汇总的覆盖率统计数据。
 - 您可以按以下列筛选“实例”列表表：
 - 账户 ID
 - 代理管理类型
 - 代理版本
 - 覆盖状态
 - 实例 ID
 - 集群 ARN
- 如果您的任何EC2实例的覆盖状态为“不健康”，则“问题”列将包含有关不健康状态的原因的其他信息。

API/CLI

- [ListCoverage](#) API使用您自己的有效检测器 ID、当前区域和服务端点运行。您可以使用它对实例列表进行筛选和排序API。
 - 您可以使用以下 CriterionKey 选项之一更改示例 filter-criteria：
 - ACCOUNT_ID
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - AGENT_VERSION
 - MANAGEMENT_TYPE
 - INSTANCE_ID
 - CLUSTER_ARN
 - 当filter-criteria包含RESOURCE_TYPE为时 EC2，运行时监控不支持使用ISSUE为AttributeName。如果你使用它，就会得到API响应InvalidInputException。

您可以使用以下选项更改 `sort-criteria` 中的示例 `AttributeName`：

- ACCOUNT_ID
- COVERAGE_STATUS
- INSTANCE_ID
- UPDATED_AT
- 你可以改变 `max-results`（最多 50 个）。
- 要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#) API。 `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}]}' --max-results 5
```

- 运行[GetCoverageStatistics](#) API 以检索基于的覆盖率聚合统计信息 `statisticsType`。
 - 您可以使用以下选项之一更改示例 `statisticsType`：
 - COUNT_BY_COVERAGE_STATUS— 表示按覆盖状态汇总的 EKS 集群的覆盖率统计信息。
 - COUNT_BY_RESOURCE_TYPE— 根据列表中的 AWS 资源类型汇总的覆盖率统计信息。
 - 您可以在命令中更改示例 `filter-criteria`。您可以对 `CriterionKey` 使用以下选项：
 - ACCOUNT_ID
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - AGENT_VERSION
 - MANAGEMENT_TYPE
 - INSTANCE_ID
 - CLUSTER_ARN
 - 要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#) API。 `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
```

```
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",  
"FilterCondition":{"EqualsValue":"123456789012"}]}]}'
```

如果您的EC2实例的覆盖状态为运行状况不佳，请参阅[排查覆盖问题](#)。

配置覆盖状态变更通知

您的 Amazon EC2 实例的覆盖状态可能显示为“不健康”。要了解覆盖状态何时发生变化，我们建议您定期监控覆盖状态，并在状态变为“不健康”时进行故障排除。或者，您可以创建 Amazon EventBridge 规则，以便在保险状态从“不健康”变为“健康”或其他情况时收到通知。默认情况下，会在[EventBridge 公交车](#)上为您的账户 GuardDuty 发布此内容。

示例通知架构

在 EventBridge 规则中，您可以使用预定义的示例事件和事件模式来接收覆盖状态通知。有关创建 EventBridge 规则的更多信息，请参阅 Amazon EventBridge 用户指南中的[创建规则](#)。

此外，您还可以使用以下示例通知架构来创建自定义事件模式。确保替换账户的值。要在您的 Amazon EC2 实例的覆盖状态从变Healthy为时收到通知Unhealthy，detail-type应为 *GuardDuty Runtime Protection Unhealthy*。要在保险状态从变为时收到通知Healthy，Unhealthy请将的detail-type值替换为 *GuardDuty Runtime Protection Healthy*。

```
{  
  "version": "0",  
  "id": "event ID",  
  "detail-type": "GuardDuty Runtime Protection Unhealthy",  
  "source": "aws.guardduty",  
  "account": "AWS ## ID",  
  "time": "event timestamp (string)",  
  "region": "AWS ##",  
  "resources": [  
    ],  
  "detail": {  
    "schemaVersion": "1.0",  
    "resourceAccountId": "string",  
    "currentStatus": "string",  
    "previousStatus": "string",  
    "resourceDetails": {  
      "resourceType": "EC2",  
      "ec2InstanceDetails": {  
        "instanceId": "",  
        "instanceType": "",  

```



```

    "clusterArn": "",
    "agentDetails": {
      "version":""
    },
    "managementType":""
  }
},
"issue": "string",
"lastUpdatedAt": "timestamp"
}
}

```

排查覆盖问题

如果您的 Amazon EC2 实例的覆盖状态为“不健康”，则可以在“问题”列下查看原因。

如果您的 EC2 实例与 EKS 集群相关联，并且的安全代理 EKS 是手动安装或通过自动代理配置安装的，则要解决覆盖范围问题，请参阅[Amazon EKS 集群的覆盖范围](#)。

下表列出了问题类型和相应的故障排除步骤。

问题类型	问题消息	故障排除步骤
	正在等待SSM通知	<p>接收SSM通知可能需要几分钟。</p> <p>确保 Amazon EC2 实例处于SSM托管状态。有关更多信息，请参阅中的“方法 1-使用 S AWS ystems Manager”下的步骤手动安装安全客户端。</p>
没有代理报告 (故意为空)		<p>如果您是手动管理 GuardDuty 安全客户端，请确保按照以下步骤操作手动管理 Amazon EC2 实例的安全代理。</p> <p>如果您启用了自动代理配置：</p> <ul style="list-style-type: none"> 您的EC2实例已被SSM托管。 定期查看您的安全代理的状态。有关更多信息，请参阅正在验证 GuardDuty 安全代理安装状态。 <p>验证您的 Amazon EC2 实例的VPC终端节点配置是否正确。有关更多信息，请参阅如何验证VPC端点配置是否正确？。</p>

问题类型	问题消息	故障排除步骤
		如果您的组织有服务控制策略 (SCP)，请验证权限边界是否限制了 <code>guardduty:SendSecurityTelemetry</code> 权限。有关更多信息，请参阅 验证您的组织服务控制策略 。
	代理已断开连接	<ul style="list-style-type: none"> 查看您的安全代理的状态。有关更多信息，请参阅 正在验证 GuardDuty 安全代理安装状态。 查看安全代理日志以确定潜在的根本原因。日志提供了详细的错误，您可以使用这些错误自行解决问题。日志文件位于下方 <code>/var/log/amzn-guardduty-agent/</code>。 <p>完成 <code>sudo journalctl -u amazon-guardduty-agent</code>。</p>
SSM创建关联失败	GuardDuty SSM 您的账户中已存在关联	<ol style="list-style-type: none"> 手动删除现有关联。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 删除关联。 删除关联后，禁用 Amazon EC2 的 GuardDuty 自动代理配置，然后重新启用。
	您的账户SSM关联过多	<p>选择以下两个选项之一：</p> <ul style="list-style-type: none"> 删除所有未使用的SSM关联。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 删除关联。 检查您的账户是否符合增加配额的资格。有关更多信息，请参阅中的 Systems Manager 服务配额AWS 一般参考。
SSM关联更新失败	GuardDuty SSM 您的账户中不存在关联	GuardDuty SSM您的账户中不存在关联。禁用，然后重新启用“运行时监控”。
SSM关联删除失败	GuardDuty SSM 您的账户中不存在关联	您的账户中不存在该SSM关联。如果SSM关联是故意删除的，则无需执行任何操作。

问题类型	问题消息	故障排除步骤
SSM实例关联执行失败	不符合架构要求或其他先决条件。	<p>有关经过验证的操作系统发行版的信息，请参见Amazon EC2 实例支持的先决条件。</p> <p>如果您仍然遇到此问题，以下步骤将帮助您识别并解决问题：</p> <ol style="list-style-type: none"> 1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。 2. 在导航窗格中的节点管理下，选择状态管理器。 3. 按“文档名称”属性筛选并输入AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin。 4. 选择相应的关联 ID 并查看其执行历史记录。 5. 使用执行历史记录，查看失败，找出潜在的根本原因，然后尝试解决问题。
VPC终端节点创建失败	<p>VPC共享不支持创建端点 VPC <i>vpcId</i></p> <p>仅当使用VPC与自动代理配置共享时</p> <p>所有者账户 ID <i>111122223333</i> 用于共享 VPC <i>vpcId</i> 未启用运行时监控、自动代理配置或两者兼而有之</p>	<p>运行时监控支持在组织VPC内使用共享。有关更多信息，请参阅 使用VPC与自动安全代理共享。</p> <p>共享VPC所有者账户必须为至少一种资源类型 (Amazon EKS 或 Amazon ECS (AWS Fargate)) 启用运行时监控和自动代理配置。有关更多信息，请参阅 特定于 GuardDuty 运行时监控的先决条件。</p>

问题类型	问题消息	故障排除步骤
	<p>启用私有 DNS 需要两者兼enableDnsSupport 而有之，且enableDnsHostnames VPC属性设置true为 <i>vpcId</i> (服务 : Ec2 , 状态代码 : 400 , 请求编号 : <i>a1b2c3d4-5678-90ab-cdef-EXA MPLE11111</i>) .</p>	<p>确保将以下VPC属性设置为 true — enableDnsSupport 和enableDnsHostnames 。有关更多信息，请参阅中的DNS属性VPC。</p> <p>如果您使用亚马逊VPC控制台创建亚马逊VPC，请务必同时选择“启用DNS主机名”和“启用DNS解析”。https://console.aws.amazon.com/vpc/有关更多信息，请参阅VPC配置选项。</p>
共享VPC端点删除失败	<p>不允许删除账户 ID 的共享VPC端点 <i>111122223333</i> ，共享VPC <i>vpcId</i> ，所有者账户 ID <i>555555555555</i> 。</p>	<p>可能的步骤：</p> <ul style="list-style-type: none"> 禁用共享VPC参与者账户的运行时监控状态不会影响共享VPC端点策略和所有者账户中存在的安全组。 <p>要删除共享VPC端点和安全组，您必须在共享VPC所有者帐户中禁用运行时监控或自动代理配置状态。</p> <ul style="list-style-type: none"> 共享VPC参与者账户无法删除共享VPC所有者账户中托管的共享VPC端点和安全组。
代理未报告	<p>(故意为空)</p>	<p>问题类型已终止支持。如果您仍然遇到此问题但尚未这样做，请为 Amazon 启用 GuardDuty 自动代理EC2。</p> <p>如果问题仍然存在，请考虑禁用运行时监控几分钟，然后再次启用。</p>

Amazon ECS 集群的覆盖范围

Amazon ECS 集群的运行时覆盖范围包括运行的任务 AWS Fargate (Fargate) 和亚马逊ECS容器实例¹。

对于在 Fargate 上运行的 Amazon ECS 集群，运行时间覆盖率是在任务级别评估的。ECS集群运行时覆盖范围包括那些在启用 Fargate 的运行时监控和自动代理配置后开始运行的 Fargate 任务（仅限）。ECS默认情况下，Fargate 任务是不可变的。GuardDuty 将无法安装安全代理来监视已在运行的任务上的容器。要包含这样的 Fargate 任务，必须停止并重新启动该任务。请务必检查相关服务是否受支持。

有关 Amazon ECS 容器的信息，请参阅[容量创建](#)。

内容

- [查看覆盖率统计数据](#)
- [配置覆盖状态变更通知](#)
- [排查覆盖问题](#)

查看覆盖率统计数据

与您自己的账户或成员账户关联的 Amazon ECS 资源的覆盖率统计数据是健康的亚马逊ECS集群占所选所有亚马逊ECS集群的百分比 AWS 区域。这包括对与 Fargate 和亚马逊ECS实例关联的亚马逊EC2 集群的保障。下式将其表示为：

$$(\text{正常集群}/\text{所有集群}) * 100$$

注意事项

- 集群的覆盖率统计数据包括与该ECS集群关联的 Fargate 任务或ECS容器实例的ECS覆盖状态。Fargate 任务的覆盖状态包括处于运行状态或最近完成运行的任务。
- 在ECS集群运行时覆盖率选项卡中，已覆盖的容器实例字段表示与您的 Amazon ECS 集群关联的容器实例的覆盖状态。

如果您的 Amazon ECS 集群仅包含 Fargate 任务，则计数将显示为 0/0。

- 如果您的 Amazon ECS 集群与没有安全代理的 Amazon EC2 实例相关联，则该亚马逊ECS集群的覆盖状态也将为“不正常”。

要确定关联亚马逊EC2实例的覆盖范围问题并对其进行故障排除，[排查覆盖问题](#)请参阅 Amazon EC2 实例。

选择一种访问方法来查看您账户的覆盖率统计数据。

Console

- 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
- 在导航窗格中，选择“运行时监控”。
- 选择“运行时覆盖范围”选项卡。
- 在 ECS 集群运行时覆盖率选项卡下，您可以查看按集群列表表中可用的每个 Amazon ECS 集群的覆盖状态汇总的覆盖率统计数据。
 - 您可以按以下列筛选“集群”列表表：
 - 账户 ID
 - 集群名称
 - 代理管理类型
 - 覆盖状态
- 如果您的任何 Amazon ECS 集群的覆盖状态为“不健康”，则“问题”列将包含有关不健康状态的原因的其他信息。

如果您的 Amazon ECS 集群与 Amazon EC2 实例关联，请导航至 EC2 实例运行时覆盖率选项卡，然后按集群名称字段进行筛选以查看关联的问题。

API/CLI

- [ListCoverage](#) API 使用您自己的有效检测器 ID、当前区域和服务端点运行。您可以使用它对实例列表进行筛选和排序 API。
 - 您可以使用以下 CriterionKey 选项之一更改示例 filter-criteria：
 - ACCOUNT_ID
 - ECS_CLUSTER_NAME
 - COVERAGE_STATUS
 - MANAGEMENT_TYPE
 - 您可以使用以下选项更改 sort-criteria 中的示例 AttributeName：
 - ACCOUNT_ID
 - COVERAGE_STATUS
 - ISSUE

- ECS_CLUSTER_NAME
- UPDATED_AT

只有在关联的 Amazon ECS 集群中创建了新任务或相应的覆盖范围状态发生变化时，才会更新该字段。

- 你可以改变 *max-results* (最多 50 个)。
- 要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion":[{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}]}' --max-results 5
```

- 运行[GetCoverageStatistics](#)API以检索基于的覆盖率聚合统计信息statisticsType。
 - 您可以使用以下选项之一更改示例 statisticsType：
 - COUNT_BY_COVERAGE_STATUS— 表示按覆盖状态汇总的ECS集群的覆盖率统计信息。
 - COUNT_BY_RESOURCE_TYPE— 根据列表中的 AWS 资源类型汇总的覆盖率统计信息。
 - 您可以在命令中更改示例 filter-criteria。您可以对 CriterionKey 使用以下选项：
 - ACCOUNT_ID
 - ECS_CLUSTER_NAME
 - COVERAGE_STATUS
 - MANAGEMENT_TYPE
 - INSTANCE_ID
 - 要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "123456789012"}}]}'
```

有关覆盖范围问题的更多信息，请参阅[排查覆盖问题](#)。

配置覆盖状态变更通知

您的 Amazon ECS 集群的覆盖状态可能显示为“不健康”。要了解覆盖状态何时发生变化，我们建议您定期监控覆盖状态，并在状态变为“不健康”时进行故障排除。或者，您可以创建 Amazon EventBridge 规则，以便在保险状态从“不健康”变为“健康”或其他情况时收到通知。默认情况下，会在[EventBridge 公交车](#)上为您的账户 GuardDuty 发布此内容。

示例通知架构

在 EventBridge 规则中，您可以使用预定义的示例事件和事件模式来接收覆盖状态通知。有关创建 EventBridge 规则的更多信息，请参阅 Amazon EventBridge 用户指南中的[创建规则](#)。

此外，您还可以使用以下示例通知架构来创建自定义事件模式。确保替换账户的值。要在您的 Amazon ECS 集群的覆盖状态从变Healthy为时收到通知Unhealthy，detail-type应为 *GuardDuty Runtime Protection Unhealthy*。要在保险状态从变为时收到通知Healthy，Unhealthy请将的detail-type值替换为 *GuardDuty Runtime Protection Healthy*。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
  "time": "event timestamp (string)",
  "region": "AWS ##",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "ECS",
      "ecsClusterDetails": {
        "clusterName": "",
        "fargateDetails": {
          "issues": [],
          "managementType": ""
        },
        "containerInstanceDetails": {
          "coveredContainerInstances": int,
          "compatibleContainerInstances": int
        }
      }
    }
  }
}
```



```

    }
  }
},
"issue": "string",
"lastUpdatedAt": "timestamp"
}
}

```

排查覆盖问题

如果您的 Amazon ECS 集群的覆盖状态为“不健康”，则可以在“问题”列下查看原因。

下表提供了 Fargate (ECS仅限亚马逊) 问题的建议故障排除步骤。有关亚马逊EC2实例覆盖范围问题的信息，[排查覆盖问题](#)请参阅 Amazon EC2 实例。

问题类型	额外信息	建议的问题排查步骤
代理未报告	代理未报告中的任务 TaskDefinition - ' <i>TASK_DEFINITION</i> '	验证您的 Amazon ECS 集群任务的VPC终端节点配置是否正确。有关更多信息，请参阅 如何验证VPC端点配置是否正确？ 。 如果您的组织有服务控制策略 (SCP)，请验证权限边界是否限制了guardduty:SendSecurityTelemetry 权限。有关更多信息，请参阅 验证您的组织服务控制策略 。
	<i>VPC_ISSUE</i> ; for task in TaskDefinition - ' <i>TASK_DEFINITION</i> '	在额外信息中查看VPC问题详情。
代理已退出	ExitCode: EXIT_CODE 用于中的任务 TaskDefinition - ' <i>TASK_DEFINITION</i> '	在额外信息中查看问题详情。
	原因： <i>REASON</i> 用于 中的任务 TaskDefin	

问题类型	额外信息	建议的问题排查步骤
	<p>ition - ' <i>TASK_DEFINITION</i> '</p> <p>ExitCode: EXIT_CODE 有理由: '<i>EXIT_CODE</i>' 用于中的任务 TaskDefinition - ' <i>TASK_DEFINITION</i> '</p> <p>代理已退出: 原因: CannotPullContainerError : 已重试提取图像清单...</p>	<p>任务执行角色必须具有以下亚马逊弹性容器注册表 (Amazon ECR) 权限:</p> <pre data-bbox="933 730 1507 1129"> ... "ecr:GetAuthorizationToken", "ecr:BatchCheckLayerAvailability", "ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage", ... </pre> <p>有关更多信息, 请参阅 提供ECR权限和子网详细信息。</p> <p>添加 Amazon ECR 权限后, 必须重新启动任务。</p> <p>如果问题仍然存在, 请参阅 我的 AWS Step Functions 工作流程意外失败。</p>

问题类型	额外信息	建议的问题排查步骤
VPC终端节点创建失败	启用私有DNS需要两者兼enableDnsSupport 而有之，且enableDnsHostnames VPC属性设置true为 <i>vpcId</i> (服务 : ECS , 状态代码 : 400 , 请求编号 : <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>).	<p>确保将以下VPC属性设置为 true — enableDnsSupport 和enableDnsHostnames 。有关更多信息，请参阅中的DNS属性VPC。</p> <p>如果您使用亚马逊VPC控制台创建亚马逊VPC，请务必同时选择“启用DNS主机名”和“启用DNS解析”。https://console.aws.amazon.com/vpc/有关更多信息，请参阅VPC配置选项。</p>
未配置代理	不支持对中的任务 <i>SERVICE</i> 进行调用 TaskDefinition - ' <i>TASK_DEFINITION</i> '	此任务是由不支持的调用 <i>SERVICE</i> 的。
	不支持的CPU架构 ' <i>TYPE</i> '用于中的任务 TaskDefinition - ' <i>TASK_DEFINITION</i> '	此任务在不支持的CPU架构上运行。有关支持的CPU架构的信息，请参见 验证架构要求 。
	TaskExecutionRole 从中丢失 TaskDefinition - ' <i>TASK_DEFINITION</i> '	缺少ECS任务执行角色。有关提供任务执行角色和所需权限的信息，请参阅 提供ECR权限和子网详细信息 。

问题类型	额外信息	建议的问题排查步骤
	<p>中的任务缺少网络配置</p> <pre><i>CONFIGURATION_DETA</i> <i>ILS</i> "" TaskDefin ition - ' <i>TASK_DEFI</i> <i>NITION</i> '</pre>	<p>由于缺少配置、子网缺失或为空，可能会出现网络VPC配置问题。</p> <p>验证您的网络配置是否正确。有关更多信息，请参阅 提供ECR权限和子网详细信息。</p> <p>有关更多信息，请参阅《亚马逊弹性容器服务开发者指南》中的亚马逊ECS任务定义参数。</p>

问题类型	额外信息	建议的问题排查步骤
其他	未识别的问题，适用于中的任务 TaskDefinition - ' <i>TASK_DEFINITION</i> '	<p>使用以下问题来确定问题的根本原因：</p> <ul style="list-style-type: none"> • 任务是在您启用“运行时监控”之前启动的吗？ <p>在 Amazon 中 ECS，任务是不可变的。要评估正在运行的 Fargate 任务的运行时行为，请确保已启用运行时监控，然后重启任务 GuardDuty 以添加容器 sidecar。</p> <ul style="list-style-type: none"> • 此任务是在启用运行时监控之前启动的服务部署的一部分吗？ <p>如果是，则可以使用更新服务中的步骤重新启动服务或更新服务。forceNewDeployment</p> <p>您也可以使用UpdateService或AWS CLI。</p> <ul style="list-style-type: none"> • 该任务是在将 ECS 集群排除在运行时监控之外后启动的吗？ <p>当您将预定义的 GuardDuty 标签从 GuardDutyManaged -更改 true 为 GuardDutyManaged -时 false，GuardDuty 将不会接收 ECS 集群的运行时事件。</p> <ul style="list-style-type: none"> • 您的服务是否包含旧格式为的任务 taskArn？ <p>GuardDuty 运行时监控不支持覆盖旧格式为的任务 taskArn。</p> <p>有关亚马逊资源的亚马逊资源名称 (ARNs) 的信息，请参阅亚马逊资源名称 (ARNs) 和 IDs。ECS</p>

Amazon EKS 集群的覆盖范围

启用 Runtime Monitoring 并手动EKS或通过自动代理配置安装 GuardDuty 安全代理（附加组件）后，就可以开始评估EKS集群的覆盖范围了。

内容

- [查看覆盖率统计数据](#)
- [配置覆盖状态变更通知](#)
- [排除EKS覆盖范围问题](#)

查看覆盖率统计数据

与您自己的账户或成员账户关联的EKS集群的覆盖率统计数据是健康EKS集群占所选集群中所有EKS集群的百分比 AWS 区域。下式将其表示为：

$$(\text{正常集群}/\text{所有集群}) * 100$$

选择一种访问方法来查看您账户的覆盖率统计数据。

Console

- 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
- 在导航窗格中，选择“运行时监控”。
- 选择EKS集群运行时覆盖率选项卡。
- 在EKS集群运行时覆盖率选项卡下，您可以查看按集群列表表中提供的覆盖率状态汇总的覆盖率统计信息。
 - 您可以按以下列筛选集群列表表：
 - 集群名称
 - 账户 ID
 - 代理管理类型
 - 覆盖状态
 - 插件版本
- 如果您的任何EKS群集的覆盖状态为 Un healthy，则“问题”列可能包含有关不健康状态的原因的其他信息。

API/CLI

- [ListCoverage](#) API 使用您自己的有效检测器 ID、区域和服务端点运行。您可以使用它对集群列表进行筛选和排序 API。
 - 您可以使用以下 CriterionKey 选项之一更改示例 filter-criteria：
 - ACCOUNT_ID
 - CLUSTER_NAME
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - ADDON_VERSION
 - MANAGEMENT_TYPE
 - 您可以使用以下选项更改 sort-criteria 中的示例 AttributeName：
 - ACCOUNT_ID
 - CLUSTER_NAME
 - COVERAGE_STATUS
 - ISSUE
 - ADDON_VERSION
 - UPDATED_AT
 - 你可以改变 *max-results* (最多 50 个)。
 - 要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}] }' --max-results 5
```

- 运行 [GetCoverageStatistics](#) API 以检索基于的覆盖率聚合统计信息 statisticsType。
 - 您可以使用以下选项之一更改示例 statisticsType：
 - COUNT_BY_COVERAGE_STATUS— 表示按覆盖状态汇总的 EKS 集群的覆盖率统计信息。
 - COUNT_BY_RESOURCE_TYPE— 根据列表中的 AWS 资源类型汇总的覆盖率统计信息。
 - 您可以在命令中更改示例 filter-criteria。您可以对 CriterionKey 使用以下选项：

- CLUSTER_NAME
 - RESOURCE_TYPE
 - COVERAGE_STATUS
 - ADDON_VERSION
 - MANAGEMENT_TYPE
- 要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#) API。detectorId

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey": "ACCOUNT_ID", "FilterCondition":{"EqualsValue": "123456789012"}}] }'
```

如果您的EKS集群的覆盖状态为“运行状况不佳”，请参阅[排除EKS覆盖范围问题](#)。

配置覆盖状态变更通知

您账户中EKS集群的覆盖状态可能显示为“不健康”。要检测覆盖状态何时变为不正常，我们建议您定期监控覆盖状态，并在状态变为不正常时进行问题排查。或者，您可以创建 Amazon EventBridge 规则，以便在保险状态从变Unhealthy为Healthy或其他状态时通知您。默认情况下，会在[EventBridge公告](#)上为您的账户 GuardDuty 发布此内容。

示例通知架构

在 EventBridge 规则中，您可以使用预定义的示例事件和事件模式来接收覆盖状态通知。有关创建 EventBridge 规则的更多信息，请参阅 Amazon EventBridge 用户指南中的[创建规则](#)。

此外，您还可以使用以下示例通知架构来创建自定义事件模式。确保替换账户的值。要在您的 Amazon EKS 集群的覆盖状态从变Healthy为Healthy时收到通知Unhealthy，detail-type应为 *GuardDuty Runtime Protection Unhealthy*。要在保险状态从变为时收到通知Healthy，Unhealthy请将的detail-type值替换为 *GuardDuty Runtime Protection Healthy*。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS ## ID",
```



```

"time": "event timestamp (string)",
"region": "AWS ##",
"resources": [
  ],
"detail": {
  "schemaVersion": "1.0",
  "resourceAccountId": "string",
  "currentStatus": "string",
  "previousStatus": "string",
  "resourceDetails": {
    "resourceType": "EKS",
    "eksClusterDetails": {
      "clusterName": "string",
      "availableNodes": "string",
      "desiredNodes": "string",
      "addonVersion": "string"
    }
  },
  "issue": "string",
  "lastUpdatedAt": "timestamp"
}
}

```

排除EKS覆盖范围问题

如果EKS集群的覆盖率状态为Unhealthy，则可以在 GuardDuty 控制台的“问题”列下或使用[CoverageResource](#)数据类型查看相应的错误。

使用包含或排除标签来有选择地监控您的EKS集群时，这些标签可能需要一些时间才能同步。这可能会影响关联EKS群集的覆盖状态。您可以再次尝试删除并添加相应的标签（包含或排除）。有关更多信息，请参阅《亚马逊EKS用户指南》中的为您的亚马逊EKS[资源添加标签](#)。

覆盖问题的结构是 Issue type:Extra information。通常，问题会有一个可选的额外信息，其中可能包括特定的客户端异常或有关问题的描述。根据额外信息，下表提供了解决EKS集群覆盖问题的推荐步骤。

问题类型（前缀）	额外信息	建议的问题排查步骤
插件创建失败	插件aws-guardduty-agent 与集群的当前集群版本不兼容	确保你使用的是支持部署插件的 Kubernetes 版本之一。aws-guard

问题类型 (前缀)	额外信息	建议的问题排查步骤
	<p><i>ClusterName</i> 。不支持指定的插件。</p>	<p>duty-agent EKS有关更多信息，请参阅 安全代理支持的 Kubernetes 版本 GuardDuty。有关更新 Kubernetes 版本的信息，请参阅更新亚马逊EKS集群 Kubernetes 版本。</p>
<p>插件创建失败</p> <p>插件更新失败</p> <p>插件状态不健康</p>	<p>EKS插件问题-AddonIssueCode : AddonIssueMessage</p>	<p>有关特定插件问题代码的推荐步骤的信息，请参阅Troubleshooting steps for Addon creation/ updatation error with Addon issue code。</p> <p>有关您可能在此问题中遇到的插件问题代码列表，请参阅AddonIssue。</p>
<p>VPC终端节点创建失败</p>	<p>VPC共享不支持创建端点 VPC <i>vpcId</i></p> <p>仅当使用VPC与自动代理配置共享时</p> <p>所有者账户 ID <i>111122223333</i> 用于共享 VPC <i>vpcId</i> 没有启用运行时监控、自动代理配置或两者兼而有之。</p>	<p>运行时监控现在支持在组织VPC内使用共享。确保您的账户满足所有先决条件。有关更多信息，请参阅 使用共享的先决条件 VPC。</p> <p>共享VPC所有者账户必须为至少一种资源类型 (Amazon EKS 或 Amazon ECS (AWS Fargate)) 启用运行时监控和自动代理配置。有关更多信息，请参阅 特定于 GuardDuty运行时监控的先决条件。</p>

问题类型 (前缀)	额外信息	建议的问题排查步骤
	<p>启用私有DNS需要两者兼enableDns Support 而有之，且enableDns Hostnames VPC属性设置true为 <i>vpcId</i> (服务 : Ec2, 状态代码 : 400, 请求编号 : <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i>).</p>	<p>确保将以下VPC属性设置为 true — enableDns Support 和enableDns Hostnames 。有关更多信息，请参阅中的DNS属性VPC。</p> <p>如果您使用亚马逊VPC控制台创建亚马逊VPC，请务必同时选择“启用DNS主机名”和“启用DNS解析”。https://console.aws.amazon.com/vpc/有关更多信息，请参阅VPC配置选项。</p>
共享VPC端点删除失败	<p>不允许删除账户 ID 的共享VPC端点 <i>111122223333</i> ，共享 VPC <i>vpcId</i> ，所有者账户 ID <i>555555555555</i> 。</p>	<p>可能的步骤：</p> <ul style="list-style-type: none"> 禁用共享VPC参与者账户的运行时监控状态不会影响共享VPC端点策略和所有者账户中存在的安全组。 <p>要删除共享VPC端点和安全组，您必须在共享VPC所有者帐户中禁用运行时监控或自动代理配置状态。</p> <ul style="list-style-type: none"> 共享VPC参与者账户无法删除共享VPC所有者帐户中托管的共享VPC端点和安全组。

问题类型 (前缀)	额外信息	建议的问题排查步骤
本地EKS集群	EKS本地前哨集群不支持插件。	不可操作。 如需了解更多信息，请参阅 Amazon EKS 关于 AWS 前哨基地 。
EKS未授予运行时监控启用权限	(可能显示额外信息，也可能不显示额外信息)	<ol style="list-style-type: none"> 1. 如果有关于此问题的额外信息，请解决根本原因并执行下一步。 2. 切换“EKS运行时监控”以将其关闭，然后再次将其打开。无论是自动部署 GuardDuty 还是手动部署，都要确保 GuardDuty 代理也已部署。
EKS运行时监控启用资源配置正在进行中	(可能显示额外信息，也可能不显示额外信息)	不可操作。 启用EKS运行时监控后，覆盖范围的状态可能会保持不变，Unhealthy 直到资源配置步骤完成。定期监控和更新覆盖状态。
其他 (任何其他问题)	由于授权失败而导致的错误	切换“EKS运行时监控”以将其关闭，然后再次将其打开。确保 GuardDuty 代理也已通过自动部署 GuardDuty 或手动部署。

	故障排除步骤
<p>插件创建或更新错误</p> <p>EKS插件问题-InsufficientNumber OfReplicas : 该插件运行状况不佳，因为它没有所需的副本数量。</p>	<ul style="list-style-type: none"> 使用问题消息，您可以确定并修复根本原因。您可以先描述您的集群。例如，kubectl describe pods用于确定 Pod 故障的根本原因。 <p>修复根本原因后，请重试该步骤（创建或更新附加组件）。</p> <ul style="list-style-type: none"> 如果问题仍然存在，请验证您的 Amazon EKS 集群的VPC终端节点配置是否正确。有关更多信息，请参阅 如何验证VPC端点配置是否正确？。
<p>EKS插件问题-AdmissionRequestDenied : 准入 webhook "validate.kyverno.svc-fail" 拒绝了请求:资源违规政策DaemonSet /amazon-guardduty/aws-guardduty-agent :: restrict-image-registries:... autogen-validate-registries</p>	<ol style="list-style-type: none"> Amazon EKS 集群或安全管理员必须查看阻止插件更新的安全策略。 您必须禁用控制器 (webhook) 或让控制器接受 Amazon 的请求EKS。
<p>EKS插件问题-ConfigurationConflict : 尝试申请时发现冲突。由于存在解决冲突模式，因此无法继续。Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image</p>	<p>创建或更新插件时，请提供OVERWRITE 解决冲突标志。这可能会覆盖使用 Kubernetes 直接对 Kubernetes 中的相关资源所做的任何更改。API 您可以先删除插件，然后重新安装。</p>
<p>EKS插件问题-AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group</p>	<p>您必须eks:addon-cluster-admin ClusterRoleBinding 手动将缺少的权限添加到。将以下内容添加yaml到eks:addon-cluster-admin :</p> <pre>---</pre>

插件创建或更新错误	故障排除步骤
<p>"scheduling.k8s.io" at the cluster scope</p>	<pre>kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/v1 metadata: name: eks:addon-cluster-admin subjects: - kind: User name: eks:addon-manager apiGroup: rbac.authorization.k8s.io roleRef: kind: ClusterRole name: cluster-admin apiGroup: rbac.authorization.k8s.io ---</pre> <p>现在，您可以使用以下命令yaml将其应用于您的 Amazon EKS 集群：</p> <pre>kubectl apply -f eks-addon-cluster-admin.yaml</pre>
<p>EKS插件问题-AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespaces-must-have-label-owner] All namespaces must have an `owner` label</p>	<p>您必须禁用控制器或让控制器接受来自 Amazon EKS 集群的请求。</p> <p>在创建或更新插件之前，您还可以创建一个 GuardDuty 命名空间并将其标记为owner。</p>

常见问题 (FAQs)

内容

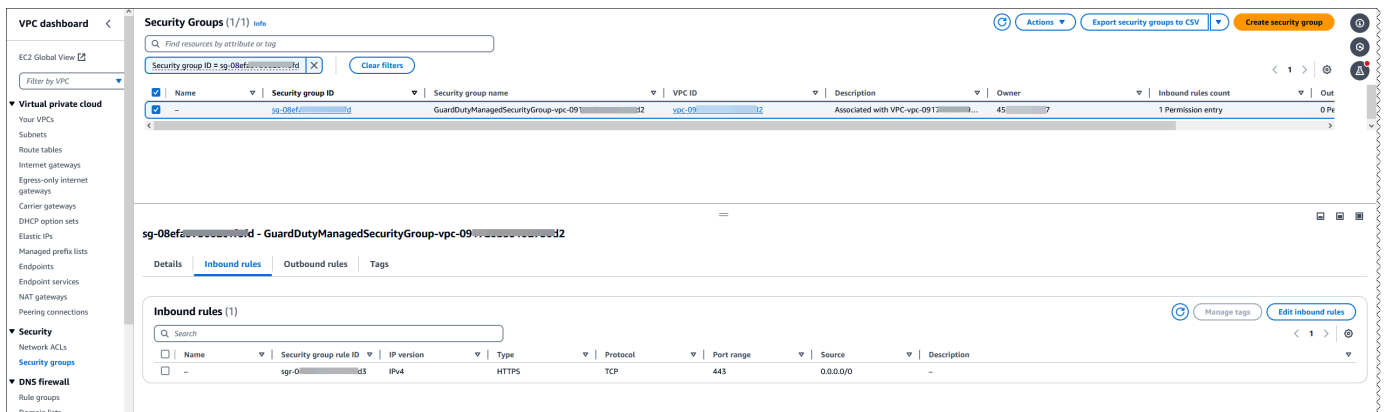
- [如何验证VPC端点配置是否正确？](#)
- [为什么我的资源处于保险状态Unhealthy？](#)
- [谁可以查看属于我的资源的运行时覆盖状态 AWS 账户？](#)

- [如何验证 GuardDuty 安全代理是否在 Fargate 任务上运行？](#)
- [更多疑难解答问题](#)

如何验证VPC端点配置是否正确？

使用以下步骤验证VPC所有者账户中是否正确设置了资源类型的VPC端点配置：

1. 登录 AWS Management Console 并打开 Amazon VPC 控制台，网址为 <https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中的虚拟私有云下，选择端点。
3. 在终端节点表中，选择服务名称与 `com.amazonaws` 相似的行。**`us-east-1.guardduty-data`**。您的终端节点的区域 (`us-east-1`) 可能有所不同。
4. 将出现一个包含端点详细信息的面板。在“安全组”选项卡下，选择关联的组 ID 链接以获取更多详细信息。
5. 在“安全组”表中，选择具有关联安全组 ID 的行以查看详细信息。
6. 在“入站规则”选项卡下，确保存在端口范围为 443、源为 0.0.0.0/0 的入口策略。入站规则控制允许到达实例的传入流量。下图显示了与安全代理VPC使用的安全组关联 GuardDuty 的安全组的入站规则。



如果您还没有启用入站端口 443 的安全组，请在 Amazon EC2 用户指南中[创建安全组](#)。

如果在限制您的VPC (或集群) 的入站权限时出现问题，请为来自任何 IP 地址 (0.0.0.0/0) 的入站 443 端口提供支持。

为什么我的资源处于保险状态Unhealthy？

如果您刚刚部署了 GuardDuty 安全客户端（通过自动代理配置或手动配置），或者按照建议的步骤对覆盖范围问题进行故障排除，则覆盖范围状态可能需要几分钟才能恢复正常。您可以定期检查保险状态，也可以将 Amazon EventBridge (EventBridge) 配置为在保险状态发生变化时收到通知。

此外，您还可以验证资源的终VPC端节点配置是否正确。有关更多信息，请参阅 [如何验证VPC端点配置是否正确？](#)。

谁可以查看属于我的资源的运行时覆盖状态 AWS 账户？

作为成员账户或独立账户，您可以查看与自己的账户关联的资源的覆盖率统计信息。作为组织的委托 GuardDuty 管理员账户，您可以查看与您的账户关联的资源以及属于您的组织的成员账户的覆盖率统计信息。

如何验证 GuardDuty 安全代理是否在 Fargate 任务上运行？

GuardDuty 安全代理作为 Fargate 任务的边车容器运行。

选择一种首选方法来验证任务运行时是否显示了 sidecar 容器。

Amazon ECS console

1. 在 <https://console.aws.amazon.com/ecs/v2> 中打开控制台。
2. 在导航窗格中，选择集群。
3. 在集群页面上，选择关联的集群名称以获取更多详细信息。
4. 选择 Tasks 选项卡。
5. 选择关联的任务链接以查看任务详细信息。
6. 在任务详细信息页面上，容器表包含边车详细信息。容器运行时 ID 将以您的任务 ID 为前缀。

CLI

运行describe-tasks并查找名称设置为、设置为aws-gd-agent的lastStatus容器RUNNING。

以下示例显示了任务的默认集群的输出 `aws:ecs:us-east-1:123456789012:task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE`

输出

名为的容器aws-gd-agent处于RUNNING状态。


```
"containers": [  
  {  
    "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/4df26bb4-f057-467b-a079-96167EXAMPLE",  
    "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE",  
    "lastStatus": "RUNNING",  
    "healthStatus": "UNKNOWN",  
    "memory": "1 GB",  
    "name": "aws-gd-agent"  
  }  
]
```

有关更多信息，请参阅[描述任务](#)。

更多疑难解答问题

有关您的 Fargate 任务的更多疑难解答问题，请参阅《亚马逊弹性容器服务开发者FAQs指南》中的[运行时监控疑难解答](#)。

设置CPU和内存监控

启用运行时监控并评估集群的覆盖状态是否为“正常”后，您可以设置和查看洞察指标。

以下主题可以帮助您评估已部署的代理在 GuardDuty 代理CPU和内存限制下的性能。

在 Amazon ECS 集群上设置监控

Amazon CloudWatch 用户指南中的以下步骤可以帮助您根据代理的内存限制评估已部署 GuardDuty 代理的执行情况：CPU

1. [在 Amazon 上设置集群和服务级别指标ECS的 Container Insights](#)
2. [Amazon ECS 容器洞察指标](#)

在 Amazon EKS 集群上设置监控

部署 GuardDuty 安全代理并评估集群的覆盖状态是否为“正常”后，您可以设置和查看容器洞察指标。

评估安全代理的性能

1. 在亚马逊用户指南中@@@ [在亚马逊EKS和 Kubernetes 上设置容器见解 CloudWatch](#)
2. [亚马逊用户EKS指南中的亚马逊和 Kubernetes 容器洞察指标 CloudWatch](#)

使用安全代理 v1.5.0 及更高版本管理性能

在安全代理 [v1.5.0 及更高版本中](#)，当见解表明关联的 GuardDuty 代理已达到分配的限制时，您可以配置特定参数。有关更多信息，请参阅 [配置EKS插件参数](#)。

收集的 GuardDuty 使用运行时事件类型

GuardDuty 安全代理收集以下事件类型并将其发送到 GuardDuty后端以进行威胁检测和分析。GuardDuty 并不能让你访问这些事件。如果 GuardDuty 检测到潜在威胁并生成运行时监控结果，则可以查看相应的发现详细信息。有关如何 GuardDuty 使用收集的事件类型的更多信息，请参阅[选择不使用您的数据来改善服务](#)。

处理事件

字段名称	描述
进程名称	观察到的进程的名称。
进程路径	进程可执行文件的绝对路径。
进程 ID	操作系统分配给进程的 ID。
命名空间 PID	除主机级PID命名空间之外的辅助PID命名空间中进程的进程 ID。对于容器内的进程，命名空间 PID 是容器内观察到的进程 ID。
进程用户 ID	执行进程的用户的唯一 ID。
进程 UUID	分配给流程的唯一 ID GuardDuty。
进程 GID	进程组的进程 ID。
进程 EGID	进程组的有效组 ID。
进程 EUID	进程的有效用户 ID。

字段名称	描述
进程用户名	执行进程的用户名。
进程开始时间	创建进程的时间。此字段采用UTC日期字符串格式 (2023-03-22T19:37:20.168Z)。
进程可执行文件 SHA -256	进程可执行文件的 SHA256 哈希值。
进程脚本路径	执行的脚本文件的路径。
进程环境变量	可供进程使用的环境变量。仅收集 LD_PRELOAD 和 LD_LIBRARY_PATH 。
流程呈现工作目录 (PWD)	进程的当前工作目录。
父进程	父进程的进程详细信息。父进程是创建观察到的进程的进程。
命令行参数	执行流程时提供的命令行参数。此字段可能包含敏感的客户数据。
<p>目前，此字段仅限于与资源类型对应的特定代理版本：</p> <ul style="list-style-type: none"> • Fargate (ECS仅限亚马逊) ， GuardDuty 安全代理 v1.0.0 及更高版本。 • 使用 GuardDuty 安全代理 v1.0.0 及更高版本的 Amazon EC2 实例。 • 使用安全代理 v1.4.0 及更高版本的亚马逊 EKS 集群。 <p>有关更多信息，请参阅 GuardDuty 代理发布历史记录。</p>	

容器事件

字段名称	描述
容器名称	容器的名称。 如果可用，该字段将显示标签 <code>io.kubernetes.container.name</code> 的值。
容器 UID	容器运行时分配的容器的唯一 ID。
容器运行时	用于运行容器的容器运行时（例如 <code>docker</code> 或 <code>containerd</code> ）。
容器映像 ID	容器映像的 ID。
容器映像名称	容器映像的名称。

AWS Fargate（ECS仅限亚马逊）任务事件

字段名称	描述
任务 Amazon 资源名称 (ARN)	ARN任务的。
集群名称	Amazon ECS 集群的名称。
姓氏	任务定义的姓氏。用作family用于启动任务的任务定义的名称。
服务名称	Amazon ECS 服务的名称（如果任务是作为服务的一部分启动的）。
启动类型	运行任务的基础架构。对于资源类型为的运行时监控ECSCluster，启动类型可以是EC2或FARGATE。
CPU	任务定义中表示的任务使用的CPU单位数。

Kubernetes 容器组事件

字段名称	描述
容器组 ID	Kubernetes 容器组的 ID。
容器组名称	Kubernetes 容器组的名称。
容器组命名空间	Kubernetes 工作负载所属的 Kubernetes 命名空间的名称。
Kubernetes 集群名称	Kubernetes 集群的名称。

DNS事件

字段名称	描述
套接字类型	指示通信语义的套接字类型。例如，SOCK_RAW。
地址系列	表示与地址关联的通信协议。例如，地址系列 AF_INET 用于 IP v4 协议。
方向 ID	连接方向的 ID。
协议编号	第 4 层协议号，例如 17 代表UDP和 6 表示TCP。
DNS远程端点 IP	连接的远程 IP。
DNS远程端点端口	连接的端口号。
DNS本地端点 IP	连接的本地 IP。
DNS本地端点端口	连接的端口号。
DNS有效载荷	包含DNS查询和响应DNS的数据包的有效负载。

公开事件

字段名称	描述
文件路径	在此事件中打开的文件的完整路径。
Flags	描述文件访问模式，例如只读、只写和读写。

加载模块事件

字段名称	描述
模块名称	加载到内核中的模块的名称。

Mprotect 事件

字段名称	描述
地址范围	修改访问保护的地址范围。
内存区域	指定进程地址空间的区域，例如堆栈和堆。
Flags	表示控制此事件行为的选项。

挂载事件

字段名称	描述
挂载目标	挂载源的挂载路径。
挂载源	挂载到挂载目标的主机上的路径。
文件系统类型	表示已安装的类型fileSystem。
Flags	表示控制此事件行为的选项。

链接事件

字段名称	描述
链接路径	创建硬链接的路径。
目标路径	硬链接指向的文件路径。

符号链接事件

字段名称	描述
链接路径	创建符号链接的路径。
目标路径	符号链接指向的文件路径。

Dup 事件

字段名称	描述
旧文件描述符	表示打开的文件对象的文件描述符。
新文件描述符	与旧文件描述符重复的新文件描述符。新旧文件描述符表示同一个打开的文件对象。
Dup 远程端点 IP	由旧文件描述符表示的网络套接字的远程 IP 地址。仅当旧文件描述符表示网络套接字时才适用。
Dup 远程端点端口	由旧文件描述符表示的网络套接字的远程端口。仅当旧文件描述符表示网络套接字时才适用。
Dup 本地端点 IP	由旧文件描述符表示的网络套接字的本地 IP 地址。仅当旧文件描述符表示网络套接字时才适用。
Dup 本地端点端口	由旧文件描述符表示的网络套接字的本地端口。仅当旧文件描述符表示网络套接字时才适用。

内存映射事件

字段名称	描述
文件路径	内存映射到的文件的路径。

套接字事件

字段名称	描述
地址系列	表示与地址关联的通信协议。例如，地址系列 AF_INET 用于 IP 版本 4 协议。
套接字类型	指示通信语义的套接字类型。例如，SOCK_RAW。
协议编号	指定地址系列中的特定协议。通常，地址系列中只有一个协议。例如，地址系列 AF_INET 只有 IP 协议。

连接事件

字段名称	描述
地址系列	表示与地址关联的通信协议。例如，地址系列 AF_INET 用于 IP v4 协议。
套接字类型	指示通信语义的套接字类型。例如，SOCK_RAW。
协议编号	指定地址系列中的特定协议。通常，地址系列中只有一个协议。例如，地址系列 AF_INET 只有 IP 协议。
文件路径	地址系列为 AF_UNIX 时的套接字文件的路径。
远程端点 IP	连接的远程 IP。
远程端点端口	连接的端口号。
本地端点 IP	连接的本地 IP。

字段名称	描述
本地端点端口	连接的端口号。

进程 VM Readv 事件

字段名称	描述
Flags	表示控制此事件行为的选项。
目标 PID	正在从中读取内存的进程的进程 ID。
目标进程 UUID	目标进程的唯一 ID。
目标可执行文件路径	目标进程可执行文件的绝对路径。

进程 VM Writev 事件

字段名称	描述
Flags	表示控制此事件行为的选项。
目标 PID	正在向其写入内存的进程的进程 ID。
目标进程 UUID	目标进程的唯一 ID。
目标可执行文件路径	目标进程可执行文件的绝对路径。

Ptrace 事件

字段名称	描述
目标 PID	目标进程的进程 ID。
目标进程 UUID	目标进程的唯一 ID。

字段名称	描述
目标可执行文件路径	目标进程可执行文件的绝对路径。
Flags	表示控制此事件行为的选项。

绑定事件

字段名称	描述
地址系列	表示与地址关联的通信协议。例如，地址系列 AF_INET 用于 IP v4 协议。
插座类型	指示通信语义的套接字类型。例如，SOCK_RAW。
协议编号	第 4 层协议号，例如 17 代表UDP和 6 表示TCP。
本地端点 IP	连接的本地 IP。
本地端点端口	连接的端口号。

收听事件

字段名称	描述
地址系列	表示与地址关联的通信协议。例如，地址系列 AF_INET 用于 IP v4 协议。
插座类型	指示通信语义的套接字类型。例如，SOCK_RAW。
协议编号	第 4 层协议号，例如 17 代表UDP和 6 表示TCP。
本地端点 IP	连接的本地 IP。
本地端点端口	连接的端口号。

重命名事件

字段名称	描述
文件路径	重命名的文件的路径。
目标	文件的新路径。

设置UID事件

字段名称	描述
全新 EUID	流程的新有效用户 ID。
全新 UID	进程的新用户 ID。

Chmod 事件

字段名称	描述
文件路径	调用此事件的文件的路径。
文件模式	关联文件已更新的访问权限。

Amazon ECR 存储库托管 GuardDuty 代理

以下各节列出了亚马逊弹性容器注册表 (Amazon ECR) 存储库，其中 GuardDuty 托管部署在您的亚马逊 EKS 和亚马逊 ECS 集群上的安全代理。

内容

- [EKS代理版本 1.6.0 或更高版本的存储库](#)
- [EKS代理版本 1.5.0 及更早版本的存储库](#)
- [GuardDuty 代理存储库 AWS Fargate \(ECS仅限 Amazon \)](#)

EKS代理版本 1.6.0 或更高版本的存储库

下表显示了每个ECR存储亚马逊EKS插件代理版本 (aws-guardduty-agent) 1.6.0 及更高版本的亚马逊存储库。AWS 区域

AWS 区域	亚马逊ECR存储库 URI
美国西部 (俄勒冈州)	602401143452.dkr.ecr.us-west-2.amazonaws.com
欧洲地区 (巴黎)	602401143452.dkr.ecr.eu-west-3.amazonaws.com
亚太地区 (孟买)	602401143452.dkr.ecr.ap-south-1.amazonaws.com
亚太地区 (海得拉巴)	900889452093.dkr.ecr.ap-south-2.amazonaws.com
加拿大 (中部)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
加拿大西部 (卡尔加里)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
中东 (UAE)	759879836304.dkr.ecr.me-central-1.amazonaws.com
欧洲地区 (伦敦)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
美国西部 (加利福尼亚北部)	602401143452.dkr.ecr.us-west-1.amazonaws.com
美国东部 (弗吉尼亚州北部)	602401143452.dkr.ecr.us-east-1.amazonaws.com
美国东部 (俄亥俄州)	602401143452.dkr.ecr.us-east-2.amazonaws.com
欧洲地区 (爱尔兰)	602401143452.dkr.ecr.eu-west-1.amazonaws.com

AWS 区域	亚马逊ECR存储库 URI
南美洲 (圣保罗)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
欧洲地区 (斯德哥尔摩)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
欧洲地区 (法兰克福)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
欧洲 (苏黎世)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
亚太地区 (新加坡)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
亚太地区 (悉尼)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
亚太地区 (雅加达)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pacific (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
亚太地区 (首尔)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
亚太地区 (大阪)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
亚太地区 (香港)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
中东 (巴林)	759879836304.dkr.ecr.me-south-1.amazonaws.com
欧洲地区 (米兰)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
欧洲 (西班牙)	455263428931.dkr.ecr.eu-south-2.amazonaws.com

AWS 区域	亚马逊ECR存储库 URI
非洲 (开普敦)	877085696533.dkr.ecr.af-south-1.amazonaws.com
亚太地区 (墨尔本)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
以色列 (特拉维夫)	066635153087.dkr.ecr.il-central-1.amazonaws.com

EKS代理版本 1.5.0 及更早版本的存储库

下表显示了每个ECR AWS 区域存储亚马逊EKS插件代理版本 (aws-guardduty-agent) 1.5.0 及更早版本的亚马逊存储库。

AWS 区域	亚马逊ECR存储库 URI
美国西部 (俄勒冈州)	039403964562.dkr.ecr.us-west-2.amazonaws.com
欧洲地区 (巴黎)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
亚太地区 (孟买)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
亚太地区 (海得拉巴)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
加拿大 (中部)	001188825231.dkr.ecr.ca-central-1.amazonaws.com
中东 (UAE)	601769779514.dkr.ecr.me-central-1.amazonaws.com
欧洲地区 (伦敦)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
美国西部 (加利福尼亚北部)	373421517865.dkr.ecr.us-west-1.amazonaws.com

AWS 区域	亚马逊 ECR 存储库 URI
美国东部 (弗吉尼亚州北部)	<code>031903291036.dkr.ecr.us-east-1.amazonaws.com</code>
美国东部 (俄亥俄州)	<code>591382732059.dkr.ecr.us-east-2.amazonaws.com</code>
欧洲地区 (爱尔兰)	<code>673884943994.dkr.ecr.eu-west-1.amazonaws.com</code>
南美洲 (圣保罗)	<code>941219317354.dkr.ecr.sa-east-1.amazonaws.com</code>
欧洲地区 (斯德哥尔摩)	<code>366771026645.dkr.ecr.eu-north-1.amazonaws.com</code>
欧洲地区 (法兰克福)	<code>409493279830.dkr.ecr.eu-central-1.amazonaws.com</code>
欧洲 (苏黎世)	<code>718440343717.dkr.ecr.eu-central-2.amazonaws.com</code>
亚太地区 (新加坡)	<code>584580519942.dkr.ecr.ap-southeast-1.amazonaws.com</code>
亚太地区 (悉尼)	<code>011662287384.dkr.ecr.ap-southeast-2.amazonaws.com</code>
亚太地区 (雅加达)	<code>617474730032.dkr.ecr.ap-southeast-3.amazonaws.com</code>
Asia Pacific (Tokyo)	<code>781592569369.dkr.ecr.ap-northeast-1.amazonaws.com</code>
亚太地区 (首尔)	<code>732248494576.dkr.ecr.ap-northeast-2.amazonaws.com</code>
亚太地区 (大阪)	<code>810724417379.dkr.ecr.ap-northeast-3.amazonaws.com</code>

AWS 区域	亚马逊ECR存储库 URI
亚太地区 (香港)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
中东 (巴林)	541829937850.dkr.ecr.me-south-1.amazonaws.com
欧洲地区 (米兰)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
欧洲 (西班牙)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
非洲 (开普敦)	379032919888.dkr.ecr.af-south-1.amazonaws.com
亚太地区 (墨尔本)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
以色列 (特拉维夫)	292660727137.dkr.ecr.il-central-1.amazonaws.com

GuardDuty 代理存储库 AWS Fargate (ECS仅限 Amazon)

下表显示了托管每个ECR存储库的 GuardDuty 代理 AWS Fargate (ECS仅限亚马逊) AWS 区域。

AWS 区域	亚马逊ECR存储库 URI
美国西部 (俄勒冈州)	733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (巴黎)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (孟买)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (海得拉巴)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate

AWS 区域	亚马逊 ECR 存储库 URI
加拿大 (中部)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
中东 (UAE)	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (伦敦)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
美国西部 (加利福尼亚北部)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
美国东部 (弗吉尼亚州北部)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
美国东部 (俄亥俄州)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (爱尔兰)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
南美洲 (圣保罗)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (斯德哥尔摩)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (法兰克福)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲 (苏黎世)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (新加坡)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (悉尼)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate

AWS 区域	亚马逊ECR存储库 URI
亚太地区 (雅加达)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacific (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (首尔)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (大阪)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (香港)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
中东 (巴林)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲地区 (米兰)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
欧洲 (西班牙)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate
非洲 (开普敦)	197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate
亚太地区 (墨尔本)	251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate
以色列 (特拉维夫)	870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate

GuardDuty 代理发布历史记录

以下各节提供了在亚马逊EC2实例、亚马逊集群和亚马逊ECSEKS集群上部署的 GuardDuty 代理的发布版本

GuardDuty Amazon EC2 实例的安全代理

代理版本	发布说明	可用日期
v1.3.0	<p>一般性能调整和增强</p> <p>包括支持捕获更多安全信号，以备将来使用运行时监控查找类型。</p>	2024年8月19日
v1.2.0	<p>支持操作系统发行版 Ubuntu 20.04、Ubuntu 22.04、Debian 11 和 Debian 12</p> <p>支持内核 6.5 和 6.8</p> <p>一般性能调整和增强</p>	2024 年 6 月 13 日
v1.1.0	<p>支持在 Amazon EC2 实例的运行时监控中 GuardDuty 自动配置代理</p> <p>支持EC2实例运行时监控宣布正式上线后发布的新安全信号和发现</p> <p>一般性能调整和增强</p>	2024 年 3 月 26 日
v1.0.2	支持最新的 Amazon ECS AMIs。	2024 年 2 月 2 日
v1.0.1	<p>在 v1.0.2 之前发布的代理版本与 2024 年 1 月 31 日之后 ECSAMIs发布的亚马逊不兼容。</p> <p>一般性能调整和增强</p>	2024 年 1 月 23 日
v1.0.0	RPM安装的初始版本	2023 年 11 月 26 日

代理版本	发布说明	可用日期
	在 v1.0.2 之前发布的代理版本与 2024 年 1 月 31 日之后 ECSAMIs 发布的亚马逊不兼容。	

RPM S3 bucket example script

公钥、x86_64 的签名 RPM、arm64 RPM 4 的签名以及指向 Amazon S3 存储桶中托管的 RPM 脚本的相应访问链接可以由以下模板构成。替换 AWS 区域、AWS 账户 ID 和 GuardDuty 代理版本的值以访问 RPM 脚本。以下模板包括适用于 Amazon EC2 实例的最新代理版本。

- 公钥：

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem
```

- GuardDuty 安全代理 RPM 签名：

x86_64 的签名 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig
```

arm64 的签名 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- 访问 Amazon S3 存储桶中 RPM 脚本的链接：

x86_64 的访问链接 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm
```

arm64 的访问链接 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.rpm
```

Debian S3 bucket example script

公钥、带有 arm64 的签名以及指向 Amazon S3 存储桶中托管的脚本的相应访问链接可以由以下模板构成。替换 AWS 区域、AWS 账户 ID 和 GuardDuty 代理版本的价值以访问脚本。以下模板包括适用于 Amazon EC2 实例的最新代理版本。

- 公钥：

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/publickey.pem
```

- GuardDuty 安全代理签名：

amd64 的签名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.sig
```

arm64 的签名

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- 访问 Amazon S3 存储桶中脚本的链接：

amd64 的访问链接

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.deb
```

arm64 的访问链接

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.deb
```

AWS 区域	区域名称	AWS 账号
eu-west-1	欧洲地区 (爱尔兰)	694911143906
us-east-1	美国东部 (弗吉尼亚州北部)	593207742271

us-east-2	美国东部 (俄亥俄州)	733349766148
eu-west-3	欧洲地区 (巴黎)	665651866788
us-east-2	美国东部 (俄亥俄州)	307168627858
eu-central-1	欧洲地区 (法兰克福)	323658145986
ap-northeast-2	亚太地区 (首尔)	914738172881
eu-north-1	欧洲地区 (斯德哥尔摩)	591436053604
ap-east-1	亚太地区 (香港)	258348409381
me-south-1	中东 (巴林)	536382113932
eu-west-2	欧洲地区 (伦敦)	892757235363
ap-northeast-1	Asia Pacific (Tokyo)	533107202818
ap-southeast-1	亚太地区 (新加坡)	174946120834
ap-south-1	亚太地区 (孟买)	251508486986
ap-southeast-3	亚太地区 (雅加达)	510637619217
sa-east-1	南美洲 (圣保罗)	758426053663
ap-northeast-3	亚太地区 (大阪)	273192626886
eu-south-1	欧洲地区 (米兰)	266869475730
af-south-1	非洲 (开普敦)	197869348890
ap-southeast-2	亚太地区 (悉尼)	005257825471
me-central-1	中东 (UAE)	000014521398
us-west-1	美国西部 (加利福尼亚北部)	684579721401
ca-central-1	加拿大 (中部)	354763396469

ap-south-2	亚太地区 (海得拉巴)	950823858135
eu-south-2	欧洲 (西班牙)	919611009337
eu-central-2	欧洲 (苏黎世)	529164026651
ap-southeast-4	亚太地区 (墨尔本)	251357961535
il-central-1	以色列 (特拉维夫)	870907303882

GuardDuty 安全代理 AWS Fargate (ECS仅限 Amazon)

下表显示了 Fargate GuardDuty 安全代理的版本历史记录 (ECS仅限亚马逊)。

代理版本	容器映像	发布说明	可用日期
v1.3.0	x86_64 (): AMD64 sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831 Graviton () ARM64: sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1	一般性能调整和增强。 包括支持捕获更多安全信号，以备将来使用 GuardDuty运行时监控查找类型 。	2024 年 8 月 9 日
v1.2.0	x86_64 (): AMD64 sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton () ARM64: sha256:91930f8446f5f95b93b8ccb18773992affa401	一般性能调整和增强。	2024年5月31日

代理版本	容器映像	发布说明	可用日期
	eb3f42da89d68077a5 6bafa6cd		
v1.1.0	x86_64 (): AMD64 sha256:83 ce3cf2ef85a349ed17 97a8cf30a008ac5d8c 9f673f2835823957e9 dcf71657 Graviton () ARM64: sha256:0d 4b61648d7bdeab8ab8 d94684f805498927c7 d437d318204dcccfe8 c9383dc7	支持新的安全信号和发现。 一般性能调整和增强。	2024年5月1日
v1.0.1	x86_64 (): AMD64 sha256:9f 8cd438fb66f62d09bf c641286439f7ed5177 988a314a6021ef4ff8 80642e68 Graviton () ARM64: sha256:82 c66bb615bd0d1e96db 77b1f1fb51dc03220c aa593b1962249571bf 7147d1b7	一般性能调整和增强。	2024年1月26日

代理版本	容器映像	发布说明	可用日期
v1.0.0	x86_64 (): AMD64 sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017 Graviton () ARM64: sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984	首次发布 GuardDuty 的安全代理 AWS Fargate (ECS仅限 Amazon)。	2023 年 11 月 26 日

GuardDuty 适用于 Amazon EKS 集群的安全代理

下表显示了 [Amazon EKS 插件 GuardDuty 代理](#) 的发布版本历史记录。

代理版本	容器映像	发布说明	可用日期	标准支持终止 1
v1.7.0	x86_64 (): AMD64 sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec Graviton () ARM64: sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbbe47ecfaeb2784435cf67ebe0a	一般性能调整和增强。 包括支持捕获更多安全信号，以备将来使用 运行时监控查找类型 。	2024年8月17日	–
v1.6.1	x86_64 (): AMD64 sha256:30650708a6601f6d6b9046f54b30f	一般性能调整和增强。	2024 年 5 月 14 日	–

代理版本	容器映像	发布说明	可用日期	标准支持终止 1
	5fd65af296b1e40b8c 24426b9bdb07c3ab1 Graviton () ARM64: sha256:5f637c42ffb 306b20f776d9d83e1e 0b4be40ce245be44af cf43a8902b4d71019			
v1.6.0	x86_64 (): AMD64 sha256:7dabcbee30d 8b053676752fbc19e8 9f77272d9a6a53cc93 731f5872180ef9010 Graviton () ARM64: sha256:9710f53afcc df4f22b265a1a6fc27 f1469403af1f7d5d08 c4869a7269cdd2650	<ul style="list-style-type: none"> 支持EKS/EC2资源的GuardDuty自动代理配置。 支持新的安全信号和发现。有关更多信息，请参阅收集的GuardDuty使用运行时事件类型和运行时监控查找类型。 一般性能调整和增强。 	2024 年 4 月 29 日	–

代理版本	容器映像	发布说明	可用日期	标准支持终止 1
v1.5.0	<p>x86_64 (): AMD64 sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d</p> <p>Graviton () ARM64: sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6</p>	<ul style="list-style-type: none"> • 一般性能调整和增强。 • 安全增强功能，包括下方的新事件类型收集的运行时事件类型。 • 围绕CPU使用情况的性能增强。 	2024年3月7日	—
v1.4.1	<p>x86_64 (): AMD64 sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c</p> <p>Graviton () ARM64: sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dff e0792c9e6d0778b40</p>	一般性能调整和增强。	2024年1月16日	—

代理版本	容器映像	发布说明	可用日期	标准支持终止 1
v1.4.0	<p>x86_64 (): AMD64 sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f</p> <p>Graviton () ARM64: sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e</p>	<p>Manifest 挂载点支持更好的数据收集</p> <p>AppArmor 清单中的配置</p> <p>收集命令行参数</p> <p>一般性能调整和增强</p>	2023 年 12 月 21 日	–
v1.3.1	<p>x86_64 (): AMD64 sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29</p> <p>Graviton () ARM64: sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd</p>	重要的安全补丁和更新。	2023 年 10 月 23 日	–

代理版本	容器映像	发布说明	可用日期	标准支持终止 1
v1.3.0	<p>x86_64 (): AMD64 sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbb69530bfbfd46c694</p> <p>Graviton () ARM64: sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb</p>	<p>支持 Ubuntu 平台</p> <p>支持 Kubernetes 版本 1.28</p> <p>一般性能增强和稳定性改进。</p>	2023 年 10 月 5 日	–
v1.2.0	<p>x86_64 (): AMD64 sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3</p> <p>Graviton () ARM64: sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa</p>	<p>除了AMD64基于实例之外，v1.2.0现在还支持ARM64基于实例的实例。增加并验证了对 Bottlerocket 的支持</p> <p>支持 Kubernetes 版本 1.27</p> <p>一般性能增强和稳定性改进。</p>	2023 年 6 月 16 日	–

代理版本	容器映像	发布说明	可用日期	标准支持终止 ¹
v1.1.0	sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c	除了 安全代理支持的 Kubernetes 版本 GuardDuty 之外，此代理版本还支持 Kubernetes 版本 1.26。 一般性能增强和稳定性改进。	2023 年 5 月 2 日	2024 年 5 月 14 日
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e	Amazon EKS 插件代理的初始版本。	2023 年 3 月 30 日	2024 年 5 月 14 日

¹ 有关更新标准支持即将结束的当前代理版本的信息，请参阅[手动更新安全代理](#)。

禁用和清理资源的影响

AWS 账户 如果您选择禁用 Runtime Monitoring，或者仅对资源类型禁用 GuardDuty 自动代理配置，则本节适用于您。

禁用 GuardDuty 自动代理配置

GuardDuty 不会移除部署在您的资源上的安全代理。但是，GuardDuty 将停止管理安全客户端的更新。

GuardDuty 继续接收来自您的资源类型的运行时事件。为防止影响您的使用情况统计信息，请务必从您的资源中移除 GuardDuty 安全代理。

无论是否 AWS 账户 使用共享VPC终端节点，都 GuardDuty 不会删除该VPC终端节点。如果需要，您需要手动删除VPC终端节点。

禁用运行时监控和EKS运行时监控

本节适用于以下场景：

- 您从未单独启用EKS运行时监控，现在您禁用了运行时监控。
- 您正在禁用“运行时监控”和“EKS运行时监控”。如果您不确定EKS运行时监控的配置状态，请参阅[检查EKS运行时监控配置状态](#)。

在不禁用运行时监控的情况下禁用EKS运行时监控

在这种情况下，在某个时间点，您启用了EKS运行时监控，之后还启用了运行时监视而不禁用EKS运行时监控。

现在，禁用“运行时监控”时，还需要禁用“EKS运行时监控”；否则，EKS运行时监控将继续产生使用成本。

如果前面列出的场景适用于您，则 GuardDuty 将在您的账户中执行以下操作：

- GuardDuty 删除带VPC有GuardDutyManaged:true标签的。VPC这是 GuardDuty 为管理自动安全代理而创建的。
- GuardDuty 删除标记为GuardDutyManaged:的安全组true。
- 对于已由至少一个参与者账户VPC使用的共享，GuardDuty 既不会删除VPC终端节点，也不会删除与共享VPC资源关联的安全组。
- 对于 Amazon EKS 资源，GuardDuty 删除安全代理。这与手动管理还是通过管理无关 GuardDuty。

对于 Amazon ECS 资源，由于ECS任务不可变，因此 GuardDuty 无法从该资源中卸载安全代理。这与您管理安全代理的方式无关，无论是手动还是自动管理 GuardDuty。禁用“运行时监控”后，在新ECS任务开始运行时 GuardDuty 不会附加 sidecar 容器。有关使用 Fargate ECS 任务的信息，请参阅[运行时监控如何与 Fargate 配合使用 \(仅限亚马逊ECS\)](#)

对于亚马逊EC2资源，只有在满足以下条件时，才能从所有 Systems Manager (SSM) 托管的亚马逊EC2实例上 GuardDuty 卸载安全代理：

- 您的资源未标有GuardDutyManaged:false排除标签。
- GuardDuty 必须有权访问实例元数据中的标签。对于此EC2资源，“访问实例元数据中的标签”设置为“允许”。

当您停止手动管理安全客户端时

无论使用哪种方法部署和管理 GuardDuty 安全代理，要停止监控资源中的运行时事件，都必须移除 GuardDuty 安全代理。当您想要停止监控账户中某个资源类型的运行时事件时，也可以删除 Amazon VPC 终端节点。

清理安全代理资源的流程

删除亚马逊VPC终端节点

- 没有共享 VPC — 当您不想再监控账户中的资源时，可以考虑删除 Amazon VPC 终端节点。
- 对于共享 VPC — 当共享VPC所有者账户删除仍在使用的共享VPC资源时，您的共享所有VPC者账户和参与账户中资源的EKS运行时监控（以及适用的运行时监控）覆盖状态可能会变得不健康。有关保险状态的信息，请参阅[评估资源的运行时间覆盖率](#)。

有关更多信息，请参阅[删除接口端点](#)。

删除安全组

- 没有共享 VPC — 当您不想再监控账户中的资源类型时，可以考虑删除与 Amazon 关联的安全组 VPC。
- 使用共享 VPC — 当共享VPC所有者账户删除安全组时，当前正在使用与共享安全组关联的任何参与者账户VPC、共享所有者账户和参与VPC者账户中资源的运行时监控覆盖状态都可能变为不健康。有关更多信息，请参阅[评估资源的运行时间覆盖率](#)。

有关更多信息，请参阅[删除安全组](#)。

从EKS集群中移除 GuardDuty 安全代理

要从EKS集群中移除您不想再监控的安全代理，请参阅[删除插件](#)。

移除EKS插件代理不会将amazon-guardduty命名空间从EKS集群中移除。要删除 amazon-guardduty 命名空间，请参阅[删除命名空间](#)。

删除amazon-guardduty命名空间（EKS集群）

禁用自动代理配置不会自动从EKS集群中移除amazon-guardduty命名空间。要删除 amazon-guardduty 命名空间，请参阅[删除命名空间](#)。

GuardDuty 恶意软件防护 EC2

恶意软件防护通过扫描附加到[亚马逊弹性计算云 \(AmazonEBS\) 实例和容器工作负载的亚马逊弹性区块存储 \(AmazonEC2\) 卷](#)来EC2帮助您检测恶意软件的潜在存在。恶意软件防护EC2提供扫描选项，您可以在扫描时决定是要包含还是排除特定的 Amazon EC2 实例和容器工作负载。它还提供了一个选项，可以在您的 GuardDuty 账户中保留附加到 Amazon EC2 实例或容器工作负载的 Amazon EBS 卷的快照。只有在发现恶意软件并生成针对EC2发现的恶意软件防护时，才会保留快照。

的恶意软件防护EC2是一项可选的增强功能，其设计方式不会影响资源的性能。GuardDuty有关恶意软件防护在内部EC2的工作原理的信息 GuardDuty，请参阅[恶意软件防护中的功能 EC2](#)。有关不同版本EC2中恶意软件防护可用性的信息 AWS 区域，请参阅[区域和端点](#)。

备注

GuardDuty 的恶意软件防护EC2不支持亚马逊或EKS亚马逊上的 Fargate。ECS

恶意软件防护EC2提供两种类型的扫描，用于检测您的 Amazon EC2 实例和容器工作负载中的潜在恶意活动：GuardDuty启动的恶意软件扫描和按需恶意软件扫描。下表展示这两种扫描类型的比较情况。

因素	GuardDuty-启动的恶意软件扫描	按需恶意软件扫描
如何调用扫描	启用 GuardDuty启动的恶意软件扫描后，每当 GuardDuty 生成发现指示 Amazon EC2 实例或容器工作负载中可能存在恶意软件时，都会 GuardDuty 自动对附加到可能受影响的资源的 Amazon EBS 卷启动无代理恶意软件扫描。有关更多信息，请参阅 GuardDuty-启动的恶意软件扫描 。	您可以通过提供与您的 Amazon EC2 实例或容器工作负载关联的 Amazon 资源名称 (ARN) 来启动按需恶意软件扫描。即使您的资源未生成任何 GuardDuty 结果，您也可以启动按需恶意软件扫描。有关更多信息，请参阅 按需恶意软件扫描 。
需要配置	要使用 GuardDuty启动的恶意软件扫描，必须为自己的帐户	您的帐户必须已 GuardDuty 启用。要使用按需恶意软件

因素	GuardDuty-启动的恶意软件扫描	按需恶意软件扫描
	启用该功能。有关更多信息，请参阅 配置 GuardDuty启动的恶意软件扫描 。	扫描，无需在功能级别进行配置。
等待以发起新的扫描	每当 GuardDuty 生成其中一个 调用 GuardDuty启动的恶意软件扫描的发现 ，恶意软件扫描仅每 24 小时自动启动一次。	在上一次扫描开始后 1 小时后，您可以随时对同一资源启动按需恶意软件扫描。
30 天免费试用期的可用性	当您在账户中首次启用 GuardDuty启动的恶意软件扫描时，可以使用 30 天的免费试用期*。 有关 GuardDuty启动的恶意软件扫描的更多信息，请参阅 30 天免费试用 。	针对新账户或现有 GuardDuty 账户的按需恶意软件扫描没有免费试用期*。
扫描选项	配置 GuardDuty启动的恶意软件扫描后，恶意软件防护EC2 还可以帮助您选择要扫描或跳过的资源。恶意软件防护EC2 不会对您选择排除在扫描范围之外的资源启动自动扫描。	按需恶意软件扫描支持全局标记 —GuardDutyExcluded 。 使用用户定义的标签扫描选项 不适用于按需恶意软件扫描，因为资源是ARN手动提供的。

*创建EBS卷快照和保留快照将产生使用费用。有关配置账户以保留快照的更多信息，请参阅[快照保留](#)。

恶意软件防护中的功能 EC2

弹性块存储 (EBS) 卷

本节介绍恶意软件保护（包括 GuardDuty启动的EC2恶意软件扫描和按需恶意软件扫描）如何扫描与您的 Amazon EC2 实例和容器工作负载关联的 Amazon EBS 卷。在继续之前，请考虑以下自定义项：

- 扫描选项 — 恶意软件防护EC2提供指定标签的功能，以便在扫描过程中包含或排除亚马逊EC2实例和亚马逊EBS卷。只有 GuardDuty启动的恶意软件扫描才支持带有用户定义标签的扫描选项。GuardDuty启动的恶意软件扫描和按需恶意软件扫描都支持全局GuardDutyExcluded标记。有关更多信息，请参阅 [使用用户定义的标签扫描选项](#)。
- 快照保留 — 恶意软件防护EC2提供了在 AWS 账户中保留 Amazon EBS 卷快照的选项。默认情况下，此选项处于关闭状态。您可以为 GuardDuty 已启动和按需的恶意软件扫描选择快照保留。有关更多信息，请参阅 [快照保留](#)。

当 GuardDuty 生成表明在 Amazon EC2 实例或容器工作负载中可能存在恶意软件的调查结果，并且您已在“恶意软件保护”中启用 GuardDuty 了已 GuardDuty启动的扫描类型时EC2，可能会根据您的扫描选项调用已启动的恶意软件扫描。

要对与亚马逊EC2实例关联的亚马逊EBS卷启动按需恶意软件扫描，请提供亚马逊EC2实例的亚马逊资源名称 (ARN)。

作为对按需恶意软件扫描或自动调用的 GuardDuty恶意软件扫描的响应，GuardDuty 创建附加到可能受影响的资源的相关EBS卷的快照，并与共享。[GuardDuty 服务账号](#)根据这些快照，在服务帐户中 GuardDuty 创建一个加密的副本EBS卷。

有关 GuardDuty 恶意软件检测方法及其使用的扫描引擎的信息，请参阅[GuardDuty 恶意软件检测扫描引擎](#)。

扫描完成后，GuardDuty 删除加密的副本EBS卷和卷的快照。如果发现恶意软件并且您已开启快照保留设置，则您的EBS卷快照不会被删除，而是会自动保留在您的 AWS 帐户中。如果未发现任何恶意软件，则无论快照保留期设置如何，都不会保留EBS卷的快照。默认情况下，快照保留设置处于关闭状态。有关快照成本及其保留的信息，请参阅 [Amazon EBS 定价](#)。

GuardDuty 将在服务帐户中保留每个副本EBS卷最多 55 小时。如果服务中断，或者副本EBS卷及其恶意软件扫描失败，则该EBS卷 GuardDuty 将保留不超过七天。延长卷保留期是为了对中断或故障进行分类和解决。GuardDuty 的恶意软件保护EC2将在中断或故障得到解决后，或者在延长的保留期过后从服务帐户中删除副本EBS卷。

支持用于恶意软件扫描的 Amazon EBS 卷

在所有 GuardDuty 支持“恶意软件保护” EC2 功能 AWS 区域 的地方，您都可以扫描未加密或加密的 Amazon EBS 卷。您可以使用客户托管密钥[AWS 托管式密钥](#)或[客户托管密钥](#)加密的 Amazon EBS 卷。目前，其中一些 AWS 区域 支持两种方式来加密您的Amazon EBS 卷，而另一些则仅支持客户托管密钥。

有关尚不支持此功能的更多信息，请参阅 [China Regions](#)

以下列表描述了无论您的 Amazon EBS 卷是否加密所 GuardDuty 使用的密钥：

- 未加密或加密的 Amazon EBS 卷 GuardDuty 使用自己的密钥对副本 Amazon EBS 卷进行加密。
AWS 托管式密钥

当您的账户 AWS 区域 属于不支持扫描使用[默认加密的 Amazon EBS 卷的 Amazon 卷时EBS](#)，[AWS 托管式密钥](#) 请参阅[修改亚马逊EBS卷的默认 AWS KMS 密钥 ID](#)。

- 使用@@ 客户托管密钥加密的 Amazon EBS 卷 — GuardDuty 使用相同的密钥来加密副本EBS卷。

的恶意软件防护EC2不支持使用 a productCode s 扫描 Amazon EC2 实例marketplace。如果针对这样的 Amazon EC2 实例启动了恶意软件扫描，则会跳过扫描。有关更多信息，请参阅[恶意软件扫描期间跳过资源的原因](#)中的UNSUPPORTED_PRODUCT_CODE_TYPE。

修改亚马逊EBS卷的默认 AWS KMS 密钥 ID

默认情况下，在[CreateVolume](#)API加密设置为true而不指定KMS密钥 ID 的情况下调用，会创建一个使用[默认加密密 AWS KMS 钥](#)加密的 Amazon EBS 卷。EBS但是，如果未明确提供加密密钥，则可以通过调用[ModifyEbsDefaultKmsKeyId](#)API或使用相应的 AWS CLI 命令来修改默认密钥。

要修改EBS默认密钥 ID，请在您的IAM策略中添加以下必要权

限-ec2:modifyEbsDefaultKmsKeyId。您选择加密但未指定关联KMS密钥 ID 的任何新创建的 Amazon EBS 卷都将使用默认密钥 ID。使用以下方法之一更新EBS默认密钥 ID：

修改亚马逊EBS卷的默认KMS密钥 ID

请执行以下操作之一：

- 使用 API —您可以使用 [ModifyEbsDefaultKmsKeyId](#)API. 有关如何查看卷加密状态的信息，请参阅[创建 Amazon EBS 卷](#)。
- 使用 AWS CLI 命令 — 以下示例修改默认KMS密钥 ID，如果您不提供密钥 ID，则该密KMS钥将加密 Amazon EBS 卷。请务必将区域替换为您 AWS 区域的 KM 密钥 ID。

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

上述命令将生成与下方输出类似的输出：

```
{
```

```
"KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"  
}
```

有关更多信息，请参阅 [modify-ebs-default-kms-key-id](#)。

恶意软件防护中的自定义设置 EC2

本节介绍在按需启动或通过调用恶意软件扫描时，如何自定义亚马逊EC2实例或容器工作负载的扫描选项 GuardDuty。

常规设置

快照保留

GuardDuty 为您提供在 AWS 账户中保留EBS卷快照的选项。默认情况下，快照保留设置处于关闭状态。只有在扫描开始之前开启此设置时，系统才会保留快照。

扫描启动后，根据EBS卷的快照 GuardDuty 生成副本EBS卷。扫描完成并且您账户中的快照保留设置已开启后，只有在发现并[适用于 EC2 查找类型的恶意软件防护](#)生成恶意软件时，才会保留EBS卷的快照。无论您是否开启了快照保留设置，当未检测到恶意软件时，GuardDuty 都会自动删除EBS卷的快照。

快照使用成本

在恶意软件扫描期间，在 GuardDuty 创建 Amazon EBS 卷的快照时，会产生与该步骤相关的使用成本。如果您为账户开启快照保留设置，则当系统发现恶意软件并保留快照时，将因此产生使用费用。有关快照成本及其保留的信息，请参阅 [Amazon EBS 定价](#)。

选择您的首选访问方式以开启快照保留设置。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格的“保护计划”下，选择“恶意软件防护” EC2。
3. 在控制台底部选择常规设置。如要保留快照，请开启快照保留。

API/CLI

1. 运行[UpdateMalwareScanSettings](#)以更新快照保留设置的当前配置。

2. 或者，当 GuardDuty 恶意软件防护 EC2 生成发现结果时，您可以运行以下 AWS CLI 命令自动保留快照。

确保更换 `detector-id` 用你自己的有效证件 `detectorId`。

3. 要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors API](#)。 `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

4. 如果要关闭快照保留，请将 `RETENTION_WITH_FINDING` 替换为 `NO_RETENTION`。

使用用户定义的标签扫描选项

通过使用 GuardDuty 启动的恶意软件扫描，您还可以指定标签，以便在扫描和威胁检测过程中包括或排除亚马逊 EC2 实例和亚马逊 EBS 卷。您可以通过编辑包含或排除标签列表中的标签来自定义每个 GuardDuty 启动的恶意软件扫描。每个列表最多可以包含 50 个标签。

如果您还没有与 EC2 资源关联的用户定义标签，请参阅亚马逊用户指南中的为 [您的亚马逊 EC2 资源添加标签或在亚马逊 EC2 用户指南中为您的亚马逊 EC2 资源添加标签](#)。

Note

按需恶意软件扫描不支持带有用户定义标签的扫描选项，而是支持 [全局 GuardDutyExcluded 标签](#)。

将 EC2 实例排除在恶意软件扫描之外

如果您想在扫描过程中排除任何亚马逊 EC2 实例或亚马逊 EBS 卷，则可以将任何亚马逊 EC2 实例或亚马逊 EBS 卷 `true` 的 `GuardDutyExcluded` 标签设置为，并且 GuardDuty 不会对其进行扫描。有关 `GuardDutyExcluded` 标签的更多信息，请参阅 [恶意软件防护的服务相关角色权限 EC2](#)。您也可以将 Amazon EC2 实例标签添加到排除列表中。如果您在排除标签列表中添加多个标签，则任何至少包含其中一个标签的 Amazon EC2 实例都将被排除在恶意软件扫描过程之外。

选择您的首选访问方法，将与 Amazon EC2 实例关联的标签添加到排除列表中。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格的“保护计划”下，选择“恶意软件防护” EC2。
3. 展开包含/排除标签部分。选择添加标签。
4. 选择排除标签，然后选择确认。
5. 指定要排除的标签 **Key** 和 **Value** 对。可以选择提供 **Value**。添加所有标签后，选择保存。

Important

标签键和值区分大小写。[有关更多信息，请参阅亚马逊EC2用户指南中的标签限制或亚马逊EC2用户指南中的标签限制。](#)

如果未提供密钥的值并且该EC2实例使用指定的密钥进行标记，则无论标签的分配值如何，该EC2实例都将被排除在 GuardDuty启动的恶意软件扫描扫描过程之外。

API/CLI

- 通过将EC2实例或容器工作负载排除在扫描过程之外，更新恶意软件扫描设置。

以下 AWS CLI 示例命令将新标签添加到排除标签列表中。确保替换示例 *detector-id* 用你自己的有效证件detectorId。

MapEquals 是 Key/Value 对的列表。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

⚠ Important

标签键和值区分大小写。[有关更多信息，请参阅亚马逊EC2用户指南中的标签限制或亚马逊EC2用户指南中的标签限制。](#)

在恶意软件扫描中包含EC2实例

如果要扫描EC2实例，请将其标签添加到包含列表中。当您将标签添加到包含标签列表时，不包含任何已添加标签的EC2实例将从恶意软件扫描中跳过。如果您向包含标签列表中添加多个标签，则恶意软件扫描中将包含至少包含其中一个标签的EC2实例。有时，在扫描过程中可能会跳过EC2实例。有关更多信息，请参阅[恶意软件扫描期间跳过资源的原因](#)。

选择您的首选访问方法，将与EC2实例关联的标签添加到包含列表中。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格的“保护计划”下，选择“恶意软件防护” EC2。
3. 展开包含/排除标签部分。选择添加标签。
4. 选择包含标签，然后选择确认。
5. 选择添加新的包含标签，然后指定要包含的标签 **Key** 和 **Value** 对。可以选择提供 **Value**。

添加完所有包含标签后，选择保存。

如果未提供密钥的值，则该EC2实例将使用指定的密钥进行标记，则无论该标签的分配值如何，该EC2实例都将包含在恶意软件防护中进行EC2扫描。

API/CLI

- 更新恶意软件扫描设置，在扫描过程中包括EC2实例或容器工作负载。

以下 AWS CLI 示例命令将新标签添加到包含标签列表中。请务必替换示例 *detector-id* 用你自己的有效证件detectorId。替换示例 *TestKey* 以及 *TestValue* 使用Key与您的EC2资源关联的标签的和Value对。

MapEquals 是 Key/Value 对的列表。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#) API。detectorId

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Include": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Important

标签键和值区分大小写。[有关更多信息，请参阅亚马逊EC2用户指南中的标签限制或亚马逊EC2用户指南中的标签限制。](#)

Note

检测到新标签最多可能需要 5 分钟。GuardDuty

您可以随时选择包含标签或排除标签，但不能同时选择两者。如果要在标签之间切换，请在添加新标签时从下拉菜单中选择该标签，然后确认您的选择。此操作将清除您当前的所有标签。

全局 GuardDutyExcluded 标签

默认情况下，您的EBS卷快照是使用GuardDutyScanId标签创建的。请勿删除此标签，因为这样做会GuardDuty阻止访问快照。恶意软件防护中的两种扫描类型都EC2不会扫描GuardDutyExcluded标签设置为的 Amazon EC2 实例或 Amazon EBS 卷true。如果对此类资源EC2使用恶意软件防护进行扫描，则会生成扫描 ID，但会跳过扫描，并说明EXCLUDED_BY_SCAN_SETTINGS原因。有关更多信息，请参阅[恶意软件扫描期间跳过资源的原因](#)。

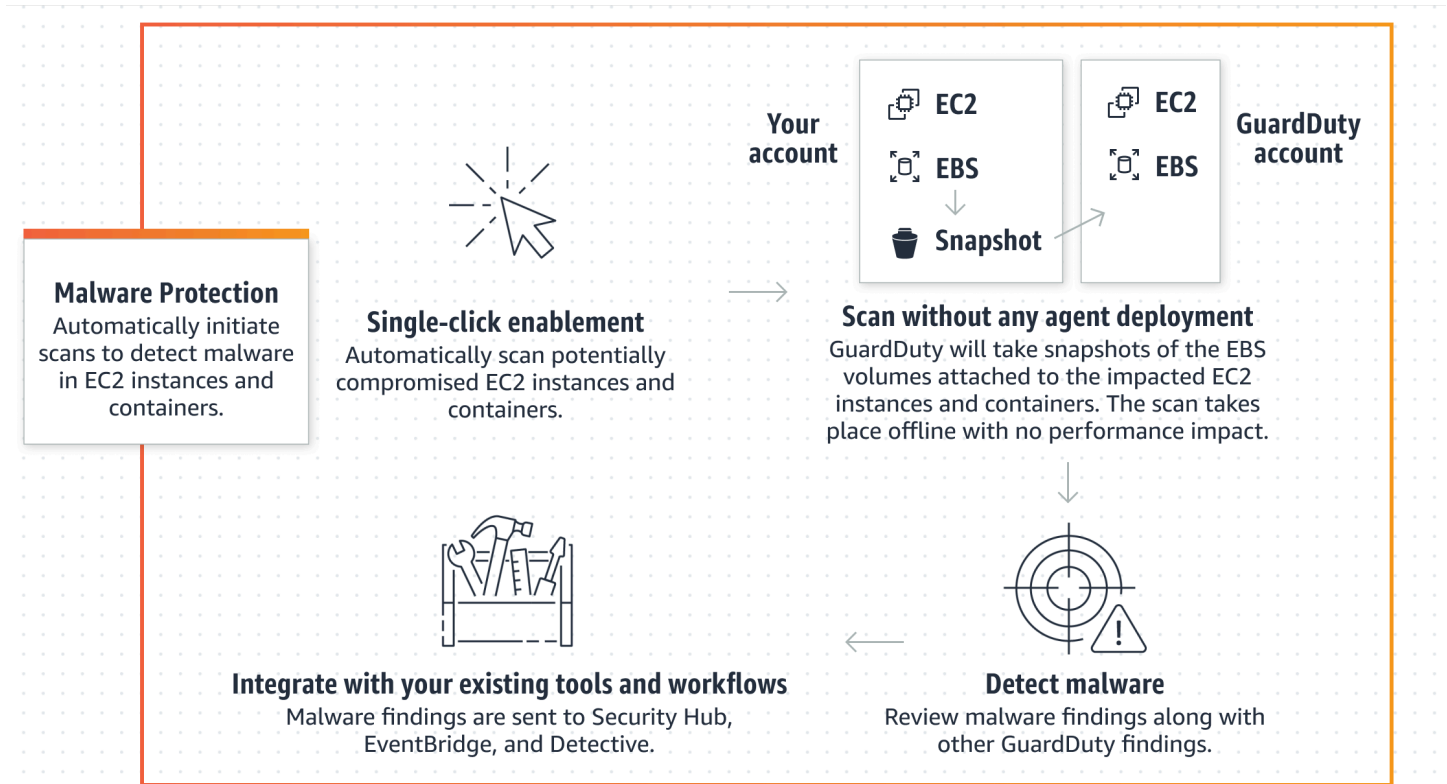
GuardDuty-启动的恶意软件扫描

启用 GuardDuty启动的恶意软件扫描后，每当 GuardDuty 检测到表明您的 Amazon 实例或容器工作负载中可能存在恶意软件的恶意活动并 GuardDuty 生成[调用 GuardDuty启动的恶意软件扫描的发现](#)时，都会 GuardDuty 自动对附加到可能受影响的亚马逊EC2实例或容器工作负载的 Amazon Elastic Block Store (AmazonEBS) 卷上启动无代理扫描，以检测是否存在恶意软件。EC2使用扫描选项，您可以

添加包含标签（与要扫描的资源相关联），也可以添加排除标签（与在扫描过程中要跳过的资源相关联）。自动扫描启动将始终考虑您的扫描选项。您也可以选择开启快照保留设置，以便仅在恶意软件防护EC2检测到存在恶意软件时才保留EBS卷的快照。有关更多信息，请参阅[恶意软件防护中的自定义设置 EC2](#)。

对于 GuardDuty 生成调查结果的每个 Amazon EC2 实例和容器工作负载，每 24 小时就会调用一次自动 GuardDuty 启动的恶意软件扫描。有关如何扫描附加到您的 Amazon EC2 实例或容器工作负载的 Amazon EBS 卷的信息，请参阅[恶意软件防护中的功能 EC2](#)。

下图描述了 GuardDuty 启动的恶意软件扫描的工作原理。



有关 GuardDuty 恶意软件检测方法及其使用的扫描引擎的信息，请参阅[GuardDuty 恶意软件检测扫描引擎](#)。

当发现恶意软件时，GuardDuty 就会生成[适用于 EC2 查找类型的恶意软件防护](#)。如果 GuardDuty 未生成表明同一资源上有恶意软件的发现，则不会调用任何 GuardDuty 启动的恶意软件扫描。您也可以在同一资源上启动按需恶意软件扫描。有关更多信息，请参阅[按需恶意软件扫描](#)。

30 天免费试用

您可以随时选择启用或禁用 AWS 区域 在支持 AWS 账户 中 GuardDuty 启动的恶意软件扫描。如果您有组织，则每个成员帐户都有自己的 30 天免费试用。

要了解 30 天免费试用的工作原理，请考虑以下场景：

- 首次启 GuardDuty 用（新 GuardDuty 帐户）时，GuardDuty 启动的恶意软件扫描也会被启用，并且包含在与该服务相关的 30 天免费试用版中 GuardDuty。
- 现有 GuardDuty 帐户可以首次启用 GuardDuty 启动的恶意软件扫描，并可免费试用 30 天。首次在其他地区启用此功能时，您将在该地区获得 30 天的免费试用。
- 如果您的现有 GuardDuty 帐户在宣布按需恶意软件扫描 EC2 之前一直在使用恶意软件防护，并且该 GuardDuty 帐户已使用其定价模式 AWS 区域，则可以继续使用 GuardDuty 启动的恶意软件扫描。

Note

即使您的免费试用期为 30 天，创建 Amazon EBS 卷快照及其保留期的标准使用费用也适用。有关更多信息，请参阅 [Amazon EBS 定价](#)。

有关启用 GuardDuty 启动的恶意软件扫描的信息，请参阅 [配置 GuardDuty 启动的恶意软件扫描](#)。

配置 GuardDuty 启动的恶意软件扫描

为独立 GuardDuty 账户配置启动的恶意软件扫描

对于与之关联的账户 AWS Organizations，您可以通过控制台设置自动执行此过程，如下一节所述。

启用或禁用 GuardDuty 启动的恶意软件扫描

选择您的首选访问方法，为独立账户配置 GuardDuty 由启动的恶意软件扫描。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格的“保护计划”下，选择“恶意软件防护” EC2。
3. “恶意软件防护 EC2”窗格列出了针对您的帐户 GuardDuty 启动的恶意软件扫描的当前状态。您可以随时通过分别选择启用或禁用，来启用或禁用扫描。
4. 选择保存。

API/CLI

- 使用您自己的区域探测器 ID 运行 [updateDetector](#) API 操作，并在 EbsVolumes 设置为 true 或的情况下传递 dataSources 对象 false。

您还可以运行以下 AWS CLI 命令，使用 AWS 命令行工具启用或禁用 GuardDuty 启动的恶意软件扫描。请务必使用自己的有效证件 *detector ID*。

Note

以下示例代码启用 GuardDuty 启动的恶意软件扫描。要将其禁用，请将 true 替换为 false。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]
```

在多 GuardDuty 账户环境中配置启动的恶意软件扫描

在多账户环境中，只有 GuardDuty 管理员帐户可以配置 GuardDuty 启动的恶意软件扫描。GuardDuty 管理员帐户可以启用或禁用对其成员帐户使用 GuardDuty 启动的恶意软件扫描。管理员帐户为成员帐户配置 GuardDuty 了启动的恶意软件扫描后，该成员帐户将遵循管理员帐户的设置，并且无法通过控制台修改这些设置。GuardDuty 在 AWS Organizations 支持下管理其成员帐户的管理员帐户可以选择在组织中的所有现有和新帐户上自动启用 GuardDuty 启动的恶意软件扫描。有关更多信息，请参阅 [使用管理 GuardDuty 账户 AWS Organizations](#)。

建立可信访问权限以启用 GuardDuty 启动的恶意软件扫描

如果 GuardDuty 委派的管理员帐户与组织中的管理帐户不同，则该管理帐户必须为其组织启用 GuardDuty 启动的恶意软件扫描。这样，委派的管理员账户就可以创建通过其管理的成员账户 AWS Organizations。 [恶意软件防护的服务相关角色权限 EC2](#)

Note

在指定委派 GuardDuty 管理员帐户之前，请参阅 [注意事项和建议](#)。

选择您的首选访问方法，以允许委派的 GuardDuty 管理员帐户对组织中的成员帐户启用 GuardDuty 启动的恶意软件扫描。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

要登录，请使用贵 AWS Organizations 组织的管理帐户。

2. a. 如果您尚未指定委派 GuardDuty 管理员帐户，那么：

在“设置”页面的委派 GuardDuty 管理员帐户下，输入您要指定用于管理组织中 GuardDuty 策略的 12 位数字 **account ID**。选择 Delegate (委派)。

- b. i. 如果您已经指定了与 GuardDuty 管理账户不同的委托管理员账户，那么：

在设置页面的委托管理员下，打开权限设置。此操作将允许委派的 GuardDuty 管理员帐户向成员帐户附加相关权限，并在这些成员帐户中启用 GuardDuty 启动的恶意软件扫描。

- ii. 如果您已经指定了与管理账户相同的委托 GuardDuty 管理员帐户，则可以直接为成员帐户启用 GuardDuty 启动的恶意软件扫描。有关更多信息，请参阅 [为所有成员帐户 GuardDuty 启用自动启动的恶意软件扫描](#)。

Tip

如果委派 GuardDuty 管理员帐户与您的管理帐户不同，则必须向委派 GuardDuty 管理员帐户提供权限，才能允许对成员帐户启用 GuardDuty 启动的恶意软件扫描。

3. 如果您想允许委托 GuardDuty 管理员帐户对其他地区的成员帐户启用 GuardDuty 启动的恶意软件扫描，请更改您的 AWS 区域帐户并重复上述步骤。

API/CLI

1. 使用您的管理帐户凭证运行以下命令：

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (可选) 要对不是委派管理员帐户的管理帐户启用 GuardDuty 启动的恶意软件扫描，管理帐户将首先在其帐户中[恶意软件防护的服务相关角色权限 EC2](#)明确创建恶意软件扫描，然后从委托管理员帐户启用 GuardDuty 启动的恶意软件扫描，类似于任何其他成员帐户。

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. 您已在当前选定的中指定了委派 GuardDuty 管理员帐户 AWS 区域。如果您在一个地区将一个帐户指定为委托 GuardDuty 管理员帐户，则该帐户必须是您在所有其他区域的委托 GuardDuty 管理员帐户。对所有其他区域重复上述步骤。

为委派 GuardDuty 的 GuardDuty 管理员帐户配置启动的恶意软件扫描

选择您的首选访问方法，为委派的 GuardDuty 管理员帐户启用或禁用 GuardDuty 启动的恶意软件扫描。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

确保使用管理帐户凭证。

2. 在导航窗格中，选择“恶意软件防护” EC2。
3. 在“恶意软件防护 EC2”页面上，选择 GuardDuty 启动的恶意软件扫描旁边的编辑。
4. 请执行以下操作之一：

使用对所有帐户启用

- 选择为所有帐户启用。这将为组织中的所有活跃 GuardDuty 帐户（包括加入 AWS 组织的新帐户）启用保护计划。
- 选择保存。

使用手动配置帐户

- 要仅为委派 GuardDuty 管理员帐户启用保护计划，请选择手动配置帐户。
- 在“委派 GuardDuty 管理员帐户（此帐户）”部分下选择“启用”。
- 选择保存。

API/CLI

使用您自己的区域探测器 ID 运行 [updateDetector](#) API 操作，并以 ENABLED 或的 status 形式传递 features 对象 name DISABLED。EBS_MALWARE_PROTECTION

您可以通过运行以下 AWS CLI 命令来启用或禁用 GuardDuty 启动的恶意软件扫描。确保使用有效的委托 GuardDuty 管理员账号 *detector ID*。

Note

以下示例代码启用 GuardDuty 启动的恶意软件扫描。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
--account-ids 555555555555 /
--features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

为所有成员账户 GuardDuty 启用自动启动的恶意软件扫描

选择您的首选访问方式，为所有成员帐户启用 GuardDuty 启动的恶意软件扫描功能。包括现有成员账户和加入组织的新账户。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。


请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

使用“恶意软件防护 EC2”页面

1. 在导航窗格中，选择“恶意软件防护”EC2。
2. 在“恶意软件防护 EC2”页面上，在“GuardDuty 启动的恶意软件扫描”部分中选择“编辑”。


3. 选择为所有账户启用。此操作会自动启用对组织中现有和新帐户 GuardDuty启动的恶意软件扫描。
4. 选择保存。

 Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在“管理自动启用首选项”窗口中，为GuardDuty启动的恶意软件扫描下的所有帐户选择“启用”。
4. 在“恶意软件防护 EC2”页面上，在“GuardDuty启动的恶意软件扫描”部分中选择“编辑”。
5. 选择为所有账户启用。此操作会自动启用对组织中现有和新帐户 GuardDuty启动的恶意软件扫描。
6. 选择保存。

 Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在“管理自动启用首选项”窗口中，为GuardDuty启动的恶意软件扫描下的所有帐户选择“启用”。
4. 选择保存。

如果您无法使用为所有账户启用选项，请参阅 [有选择地启用或禁用对成员 GuardDuty帐户启动的恶意软件扫描](#)。

API/CLI

- 要有选择地为你的成员账户启用或禁用 GuardDuty启动的恶意软件扫描，请使用你自己的账户调用该[updateMemberDetectors](#)API操作 *detector ID*。
- 以下示例显示如何为单个成员帐户 GuardDuty启用启动的恶意软件扫描。要禁用成员账户，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

对所有现有活跃成员账户启用 GuardDuty启动的恶意软件扫描

选择您的首选访问方法，对组织中所有现有活跃成员帐户启用 GuardDuty启动的恶意软件扫描。

为所有现有活跃成员账户配置 GuardDuty启动的恶意软件扫描

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

使用委派的 GuardDuty 管理员账户凭据登录。

2. 在导航窗格中，选择“恶意软件防护” EC2。
3. 在的恶意软件防护中EC2，您可以查看GuardDuty启动的恶意软件扫描配置的当前状态。在活跃成员账户部分下，选择操作。
4. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
5. 选择保存。

为新成员账户 GuardDuty 启用自动启动的恶意软件扫描

在选择配置 GuardDuty 启动的恶意软件扫描 GuardDuty 之前，必须启用新添加的成员帐户。通过邀请管理的成员帐户可以为其帐户手动配置 GuardDuty 启动的恶意软件扫描。有关更多信息，请参阅 [Step 3 - Accept an invitation](#)。

选择您的首选访问方式，对加入组织的新帐户启用 GuardDuty 启动的恶意软件扫描。

Console

委派的 GuardDuty 管理员帐户可以使用“恶意软件防护”或“帐户”页面，对组织中的新成员帐户启用 GuardDuty 启动的 EC2 恶意软件扫描。

自动启用对新成员 GuardDuty 帐户启动的恶意软件扫描

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员帐户证书。

2. 请执行以下操作之一：

- 使用以下 EC2 页面的恶意软件防护：

1. 在导航窗格中，选择“恶意软件防护” EC2。
2. 在“恶意软件防护 EC2”页面上，在 GuardDuty 启动的恶意软件扫描中选择“编辑”。
3. 选择手动配置帐户。
4. 选择为新成员帐户自动启用。此步骤可确保每当有新帐户加入您的组织时，系统都会自动为其帐户启用 GuardDuty 启动的恶意软件扫描。只有组织委派的 GuardDuty 管理员帐户才能修改此配置。
5. 选择保存。

- 使用帐户页面：

1. 在导航窗格中，选择帐户。
2. 在帐户页面上，选择自动启用首选项。
3. 在“管理自动启用首选项”窗口中，在“GuardDuty 启动的恶意软件扫描”下选择“为新帐户启用”。
4. 选择保存。

API/CLI

- 要启用或禁用对新成员帐户 GuardDuty启动的恶意软件扫描，请使用您自己的帐户调用该[UpdateOrganizationConfiguration](#)API操作 *detector ID*。
- 以下示例显示如何为单个成员帐户 GuardDuty启用启动的恶意软件扫描。要将其禁用，请参阅 [有选择地启用或禁用对成员 GuardDuty帐户启动的恶意软件扫描](#)。如果您不想为所有加入组织的新帐户启用该功能，请将 AutoEnable 设置为 NONE。

要查找您的帐户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

您也可以传递用空格IDs分隔的帐户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改帐户的检测器设置时出现任何问题，则会列出该帐户 ID 和问题摘要。

有选择地启用或禁用对成员 GuardDuty帐户启动的恶意软件扫描

选择您的首选访问方法，有选择地为成员帐户配置 GuardDuty由启动的恶意软件扫描。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择帐户。
3. 在“帐户”页面上，查看GuardDuty启动的恶意软件扫描列，了解您的成员帐户的状态。
4. 选择要为其配置 GuardDuty启动的恶意软件扫描的帐户。您可以一次选择多个帐户。
5. 从“编辑保护计划”菜单中，为GuardDuty启动的恶意软件扫描选择相应的选项。

API/CLI

要有选择地为你的成员帐户启用或禁用 GuardDuty启动的恶意软件扫描，请使用你自己的帐户调用该[updateMemberDetectors](#)API操作 *detector ID*。

以下示例显示如何为单个成员帐户 GuardDuty启用启动的恶意软件扫描。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
"Status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

要有选择地为你的成员账户启用或禁用 GuardDuty启动的恶意软件扫描，请使用你自己的账户运行该[updateMemberDetectors](#)API操作 *detector ID*。以下示例显示如何为单个成员帐户 GuardDuty启用启动的恶意软件扫描。要将其禁用，请将 true 替换为 false。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

对通过 GuardDuty邀请管理的组织中的现有账户启用启动的恶意软件扫描

必须在成员账户中创建EC2服务相关角色 (SLR) 的 GuardDuty 恶意软件防护。管理员帐户无法在不由 AWS Organizations管理 GuardDuty的成员帐户中启用启动的恶意软件扫描功能。

目前，您可以通过 GuardDuty 控制台执行以下步骤，为现有成员帐户启用 GuardDuty 启动的恶意软件扫描。<https://console.aws.amazon.com/guardduty/>

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
使用您的管理员帐户凭据登录。
2. 在导航窗格中，选择账户。
3. 选择要为其启用 GuardDuty 启动的恶意软件扫描的成员帐户。您可以一次选择多个账户。
4. 选择操作。
5. 选择取消关联成员。
6. 在您的成员账户中，在导航窗格的保护计划下选择恶意软件防护。
7. 选择启用 GuardDuty 启动的恶意软件扫描。GuardDuty 将 SLR 为成员账户创建一个。有关的信息 SLR，请参阅[恶意软件防护的服务相关角色权限 EC2](#)。
8. 在您的管理员帐户中，选择导航窗格上的帐户。
9. 选择需要重新添加到组织的成员账户。
10. 选择操作，然后选择添加成员。

API/CLI

1. 使用管理员帐户在想要启用 GuardDuty 启动的恶意软件扫描的成员帐户 [DisassociateMembers](#) API 上运行。
2. 使用您的成员帐户调用 [UpdateDetector](#) 以启用 GuardDuty 启动的恶意软件扫描。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. 使用管理员帐户运行 [CreateMembers](#) API 以将成员重新添加到组织。

调用 GuardDuty 启动的恶意软件扫描的发现

当在 GuardDuty Amazon EC2 实例或容器工作负载上 GuardDuty 检测到表明有恶意软件的可疑行为时，就会调用启动的恶意软件扫描。

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#) (仅限出站)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)

- [UnauthorizedAccess:EC2/RDPBruteForce](#) (仅限出站)
- [UnauthorizedAccess:EC2/SSHBruteForce](#) (仅限出站)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

按需恶意软件扫描

按需恶意软件扫描可帮助您检测与您的亚马逊EC2实例关联的 Amazon Elastic Block Store (AmazonEBS) 卷上是否存在恶意软件。无需配置，您就可以通过提供要扫描的亚马逊EC2实例的 Amazon 资源名称 (ARN) 来启动按需恶意软件扫描。您可以通过 GuardDuty 控制台或启动按需恶意软件扫描API。在启动按需恶意软件扫描之前，您可以设置首选 [快照保留](#) 设置。以下场景可以帮助您确定何时使用按需恶意软件扫描类型 GuardDuty：

- 您想在不启用 GuardDuty启动的恶意软件扫描的情况下检测您的 Amazon EC2 实例中是否存在恶意软件。
- 您已启用 GuardDuty启动的恶意软件扫描，并且扫描已自动调用。按照针对EC2查找类型生成的恶意软件保护的[建议补救措施](#)后，如果要对同一资源启动扫描，则可以在距离上次扫描开始时间 1 小时后启动按需恶意软件扫描。

在上次启动恶意软件扫描后，无需等待 24 小时再启动按需恶意软件扫描。应在一小时后对同一资源启动按需恶意软件扫描。要避免在同一EC2实例上重复恶意软件扫描，请参阅[重新扫描同一 Amazon 实例 EC2](#)。

Note

30 天免费试用期内不包括按需恶意软件扫描。GuardDuty使用费用适用于每次恶意软件扫描时扫描的 Amazon 总EBS量。有关更多信息，请参阅 [Amazon GuardDuty 定价](#)。有关创建 Amazon EBS 卷快照的费用及其保留的信息，请参阅 [Amazon EBS 定价](#)。

按需恶意软件扫描工作原理

通过按需恶意软件扫描，即使您的 Amazon EC2 实例正在使用中，您也可以为其启动恶意软件扫描请求。启动按需恶意软件扫描后，GuardDuty 会创建附加到为扫描提供亚马逊资源名称 (ARN) 的亚马逊EC2实例的亚马逊EBS卷的快照。接下来，与 GuardDuty 共享这些快照[GuardDuty 服务账号](#)。GuardDuty 使用 GuardDuty 服务帐户中的这些快照创建加密的副本EBS卷。有关如何扫描 Amazon EBS 卷的更多信息，请参阅[弹性块存储 \(EBS\) 卷](#)。

Note

GuardDuty 创建启动按需恶意软件扫描 point-in-time 时已写入 Amazon EBS 卷的数据的快照。

如果发现恶意软件并且您已启用快照保留设置，则您的EBS卷快照将自动保留在您的中 AWS 账户。按需恶意软件扫描生成 [适用于 EC2 查找类型的恶意软件防护](#)。如果未发现恶意软件，则无论快照保留期设置如何，您的EBS卷快照都会被删除。

默认情况下，您的EBS卷快照是使用GuardDutyScanId标签创建的。请勿删除此标签，因为这样做会GuardDuty阻止访问快照。恶意软件防护中的两种扫描类型都EC2不会扫描GuardDutyExcluded标签设置为的 Amazon EC2 实例或 Amazon EBS 卷true。如果对此类资源EC2使用恶意软件防护进行扫描，则会生成扫描 ID，但会跳过扫描，并说明EXCLUDED_BY_SCAN_SETTINGS原因。有关更多信息，请参阅 [恶意软件扫描期间跳过资源的原因](#)。

AWS Organizations 服务控制策略-拒绝访问

使用中的[服务控制策略 \(SCPs\)](#) AWS Organizations，委派的 GuardDuty 管理员账户可以限制权限并拒绝诸如对账户拥有的 Amazon EC2 实例启动按需恶意软件扫描之类的操作。

作为 GuardDuty 会员账户，当您为 Amazon EC2 实例启动按需恶意软件扫描时，您可能会收到错误消息。您可以与管理账户建立联系，以了解SCP为何为您的成员账户设置了。有关更多信息，请参阅[SCP对权限的影响](#)。

按需恶意软件扫描入门

作为 GuardDuty 管理员帐户，您可以代表账户中设置了以下先决条件的活跃成员账户启动按需恶意软件扫描。独立账户和中的活跃成员账户 GuardDuty 也可以为自己的 Amazon EC2 实例启动按需恶意软件扫描。

先决条件

- GuardDuty 必须在要启动按需恶意软件扫描的 AWS 区域 位置启用。
- 确保[AWS 托管策略 : AmazonGuardDutyFullAccess](#)已附加到IAM用户或IAM角色。您将需要与IAM用户或IAM角色关联的访问密钥和私有密钥。
- 作为委托 GuardDuty 管理员帐户，您可以选择代表活跃的成员帐户启动按需恶意软件扫描。
- 如果您是[没有 Amazon 实例的会员账户](#) [恶意软件防护的服务相关角色权限 EC2](#)，则对属于您账户的 Amazon EC2 实例启动按需恶意软件扫描将自动SLR为其创建恶意软件防护EC2。

Important

当[恶意软件扫描（无论是 GuardDuty启动的还是按需的）仍在进行EC2时，确保没有人删除恶意软件防护的SLR权限](#)。若有人删除，会使扫描无法成功完成并无法提供明确的扫描结果。

在启动按需恶意软件扫描之前，请确保在过去 1 小时内没有对同一资源启动扫描，否则，扫描中的重复数据将被删除。有关更多信息，请参阅 [重新扫描相同的资源](#)。

启动按需恶意软件扫描

选择您启动按需恶意软件扫描的首选访问方法。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
 2. 使用以下选项之一启动扫描：
 - a. 使用以下 EC2 页面的恶意软件防护：
 - i. 在导航窗格的“保护计划”下，选择“恶意软件防护” EC2。
 - ii. 在“恶意软件防护 EC2”页面上，提供您要启动扫描的 Amazon EC2 实例 ARN ¹。
 - b. 使用恶意软件扫描页面：
 - i. 在导航窗格中，选择恶意软件扫描。
 - ii. 选择“开始按需扫描”，然后提供要为其启动扫描的 Amazon EC2 实例 ARN ¹。
 - iii. 如果是重新扫描，请在恶意软件扫描页面上选择一个 Amazon EC2 实例 ID。
- 展开开始按需扫描下拉列表，并选择重新扫描所选实例。
3. 使用任一方法成功启动扫描后，系统将生成扫描 ID。您可以使用此扫描 ID 来跟踪扫描进度。有关更多信息，请参阅 [监控恶意软件扫描状态和结果](#)。

API/CLI

接受您要启动按需恶意软件扫描的 Amazon EC2 实例 ¹ 的调用 [StartMalwareScan](#)。resourceArn

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

成功启动扫描后，StartMalwareScan 会返回 scanId。调用 [DescribeMalwareScans](#) 监控已启动扫描的进度。

¹ 有关您的亚马逊EC2实例格式的信息ARN，请参阅[亚马逊资源名称 \(ARN\)](#)。对于亚马逊EC2实例，您可以使用以下示例ARN格式，替换分区、区域、AWS 账户 ID 和亚马逊EC2实例 ID 的值。有关您的实例 ID 长度的信息，请参阅[资源IDs](#)。

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

重新扫描同一 Amazon 实例 EC2

无论扫描是按需 GuardDuty 启动还是按需扫描，您都可以在上一次恶意软件扫描开始后 1 小时后在同一 EC2 实例上启动新的按需恶意软件扫描。如果在上一次恶意软件扫描启动后 1 小时内，启动了新的恶意软件扫描，则您的请求将导致以下错误，并且系统不会为此请求生成扫描 ID。

```
A scan was initiated on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.
```

有关如何对同一资源启动新扫描的信息，请参阅 [启动按需恶意软件扫描](#)。

要跟踪恶意软件扫描的状态，请参阅 [监控 GuardDuty 恶意软件防护中的扫描状态和结果 EC2](#)。

监控 GuardDuty 恶意软件防护中的扫描状态和结果 EC2

您可以监控每个 GuardDuty 恶意软件防护的扫描状态以进行 EC2 扫描。扫描状态的可能值为 Completed、Running、Skipped 和 Failed。

扫描完成后，将为状态为 Completed 的扫描填充扫描结果。扫描结果的可能值为 Clean 和 Infected。使用扫描类型，您可以识别恶意软件扫描是否为 GuardDuty initiated 或 On demand。

每次恶意软件扫描的扫描结果保留期为 90 天。选择您的首选访问方式来跟踪恶意软件扫描的状态。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择恶意软件扫描。
3. 您可以通过筛选条件中提供的以下属性，来筛选恶意软件扫描。
 - 扫描 ID
 - 账户 ID

- EC2实例 ARN
- 扫描类型
- 扫描状态

有关用于筛选条件的属性的信息，请参阅 [调查发现详细信息](#)。

API/CLI

- 恶意软件扫描得出扫描结果后，您可以根据 EC2_INSTANCE_ARN、SCAN_ID、ACCOUNT_ID、SCAN_TYPE、GUARDDUTY_FINDING_ID、SCAN_START_TIME 和 SCAN_START_TIME，来筛选恶意软件扫描。

GuardDuty 启动时，GUARDDUTY_FINDING_ID筛选条件可用。SCAN_TYPE有关任何筛选条件的信息，请参阅 [调查发现详细信息](#)。

- 你可以改变这个例子 *filter-criteria* 在下面的命令中。目前，您可以一次根据一个 CriterionKey 进行筛选。CriterionKey 的选项为 EC2_INSTANCE_ARN、SCAN_ID、ACCOUNT_ID、SCAN_TYPE、GUARDDUTY_FINDING_ID、SCAN_START_TIME 和 SCAN_START_TIME。

如果您使用CriterionKey如下所示的示例，请确保将示例EqualsValue替换为您自己的有效示例 AWS *scan-id*。

将示例 detector-id 替换为您自己的有效 *detector-id*。你可以改变 *max-results* (最多 50) 和 *sort-criteria*。AttributeName是必填项，必须是scanStartTime。

```
aws guardduty describe-malware-scans --detector-id 60b8777933648562554d637e0e4bb3b2 --max-results 1 --sort-criteria '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

- 此命令的响应最多显示一个结果，其中包含有关受影响资源和恶意软件调查发现的详细信息 (如果 Infected)。

GuardDuty 服务账号由 AWS 区域

创建快照并与 GuardDuty 服务帐号共享时，会在您的 CloudTrail 日志中创建一个新事件。此事件指定了相应的 snapshotId 和 userId（该事件的 GuardDuty 服务帐号 AWS 区域）。有关更多信息，请参阅 [恶意软件防护中的功能 EC2](#)。

以下示例是显示请求正文 CloudTrail 的事件片段：ModifySnapshotAttribute

```
"requestParameters": {
  "snapshotId": "snap-1234567890abcdef0",
  "createVolumePermission": {
    "add": {
      "items": [
        {
          "userId": "111122223333"
        }
      ]
    }
  },
  "attributeType": "CREATE_VOLUME_PERMISSION"
}
```

下表显示了每个地区的 GuardDuty 服务账号。userId 是 GuardDuty 服务帐号，取决于所选区域。

AWS 区域	区域代码	GuardDuty 服务帐号 ID (userId)
美国东部 (弗吉尼亚州北部)	us-east-1	652050842985
美国东部 (俄亥俄州)	us-east-2	17812396868615
美国西部 (加利福尼亚北部)	us-west-1	669213148797
美国西部 (俄勒冈州)	us-west-2	447226417196
亚太地区 (孟买)	ap-south-1	913179291432
亚太地区 (大阪)	ap-northeast-3	089661699081
亚太地区 (首尔)	ap-northeast-2	039163547507

AWS 区域	区域代码	GuardDuty 服务帐号 ID (userId)
Asia Pacific (Tokyo)	ap-northeast-1	874749492622
亚太地区 (新加坡)	ap-southeast-1	247460962669
亚太地区 (悉尼)	ap-southeast-2	124839743349
加拿大 (中部)	ca-central-1	175877067165
加拿大西部 (卡尔加里)	ca-west-1	894794104037
欧洲地区 (法兰克福)	eu-central-1	002294850712
欧洲地区 (爱尔兰)	eu-west-1	283769539786
欧洲地区 (伦敦)	eu-west-2	310125036783
欧洲地区 (巴黎)	eu-west-3	866607715269
欧洲地区 (斯德哥尔摩)	eu-north-1	693780578038
中国 (北京)	cn-north-1	448721096076
中国 (宁夏)	cn-northwest-1	480864352451
南美洲 (圣保罗)	sa-east-1	546914126324
亚太地区 (海得拉巴) (选择加入)	ap-south-2	682251015962
亚太地区 (墨尔本) (选择加入)	ap-southeast-4	353488359550
欧洲 (西班牙) (选择加入)	eu-south-2	936182149045
欧洲 (苏黎世) (选择加入)	eu-central-2	867642063380

AWS 区域	区域代码	GuardDuty 服务帐号 ID (userId)
以色列 (特拉维夫) (选择加入)	il-central-1	619233833001
欧洲地区 (米兰) (选择加入)	eu-south-1	977238331021
亚太地区 (香港) (选择加入)	ap-east-1	249472122084
中东 (巴林) (选择加入)	me-south-1	404001805210
非洲 (开普敦) (选择加入)	af-south-1	9576664736811
亚太地区 (雅加达) (选择加入)	ap-southeast-3	452118225523
中东 (UAE) (选择加入)	me-central-1	828603743433

EC2配额恶意软件防护

的恶意软件防护EC2具有该功能使用的各种资源的默认可用性。

范围	默认	注释
提取和分析压缩或存档文件中的数据	5	可以在存档文件中存在的最大嵌套级别数。
一个存档文件中的文件数	1000	一个存档中可扫描文件的最大数量。此数量是从存档中提取的文件数与从所有嵌套存档中提取的文件数之和。
威胁数量	32	您可以在调查结果面板中查看的最大威胁数量。 GuardDuty

范围	默认	注释
		的恶意软件防护EC2可能已检测到更多威胁名称。如果检测到的威胁名称的数量大于默认值，则可以在 GuardDuty 控制台的JSON详细信息面板中选择查找名称下方的查找 ID 来查看详细信息。
每个已检测威胁的文件数	5	每个检测到的威胁所识别文件的最大数量。例如，如果 GuardDuty 检测到与单个威胁关联的 10 个文件，则该威胁最多会显示 5 个文件。
EBS每个实例的每次扫描量	11	每个EC2实例 GuardDuty 可以扫描的最大EBS卷数。如果需要扫描的EBS卷超过 11 个，则 GuardDuty 恶意软件防护deviceName 按字母顺序对卷进行排EC2序，然后选择前 11 个EBS卷。
EBS 卷大小	2048 GB	与 Amazon EC2 实例和容器工作负载相关联，GuardDuty 恶意软件防护EC2可以扫描每个大小不超过 2048 GB 的 Amazon EBS 卷。此配额适用于支持恶意软件防护的EC2每个 AWS 区域 地方。

范围	默认	注释
受支持的文件系统类型	GuardDuty 恶意软件防护EC2 可以扫描以下文件系统类型： <ul style="list-style-type: none"> 新技术文件系统 (NTFS) X 文件系统 (XFS) 第二代扩展 (ext2) 文件系统 第四代扩展 (ext4) 文件系统 文件分配表 (FAT) 文件系统 虚拟文件分配表 (VFAT) 文件系统 	不适用。
扫描选项标签	50	自定义恶意软件扫描选项设置时，可以添加的最大资源标签数。有关更多信息，请参阅 使用用户定义的标签扫描选项 。
调查发现保留期	90	GuardDuty 保留查找结果的最大天数。有关最新信息，请参阅 亚马逊 GuardDuty 配额 。
恶意软件扫描保留期	90	GuardDuty 恶意软件防护EC2 保留扫描历史记录的最大天数。有关查看最近恶意软件扫描的更多信息，请参阅 监控 GuardDuty 恶意软件防护中的扫描状态和结果 EC2 。
按需恶意软件扫描的每秒事务数 (TPS)	1	每个区域每秒可以发起的按需恶意软件扫描请求的数量。
按需恶意软件扫描的突增限制	1	每个区域每秒可以发起的并发按需恶意软件扫描请求的数量。

GuardDuty S3 恶意软件防护

S3 恶意软件防护通过扫描新上传到所选亚马逊简单存储服务 (Amazon S3) 存储桶中的对象，帮助您检测可能存在的恶意软件。当 S3 对象或现有 S3 对象的新版本上传到您选择的存储桶时，GuardDuty 会自动启动恶意软件扫描。

[S3 恶意软件防护-概述和演示](#)

为 S3 启用恶意软件防护的两种方法

如果您启用了 S3 的恶意软件防护，并且将适用于 S3 的恶意软件防护作为整体 GuardDuty 体验的一部分，或者您想在不启用该 GuardDuty 服务的情况下单独使用适用于 S3 的恶意软件防护功能，则可以启用该 GuardDuty 服务。AWS 账户 当您单独启用 S3 的恶意软件防护时，GuardDuty 文档将其称为使用 S3 的恶意软件防护作为一项独立功能。

单独使用 S3 恶意软件防护的注意事项

- GuardDuty 安全发现 — 探测器 ID 是与您在某个地区中的账户关联的唯一标识符。当您在账户的一个或多个区域 GuardDuty 中启用检测器时，系统会在您启用的每个区域中自动为该账户创建检测器 ID GuardDuty。有关更多信息，请参阅[概念和术语](#)文档中的探测器。

当您在账户中单独启用 S3 的恶意软件防护时，该账户将没有关联的检测器 ID。这会影响您可能使用的 GuardDuty 功能。例如，当 S3 恶意软件扫描检测到恶意软件的存在时，AWS 账户 由于所有 GuardDuty 发现都与检测器 ID 相关联，因此不会在您的系统中生成任何 GuardDuty 发现结果。

- 检查扫描的对象是否为恶意对象-默认情况下，会将恶意软件扫描结果 GuardDuty 发布到您的默认 Amazon EventBridge 事件总线 and Amazon CloudWatch 命名空间。当您在为存储桶启用 S3 恶意软件防护时启用标记时，扫描的 S3 对象将获得一个提及扫描结果的标签。有关标记的更多信息，请参阅[根据扫描结果对对象进行可选标记](#)。

为 S3 启用恶意软件防护的一般注意事项

无论您是单独使用适用于 S3 的恶意软件防护，还是作为 GuardDuty 体验的一部分，以下一般考虑因素都适用：

- 您可以为属于您自己账户的 Amazon S3 存储桶启用 S3 的恶意软件防护。作为委托 GuardDuty 管理员账户，您无法在属于成员账户的 Amazon S3 存储桶中启用此功能。
- 您可以在属于当前在 GuardDuty 控制台选择的同一区域的 S3 存储桶中启用此功能。GuardDuty 不支持在跨区域 S3 存储桶中启用此功能。

- 作为委托 GuardDuty 管理员账户，每当您的组织成员账户为该[恶意软件防护计划资源状态](#)功能配置的 S3 存储桶发生变化时，您都会收到 Amazon EventBridge 通知。

内容

- [S3 恶意软件防护定价](#)
- [S3 恶意软件防护如何运作？](#)
- [S3 恶意软件防护功能](#)
- [\(可选 \) 独立开始使用 S3 GuardDuty 恶意软件防护 \(仅限控制台 \)](#)
- [为您的存储桶配置 S3 的恶意软件防护](#)
- [恶意软件防护计划资源状态](#)
- [恶意软件防护计划故障排除状态详细信息](#)
- [在 S3 的恶意软件防护中进行监控](#)
- [使用基于标签的访问控制 \(TBAC\) 和 S3 的恶意软件防护](#)
- [为受保护存储桶编辑 S3 的恶意软件防护](#)
- [查看 S3 恶意软件防护的使用情况和费用](#)
- [为受保护的存储桶禁用 S3 的恶意软件防护](#)
- [亚马逊 S3 功能的可支持性](#)
- [S3 恶意软件防护配额](#)

S3 恶意软件防护定价

免费套餐计划 (扫描费用)

AWS 账户 每个人都可获得 12 个月的免费套餐，其中包括每个地区每月不超过特定限额的使用量。如果您的使用量超过了指定的限制，则将开始产生超过限制的使用费用。有关指定限制和定价示例的信息，请参阅[GuardDuty 保护计划定价](#)。

- 所有现有用户 AWS 账户 都有资格使用此功能的 12 个月免费套餐，该套餐从 2024 年 6 月 11 日开始，到 2025 年 6 月 11 日结束。此延长的 12 个月免费套餐适用于使用适用于 S3 的恶意软件防护，不适用于其他 AWS 服务 或其他 GuardDuty 功能。

如果现有账户在 2025 年 6 月 11 日之后或账户的 12 个月免费套餐结束后 AWS 账户 开始使用适用于 S3 的恶意软件防护，则您将开始产生相关的使用费用。

- 如果您有新的免费套餐，AWS 账户 并且您的 12 个月免费套餐在 S3 恶意软件防护正式上市（2024 年 6 月 11 日）后开始，则该功能的 12 个月免费套餐期限将与您账户的 12 个月免费套餐期限相同。

有关启用 S3 恶意软件防护后的使用成本的信息，请参阅[查看 S3 恶意软件防护的使用情况和费用](#)。

S3 对象标记使用成本

启用 S3 的恶意软件防护时，可以选择为扫描的 S3 对象启用标记。当您选择启用 S3 对象标记时，会产生相关的使用成本。有关费用的更多信息，请参阅 Amazon S3 定价页面上的“[管理和见解](#)”选项卡。

S3 对象标记使用费用不包含在免费套餐计划中。

亚马逊 S3 APIs-GET 和PUT使用成本

APIs根据IAM角色 GuardDuty 运行 Amazon S3 时，您将产生使用费用。例如，在担任该IAM角色后，GuardDuty 运行PutObjectAPI以将测试对象添加到您选择的存储桶。这有助于 GuardDuty 评估该功能的启用状态。

有关API调用 S3 的定价的信息 AWS 区域，请参阅 Amazon S3 定价页面“[存储和请求](#)”选项卡下的“[请求和数据检索](#)”。

S3 恶意软件防护如何运作？

本节介绍了 S3 恶意软件防护的组件，以及为 S3 存储桶启用恶意软件防护后的工作原理。

概述

您可以为属于自己的 Amazon S3 存储桶启用 S3 的恶意软件防护 AWS 账户。GuardDuty 允许您灵活地为整个存储桶启用此功能，或者将恶意软件扫描的范围限制为特定的[对象前缀](#)，其中 GuardDuty 扫描以选定前缀之一开头的每个上传对象。您最多可以添加 5 个前缀。当您为 S3 存储桶启用该功能时，该存储桶被称为受保护存储桶。

IAM角色权限

S3 恶意软件防护使用 GuardDuty 允许代表您执行恶意软件扫描操作的IAM角色。这些操作包括收到所选存储桶中新上传对象的通知、扫描这些对象以及可选地向扫描的对象添加标签。这是使用此功能配置 S3 存储桶的先决条件。

您可以选择更新现有IAM角色，也可以为此目的创建新角色。当您为多个存储桶启用适用于 S3 的恶意软件防护时，您可以根据需要更新现有IAM角色以包含另一个存储桶名称。有关更多信息，请参阅 [先决条件-创建或更新IAM角色策略](#)。

根据扫描结果对对象进行可选标记

在为您的存储桶启用 S3 的恶意软件防护时，有一个可选步骤可以为已扫描的 S3 对象启用标记。该 IAM 角色已经包含在扫描后向对象添加标签的权限。但是，GuardDuty 只有在设置时启用此选项时，才会添加标签。

在上传对象之前，您必须启用此选项。扫描结束后，使用以下 key: value 对向扫描的 S3 对象 GuardDuty 添加预定义标签：

```
GuardDutyMalwareScanStatus:Potential scan result
```

潜在的扫描结果标签值包

括 NO_THREATS_FOUND、THREATS_FOUND、UNSUPPORTED、ACCESS_DENIED、和 FAILED。有关这些值的更多信息，请参阅 [S3 object potential scan result values](#)。

启用标记是了解 S3 对象扫描结果的方法之一。您可以进一步使用这些标签来添加基于标签的访问控制 (TBAC) S3 资源策略，以便可以对潜在的恶意对象采取操作。有关更多信息，请参阅 [TBAC在 S3 存储桶上添加资源](#)。

我们建议您在为存储桶配置 S3 的恶意软件防护时启用标记。如果您在上传对象后启用标记，并且扫描可能已启动，则 GuardDuty 将无法向扫描的对象添加标签。有关关联的 S3 对象标记成本的信息，请参阅 [S3 恶意软件防护定价](#)。

为存储桶启用 S3 恶意软件防护之后的处理

启用 S3 的恶意软件防护后，将专门为选定的 S3 存储桶创建恶意软件保护计划资源。此资源与恶意软件防护计划 ID 相关联，后者是受保护资源的唯一标识符。使用其中一个 IAM 权限，GuardDuty 然后按名称创建 EventBridge 和管理托管规则 DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*。

如何 GuardDuty 处理您的数据-数据保护的护栏

适用于 S3 的恶意软件防护会监听 Amazon EventBridge 通知。将对象上传到选定的存储桶或其中一个前缀时，使用从 S3 存储桶 GuardDuty 下载该对象，[AWS PrivateLink](#) 然后在同一区域的隔离环境中对其进行读取、解密和扫描。扫描环境在锁定的虚拟私有云 (VPC) 中运行，无法访问互联网。附加到 DNS 防火墙规则组，该规则组仅允许与所拥有的已列入许可名单的域进行通信。VPC AWS 在扫描期

间，将下载的 S3 对象 GuardDuty 临时存储在使用 [AWS Key Management Service \(AWS KMS\)](#) 密钥加密的扫描环境中。

有关 GuardDuty 恶意软件检测方法及其使用的扫描引擎的信息，请参阅[GuardDuty 恶意软件检测扫描引擎](#)。

恶意软件扫描完成后，使用扫描状态 GuardDuty 处理扫描元数据，然后删除已下载的对象副本。

GuardDuty 每次在新的扫描开始之前都会清理扫描环境。GuardDuty 对操作员访问扫描环境使用临时授权，并且每个访问请求都经过审查、批准和审计。

查看 S3 对象扫描结果

GuardDuty 将 S3 对象扫描结果事件发布到 Amazon EventBridge 默认事件总线。GuardDuty 还将扫描指标（例如扫描的对象数量和扫描的字节数）发送给 Amazon CloudWatch。如果您启用了标记，则 GuardDuty 会将预定义的标签 GuardDutyMalwareScanStatus 和潜在的扫描结果添加为标签值。

有关更多信息，请参阅 [在 S3 的恶意软件防护中进行监控](#)。

查看生成的调查结果

查看调查结果取决于您是否使用了 S3 恶意软件防护 GuardDuty。考虑以下场景：

启用 GuardDuty 服务后对 S3 使用恶意软件防护（检测器 ID）

如果恶意软件扫描在 S3 对象中检测到潜在的恶意文件，则 GuardDuty 会生成相关的调查结果。您可以查看发现的详细信息，并使用建议的步骤来修复发现结果。根据您的[导出结果频率](#)，生成的查找结果将导出到 S3 存储桶和 EventBridge 事件总线。

将 S3 的恶意软件防护作为一项独立功能使用（无检测器 ID）

GuardDuty 将无法生成调查结果，因为没有相关的探测器 ID。要了解 S3 对象恶意软件扫描状态，您可以查看 GuardDuty 自动发布到默认事件总线的扫描结果。您还可以查看 CloudWatch 指标以评估 GuardDuty 尝试扫描的对象和字节数。您可以设置 CloudWatch 警报以获得有关扫描结果的通知。如果您启用了 S3 对象标记，还可以通过检查 S3 对象的 GuardDutyMalwareScanStatus 标签键和扫描结果标签值来查看恶意软件扫描状态。

S3 恶意软件防护功能

以下列表概述了在为存储桶启用 S3 恶意软件防护后，您可以期待或执行的操作：

- 选择要扫描的内容-在文件上传到与所选 S3 存储桶关联的所有或特定前缀（最多 5 个）时对其进行扫描。
- 自动扫描上传的对象-为存储桶启用 S3 恶意软件防护后，GuardDuty 将自动开始扫描，以检测新上传的对象中的潜在恶意软件。
- 通过控制台启用，使用API/AWS CLI或 AWS CloudFormation — 选择首选方法为 S3 启用恶意软件防护。

您可以使用 Terraform 等基础设施即代码 (IaC) 平台为 S3 启用恶意软件防护。有关更多信息，请参阅[资源：aws_guarddduty_malware_protection_plan](#)。

- 支持的文件格式、S3 配额的恶意软件防护和 Amazon S3 功能 — S3 恶意软件防护支持您可以上传到 S3 存储桶的所有文件格式。如果上传的文件受密码保护，则 GuardDuty 将跳过对文件的扫描。有关与对象大小、最大存档深度级别相关的配额以及其他详细信息的信息，请参阅[S3 恶意软件防护配额](#)。

有关是否支持 Amazon S3 功能的信息，请参阅[亚马逊 S3 功能的可支持性](#)。

- 支持标记已扫描的 S3 对象-启用后[根据扫描结果对对象进行可选标记](#)，每次恶意软件扫描后，GuardDuty 都会添加一个指示扫描状态的标签。您可以使用此标签为 S3 对象设置基于标签的访问控制 (TBAC)。例如，您可以限制对标记为恶意且标签值为的 S3 对象的访问权限THREATS_FOUND。
- Amazon EventBridge 通知 — EventBridge 当恶意软件保护计划资源状态发生变化或对 S3 对象的恶意软件扫描完成时，向 Amazon GuardDuty 发送事件。这些事件被发送到默认事件总线。您可以使用 EventBridge 和这些事件来编写执行操作的规则，例如监控这些事件何时发生。有关更多信息，请参阅 [使用 Amazon 进行监控 EventBridge](#)。
- CloudWatch 指标-查看 CloudWatch 指标以启用对特定恶意软件扫描状态的警报。有关更多信息，请参阅 [使用 Amazon 监控扫描状态指标 CloudWatch](#)。

(可选) 独立开始使用 S3 GuardDuty 恶意软件防护 (仅限控制台)

如果您想开始使用 S3 威胁检测的恶意软件防护选项，请使用此可选步骤，而不受您的 GuardDuty 状态影响 AWS 账户。如果您已经 GuardDuty 在账户中启用，则可以跳过此步骤并继续[为您的存储桶配置 S3 的恶意软件防护](#)。

开始使用仅适用于 S3 威胁检测的恶意软件防护的步骤

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guarddduty/](https://console.aws.amazon.com/guarddduty/)。

2. 仅为 S3 选择 GuardDuty 恶意软件防护。这可以帮助您检测您的亚马逊简单存储服务 (Amazon S3) 存储桶中新上传的文件是否可能包含恶意软件。

Try threat detection with GuardDuty

Amazon GuardDuty - all features

Experience threat detection capabilities in your AWS environment.

GuardDuty Malware Protection for S3 only

Detect malicious file upload to your Amazon S3 buckets. You don't need to enable Amazon GuardDuty.

Get started

3. 选择开始。现在，您可以继续执行以下步骤[为您的存储桶配置 S3 的恶意软件防护](#)。

为您的存储桶配置 S3 的恶意软件防护

本节包括为属于您自己账户的 Amazon S3 存储桶添加先决条件和启用 S3 恶意软件防护的步骤。无论您是单独开始使用 S3 恶意软件防护，还是将其作为 GuardDuty 服务的一部分启用，以下各节中的步骤都保持不变。

每次要将此威胁检测添加到 S3 存储桶时，请使用以下步骤。

1. [先决条件-创建或更新IAM角色策略](#)
2. [为您的存储桶启用 S3 的恶意软件防护](#)

先决条件-创建或更新IAM角色策略

要让 S3 恶意软件防护扫描以及（可选）向 S3 对象添加标签，您必须创建并附加一个包含以下所需权限的IAM角色：

- 允许 Amazon EventBridge 操作创建和管理 EventBridge 托管规则，以便 S3 恶意软件防护可以监听您的 S3 对象通知。

有关更多信息，请参阅《[亚马逊 EventBridge 用户指南](#)》中的[亚马逊 EventBridge 托管规则](#)。

- 允许 Amazon S3 和 EventBridge 操作向发送 EventBridge 有关此存储桶中所有事件的通知

有关更多信息，请参阅 [Amazon S3 用户指南 EventBridge中的启用亚马逊](#)。

- 允许 Amazon S3 操作访问上传的 S3 对象GuardDutyMalwareScanStatus，并向扫描的 S3 对象添加预定义标签。使用对象前缀时，请仅在目标前缀上添加s3:prefix条件。这样可以 GuardDuty 防止访问存储桶中的所有 S3 对象。
- 在扫描测试对象并将测试对象放到存储桶之前，允许KMS关键操作访问对象，然后使用支持的 DSSEKMS和加密进行SSE加KMS密。

Note

每次为账户中的存储桶启用 S3 恶意软件防护时，都需要执行此步骤。如果您已有IAM角色，则可以更新其策略以包含其他 S3 存储桶资源的详细信息。该[添加IAM策略权限](#)主题提供了有关如何执行此操作的示例。

使用以下策略创建或更新IAM角色。

策略

- [添加IAM策略权限](#)
- [添加信任关系策略](#)

添加IAM策略权限

您可以选择更新现有IAM角色的内联策略，也可以选择创建新IAM角色。有关步骤的信息，请参阅《IAM用户指南》中的[创建IAM角色或修改角色权限策略](#)。

将以下权限模板添加到您的首选IAM角色。将以下占位符值替换为与您的账户关联的相应值：

- 对于 *amzn-s3-demo-bucket*，替换为您的 Amazon S3 存储桶名称。

要将同一个IAM角色用于多个 S3 存储桶资源，请更新现有策略，如以下示例所示：

```

...
...
"Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"
],
...
...

```

在添加与 S3 存储桶ARN关联的新存储桶之前，请务必添加逗号 (,)。无论您在策略模板Resource中提及 S3 存储桶的任何地方，都要执行此操作。

- 对于 *111122223333*，请替换为您的 AWS 账户 身份证。
- 对于 *us-east-1*，替换为你的 AWS 区域。
- 对于 *APKAEIBAERJR2EXAMPLE*，替换为您的客户托管密钥 ID。如果您的存储桶是使用加密的 AWS KMS key，请将占位符值替换为*，如以下示例所示：

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

IAM角色策略模板

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
    "Effect": "Allow",
    "Action": [
      "events:PutRule",

```

```

        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource": [
        "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
        "StringLike": {
            "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
    "Effect": "Allow",
    "Action": [
        "events:DescribeRule",
        "events:ListTargetsByRule"
    ],
    "Resource": [
        "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ]
},
{
    "Sid": "AllowPostScanTag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:GetObjectVersionTagging"
    ],
    "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket/*"
    ]
},
{
    "Sid": "AllowEnableS3EventBridgeEvents",
    "Effect": "Allow",
    "Action": [

```

```
        "s3:PutBucketNotification",
        "s3:GetBucketNotification"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
},
{
    "Sid": "AllowPutValidationObject",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
    ]
},
{
    "Sid": "AllowCheckBucketOwnership",
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
},
{
    "Sid": "AllowMalwareScan",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
},
{
    "Sid": "AllowDecryptForMalwareScan",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
```

```

        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "s3.us-east-1.amazonaws.com"
        }
    }
}
]
}

```

添加信任关系策略

将以下信任策略附加到您的IAM角色。有关步骤的信息，请参阅[修改角色信任策略](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

为您的存储桶启用 S3 的恶意软件防护

本节提供了有关如何为自己账户中的选定存储桶启用 S3 恶意软件防护的详细步骤。

为存储桶启用 S3 恶意软件防护的步骤

- [输入 S3 存储桶详细信息](#)
- [为扫描的对象启用标记](#)
- [权限](#)
- [\(可选 \) 标记恶意软件防护计划 ID](#)

输入 S3 存储桶详细信息

使用以下步骤提供 Amazon S3 存储桶的详细信息：

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 使用页面右上角的 AWS 区域选择器，选择要为 S3 启用恶意软件防护的区域。
3. 在导航窗格中，选择 S3 的恶意软件防护。
4. 在“受保护的存储桶”部分中，选择“启用”，为属于您自己 AWS 账户的 S3 存储桶启用 S3 的恶意软件防护。
5. 在输入 S3 存储桶详细信息下，输入 Amazon S3 存储桶名称。或者，选择“浏览 S3”以选择 S3 存储桶。

S3 存储桶和为 S3 启用恶意软件防护的 AWS 账户位置必须相同。AWS 区域例如，如果您的账户属于该 us-east-1 区域，则您的 Amazon S3 存储桶区域也必须属于该区域 us-east-1。

6. 在“前缀”下，您可以选择 S3 存储桶中的所有对象或以特定前缀开头的对象。
 - 如果您想 GuardDuty 扫描选定存储桶中所有新上传的对象，请选择 S3 存储桶中的所有对象。
 - 如果要扫描新上传的属于特定前缀的对象，请选择以特定前缀开头的对象。此选项可帮助您将恶意软件扫描的范围仅集中在选定的对象前缀上。有关使用前缀的更多信息，请参阅 Amazon S3 用户指南中的使用文件夹在 Amazon S3 [控制台中组织对象](#)。

选择添加前缀并输入前缀。您最多可以添加五个前缀。

为扫描的对象启用标记

此为可选步骤。当您在对象上传到存储桶之前启用标记选项时，在完成扫描后，GuardDuty 将添加一个预定义的标签，键为 GuardDutyMalwareScanStatus，值为扫描结果。要以最佳方式使用 S3 的恶意软件防护，我们建议启用扫描结束后向 S3 对象添加标签的选项。适用标准 S3 对象标签费用。有关更多信息，请参阅 [S3 恶意软件防护定价](#)。

为什么要启用标记？

- 启用标记是了解恶意软件扫描结果的方法之一。有关 S3 恶意软件扫描结果的信息，请参阅 [在 S3 的恶意软件防护中进行监控](#)。
- 在包含潜在恶意对象的 S3 存储桶上设置基于标签的访问控制 (TBAC) 策略。有关注意事项以及如何实现基于标签的访问控制 (TBAC) 的信息，请参阅 [使用基于标签的访问控制 \(TBAC\) 和 S3 的恶意软件防护](#)。

GuardDuty 向 S3 对象添加标签的注意事项：

- 默认情况下，您最多可以将 10 个标签与一个对象关联。有关更多信息，请参阅 Amazon S3 用户指南中的[使用标签对存储进行分类](#)。

如果所有 10 个标签都已在使用中，则 GuardDuty 无法将预定义的标签添加到扫描的对象。

GuardDuty 还会将扫描结果发布到您的默认 EventBridge 事件总线。有关更多信息，请参阅[使用 Amazon 进行监控 EventBridge](#)。

- 当所选 IAM 角色不包括标记 S3 对象的权限时，即使为受保护的存储桶启用了标记，GuardDuty 也无法向扫描的 S3 对象添加标签。GuardDuty 有关标记所需的 IAM 角色权限的更多信息，请参阅[先决条件-创建或更新 IAM 角色策略](#)。

GuardDuty 还会将扫描结果发布到您的默认 EventBridge 事件总线。有关更多信息，请参阅[使用 Amazon 进行监控 EventBridge](#)。

在“标记已扫描对象”下选择一个选项

- 如果 GuardDuty 要为扫描的 S3 对象添加标签，请选择标记对象。
- 如果您不 GuardDuty 想为扫描的 S3 对象添加标签，请选择不标记对象。

权限

使用以下步骤选择具有代表您执行恶意软件扫描操作所需权限的 IAM 角色。这些操作可能包括扫描新上传的 S3 对象以及（可选）向这些对象添加标签。

选择 IAM 角色名称

- 如果您已经执行了以下步骤[先决条件-创建或更新 IAM 角色策略](#)，请执行以下操作：
 - 在“权限”部分下，为 IAM 角色名称选择包含必要权限的 IAM 角色名称。
- 如果您尚未执行以下步骤[先决条件-创建或更新 IAM 角色策略](#)，请执行以下操作：
 - 选择“查看权限”。
 - 在“权限详细信息”下，选择“策略”选项卡。这显示了所需 IAM 权限的模板。

复制此模板，然后在“权限详细信息”窗口末尾选择“关闭”。

- 选择附加策略，在新选项卡中打开 IAM 控制台。您可以选择使用复制的模板中的权限创建新 IAM 角色或更新现有角色。

此模板包含占位符值，您必须将这些值替换为与您的存储桶关联的相应值和 AWS 账户。

- d. 使用 GuardDuty 控制台返回浏览器选项卡。再次选择“查看权限”。
- e. 在“权限详细信息”下，选择“信任关系”选项卡。这显示了您的IAM角色的信任关系策略模板。

复制此模板，然后在“权限详细信息”窗口末尾选择“关闭”。

- f. 转到打开IAM控制台的浏览器选项卡。将此信任关系策略添加到您的首选IAM角色中。
3. 要向为此受保护资源创建的恶意软件防护计划 ID 添加标签，请继续下一节；否则，请选择此页面末尾的启用，将 S3 存储桶添加为受保护资源。

(可选) 标记恶意软件防护计划 ID

这是一个可选步骤，可帮助您向将为您的 S3 存储桶资源创建的恶意软件防护计划资源添加标签。

每个标签分为两部分：标签键和可选标签值。有关标记及其优势的更多信息，请参阅为资源[添加标签](#)。
[AWS](#)

向您的恶意软件防护计划资源添加标签

1. 输入标签的密钥和可选值。标签键和标签值均区分大小写。有关标签键名称和标签值的信息，请参阅[标签命名限制和要求](#)。
2. 要向您的恶意软件防护计划资源添加更多标签，请选择添加新标签并重复上一步操作。您最多可以为每个资源添加 50 个标签。
3. 请选择 启用。

启用 S3 恶意软件防护后的步骤

为存储桶 (或特定对象前缀) 启用 S3 恶意软件防护后，请按所列顺序执行以下步骤：

1. 添加基于标签的访问控制 (TBAC) 资源策略 — 启用标记时，在将对象上传到所选存储桶之前，请确保将该TBAC策略添加到 S3 存储桶资源。有关更多信息，请参阅 [TBAC在 S3 存储桶上添加资源](#)。
2. 监控恶意软件防护计划状态-监控每个受保护存储桶的状态列。有关潜在状态及其含义的信息，请参阅[恶意软件防护计划资源状态](#)。
3. 上传对象：
 1. 打开 Amazon S3 控制台，网址为<https://console.aws.amazon.com/s3/>。

2. 将文件上传到启用此功能的 S3 存储桶或对象前缀。有关上传文件的步骤，请参阅 Amazon S3 用户指南中的[将对象上传到您的存储桶](#)。
4. 监控 S3 对象扫描状态-此步骤包括有关如何检查 S3 对象的恶意软件扫描状态的信息。

已启用 S3 GuardDuty 和恶意软件防护	仅为 S3 启用恶意软件防护
<ul style="list-style-type: none"> • 启用后，它可能会生成，适用于 S3 查找类型的恶意软件防护以表明扫描的 S3 对象中存在恶意软件。GuardDuty • 您可以使用下面的一个或多个选项来检查 S3 对象扫描结果在S3 的恶意软件防护中进行监控。其中包括使用 Amazon EventBridge、恶意软件防护计划的 CloudWatch 指标以及标记扫描的对象。 	<p>您可以使用下面的一个或多个选项来检查 S3 对象扫描结果在S3 的恶意软件防护中进行监控。其中包括使用 Amazon EventBridge、恶意软件防护计划的 CloudWatch 指标以及标记扫描的对象。</p>

恶意软件防护计划资源状态

本节介绍与您的恶意软件防护计划资源相关的各种保护状态值。

Status	描述
Active	您的 S3 存储桶已成功配置了 S3 恶意软件防护。
警告 [*]	S3 的恶意软件防护旨在在出现警告时不会受到影响。当 GuardDuty 注意到新的 S3 对象时，它将启动恶意软件扫描。成功启动扫描后，“状态”列的值可能需要几分钟才能更改为“活动”。在“状态”列值更新后，您将收到 EventBridge 通知。
错误 [*]	您的存储桶未受到保护。与此 S3 存储桶关联的所有恶意软件扫描都不会完成。可能有一个或多个潜在的根本原因。

^{*} 有关潜在问题以及解决这些问题的相应步骤的信息，请参阅[恶意软件防护计划故障排除状态详细信息](#)。

恶意软件防护计划故障排除状态详细信息

对于任何受保护的存储桶，都会根据排名 GuardDuty 显示状态。例如，如果受保护的存储桶在“错误”和“警告”类别下都存在问题，则 GuardDuty 将首先显示与错误状态相关的问题。

以下列表包括错误和恶意软件防护计划状态警告。

错误

- [EventBridge 此 S3 存储桶的通知已禁用](#)
- [EventBridge 缺少用于接收 S3 存储桶事件的托管规则](#)
- [S3 存储桶已不存在](#)

警告

[无法放置测试对象](#)

EventBridge 此 S3 存储桶的通知已禁用

关联的状态原因代码是EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED。

状态详情

GuardDuty 用于 EventBridge 在将新对象上传到此 S3 存储桶时收到通知。您的IAM角色中缺少此权限。

疑难解答步骤

选项 1：向您的IAM角色添加以下权限声明：

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}
```

Replace (替换) *amzn-s3-demo-bucket* 使用您的 Amazon S3 存储桶名称。

选项 2：使用 Amazon S3 控制台启用 EventBridge 通知

1. 打开 Amazon S3 控制台，网址为<https://console.aws.amazon.com/s3/>。
2. 在 Buckets 页面的通用存储桶选项卡下，选择与此错误关联的存储桶名称。
3. 在此存储桶页面上，选择属性选项卡。
4. 在“亚马逊 EventBridge”部分下，选择“编辑”。
5. 在“编辑亚马逊 EventBridge”页面上，在“向亚马逊 EventBridge 发送此存储桶中所有事件的通知”中，选择“开”。
6. 选择 Save changes (保存更改)。

“状态”列的值可能需要几分钟才能更改为“活动”。

EventBridge 缺少用于接收 S3 存储桶事件的托管规则

关联的状态原因代码是EVENTBRIDGE_MANAGED_RULE_DISABLED。

状态详情

缺少 EventBridge 管理规则设置的托管 EventBridge 规则权限。

疑难解答步骤

向您的IAM角色添加以下权限声明：

```
{
  "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
  "Effect": "Allow",
  "Action": [
    "events:PutRule",
    "events>DeleteRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource": [
    "arn:aws:events::*:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
  ],
  "Condition": {
```

```
    "StringEquals": {
      "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
    }
  }
}
```

“状态”列的值可能需要几分钟才能更改为“活动”。

S3 存储桶已不存在

关联的状态原因代码是PROTECTED_RESOURCE_DELETED。

状态详情

此 S3 存储桶已从您的账户中删除，已不复存在。

疑难解答步骤

如果删除 S3 存储桶不是故意的，则可以使用 Amazon S3 控制台创建新的存储桶。

成功创建存储桶后，按照[为您的存储桶配置 S3 的恶意软件防护](#)页面下方的步骤启用 S3 的恶意软件防护。

无法放置测试对象

关联的状态原因代码是INSUFFICIENT_TEST_OBJECT_PERMISSIONS。

Note

添加测试对象的权限是可选的。您的IAM角色中缺少此权限并不能阻止 S3 的恶意软件防护对新上传的对象启动恶意软件扫描。成功启动扫描后，恶意软件防护计划的状态可能需要几分钟才能从“警告”更改为“活动”。

如果IAM角色已经包含此权限，则此警告表示存在限制性的 Amazon S3 存储桶策略，不允许该IAM角色包含此权限。

状态详情

要验证所选存储桶的设置，请在存储桶中 GuardDuty 放置一个测试对象。

疑难解答步骤

您可以选择更新IAM角色以包含缺少的权限。为所选IAM角色添加以下权限，以便 GuardDuty可以将测试对象置于所选资源：

```
{
    "Sid": "AllowPutValidationObject",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
    ]
}
```

Replace（替换）`amzn-s3-demo-bucket` 使用您的 Amazon S3 存储桶名称。有关IAM角色权限的信息，请参阅[先决条件-创建或更新IAM角色策略](#)。

“状态”列的值可能需要几分钟才能更改为“活动”。

在 S3 的恶意软件防护中进行监控

使用带有 GuardDuty 检测器 ID 的 S3 恶意软件防护时，如果您的 Amazon S3 对象可能是恶意的，则 GuardDuty 会生成[适用于 S3 查找类型的恶意软件防护](#)。使用 GuardDuty 控制台和APIs，您可以查看生成的调查结果。有关了解此发现类型的信息，请参见[调查发现详细信息](#)。

在未启用 GuardDuty（无检测器 ID）的情况下对 S3 使用恶意软件防护时，即使扫描的 Amazon S3 对象可能是恶意的，也 GuardDuty 无法生成任何发现。

以下列表提供了可能的 S3 对象扫描结果状态值：

- NO_THREATS_FOUND— 未 GuardDuty 检测到与扫描对象相关的潜在威胁。
- THREATS_FOUND— GuardDuty 检测到与扫描对象相关的潜在威胁。
- UNSUPPORTED— S3 恶意软件防护会跳过扫描的原因有几个。潜在原因包括受密码保护的文件、S3 配额的恶意软件防护以及某些 Amazon S3 功能。有关更多信息，请参阅[S3 恶意软件防护功能](#)。
- ACCESS_DENIED— GuardDuty 无法访问此对象进行扫描。检查与此存储桶关联的IAM角色权限。有关更多信息，请参阅[先决条件-创建或更新IAM角色策略](#)。

- FAILED— 由于内部错误，GuardDuty 无法对此对象执行恶意软件扫描。

以下列表提供了潜在的 S3 对象扫描状态值及其与 S3 对象扫描结果的映射：

- 已完成-扫描成功完成并指示 S3 对象是否有恶意软件。在这种情况下，潜在的 S3 对象扫描结果值可以是THREATS_FOUND或NO_THREATS_FOUND。
- 已跳过 — GuardDuty 当 S3 对象的详细信息与选定存储桶中上传的 S3 对象不一致或 GuardDuty 无法访问已上传的 S3 对象时，会跳过恶意软件扫描。[S3 恶意软件防护配额](#)

在这种情况下，潜在的 S3 对象扫描结果值可以是UNSUPPORTED或ACCESS_DENIED。

- 失败 — 与 S3 对象扫描结果值类似FAILED，此扫描状态表示 GuardDuty 由于内部错误而无法对 S3 对象执行恶意软件扫描。

主题

- [使用 Amazon 进行监控 EventBridge](#)
- [使用 Amazon 监控扫描状态指标 CloudWatch](#)
- [使用 S3 对象标签进行监控](#)

使用 Amazon 进行监控 EventBridge

Amazon EventBridge 是一项无服务器事件总线服务，可以轻松地将您的应用程序与来自各种来源的数据连接起来。EventBridge 提供来自您自己的应用程序、Software-as-a-Service (SaaS) 应用程序和 AWS 服务的实时数据流，并将这些数据路由到 Lambda 等目标。这使您能够监控服务中发生的事件，并构建事件驱动的架构。有关更多信息，请参阅 [Amazon EventBridge 用户指南](#)。

作为受 S3 恶意软件防护保护的 S3 存储桶的所有者账户，在以下情况下向默认事件总线 GuardDuty 发布 EventBridge 通知：

- 您的任何受@@ 保护存储桶的恶意软件防护计划资源状态会发生变化。有关各种状态的信息，请参见[恶意软件防护计划资源状态](#)。
- 由于以下原因，标签事件失败：
 - 您的IAM角色缺少标记对象的权限。

该[添加IAM策略权限](#)模板包括为对象 GuardDuty 添加标签的权限。

- IAM角色中指定的存储桶资源或对象已不存在。

- 关联的 S3 对象已达到最大标签限制。有关标签限制的更多信息，请参阅 Amazon S3 用户指南中的[使用标签对存储进行分类](#)。
- S3 对象扫描结果将发布到您的默认 EventBridge 事件总线。

设置 EventBridge 规则

您可以在账户中设置 EventBridge 规则，将资源状态、扫描后标签失败事件或 S3 对象扫描结果发送给其他 AWS 服务人。作为委托 GuardDuty 管理员帐户，当恶意软件防护计划资源状态发生变化时，您将收到恶意软件防护计划资源状态通知。

将适用标准 EventBridge 定价。有关更多信息，请参阅[Amazon EventBridge 定价](#)。

显示在中的所有值 *red* 是该示例的占位符。这些值将根据您账户中的值以及是否检测到恶意软件而变化。

恶意软件防护计划资源状态

您可以根据以下场景创建 EventBridge 事件模式：

潜在 **detail-type** 值

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

事件模式

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guardduty"]
}
```

以下 @@ 示例通知架构 **GuardDuty Malware Protection Resource Status Active**：

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status Active",
  "source": "aws.guardduty",
}
```

```

"account": "111122223333",
"time": "2017-12-22T18:43:48Z",
"region": "us-east-1",
"resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
"detail": {
  "schemaVersion": "1.0",
  "eventTime": "2024-02-28T01:01:01Z",
  "s3BucketDetails": {
    "bucketName": "amzn-s3-demo-bucket"
  },
  "resourceStatus": "ACTIVE"
}
}

```

以下@@ 示例通知架构 **GuardDuty Malware Protection Resource Status Warning** :

```

{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status warning",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "WARNING",
    "statusReasons": [
      {
        "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
      }
    ]
  }
}

```

以下@@ 示例通知架构 **GuardDuty Malware Protection Resource Status Error** :


```
{
  "version": "0",
  "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
  "detail-type": "GuardDuty Malware Protection Resource Status Error",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ERROR",
    "statusReasons": [
      {
        "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
      }
    ]
  }
}
```

根据背后的原因 `resourceStatusERROR`，将填充该 `statusReasons` 值。

有关以下警告和错误的疑难解答步骤的信息，请参阅[恶意软件防护计划故障排除状态详细信息](#)。

S3 对象扫描结果

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

以下 @@ 示例通知架构 `NO_THREATS_FOUND`：

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
```

```

"source": "aws.guardduty",
"account": "111122223333",
"time": "2024-02-28T01:01:01Z",
"region": "us-east-1",
"resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "COMPLETED",
  "resourceType": "S3_OBJECT",
  "s3objectDetails": {
    "bucketName": "amzn-s3-demo-bucket",
    "objectKey": "APKAEIBAERJR2EXAMPLE",
    "eTag": "ASIAI44QH8DHBEXAMPLE",
    "versionId": "d41d8cd98f00b204e9800998eEXAMPLE"
  },
  "scanResultDetails": {
    "scanResultStatus": "NO_THREATS_FOUND",
    "threats": null
  }
}
}

```

以下@@ 示例通知架构 **THREATS_FOUND** :

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",

```

```

        "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
        "scanResultStatus": "THREATS_FOUND",
        "threats": [
            {
                "name": "EICAR-Test-File (not a virus)"
            }
        ]
    }
}
}

```

扫描结果状态的示例通知架构**UNSUPPORTED** (已跳过) :

```

{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3objectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null
        }
    }
}
}

```

扫描结果状态的示例通知架构**ACCESS_DENIED** (已跳过) :

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "ACCESS_DENIED",
      "threats": null
    }
  }
}
```

扫描结果状态的示例通知架构 **FAILED** :

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "FAILED",
    "resourceType": "S3_OBJECT",
```

```

    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "FAILED",
      "threats": null
    }
  }
}

```

扫描后标签失败事件

事件模式：

```

{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty"
}

```

以下@@@ 示例通知架构 **ACCESS_DENIED**：

```

{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
  },
}

```

```

    "postScanActions": [{
      "actionType": "TAGGING",
      "status": "FAILED",
      "failureReason": "ACCESS_DENIED"
    }]
  }
}

```

以下@@ 示例通知架构 **MAX_TAG_LIMIT_EXCEEDED** :

```

{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "postScanActions": [{
      "actionType": "TAGGING",
      "status": "FAILED",
      "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
    }]
  }
}

```

要对这些失败原因进行故障排除，请参阅[排除 S3 对象扫描后标签故障](#)。

使用 Amazon 监控扫描状态指标 CloudWatch

您可以使用 GuardDuty 进行监控 CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保留 15 个月，因此您可以访问历史信息并更好地了解 S3 恶意软件防护的表

现。还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。

S3 恶意软件防护 CloudWatch 指标可在资源级别获得。您可以分别查询每个受保护资源的这些指标。指标在AWS/GuardDuty/MalwareProtection命名空间中报告。您可以对特定资源设置警报，以监控安全状况。

恶意软件扫描状态指标

指标	描述
CompletedScanCount	<p>在给定时间范围内完成的 S3 对象恶意软件扫描次数。</p> <p>有效尺寸：</p> <ul style="list-style-type: none"> Malware Protection Plan Id Resource Name <p>单位：计数</p>
FailedScanCount	<p>在给定时间范围内失败的 S3 对象恶意软件扫描次数。</p> <p>有效尺寸：</p> <ul style="list-style-type: none"> Malware Protection Plan Id Resource Name <p>单位：计数</p>
SkippedScanCount	<p>在给定时间范围内跳过的 S3 对象恶意软件扫描次数。</p> <p>有效尺寸：</p> <ul style="list-style-type: none"> Malware Protection Plan Id

Resource Name

Skipped Reason

潜在值

- UnSupported
- MissingPermissions

单位：计数

恶意软件扫描结果指标

InfectedScanCount

在给定时间范围内检测到潜在恶意对象的 S3 对象恶意软件扫描次数。

有效尺寸：

- Malware Protection Plan Id

Resource Name

单位：计数

CompletedScanBytes

在给定时间范围内扫描的 S3 对象字节数。

有效尺寸：

- Malware Protection Plan Id

Resource Name

单位：计数

Note

默认情况下，CloudWatch 指标中的统计数据为AVG。

S3 恶意软件防护指标支持以下维度。

维度	描述
Malware Protection Plan Id	与为您的受保护资源 GuardDuty 创建的恶意软件防护计划资源关联的唯一标识符。
Resource Name	受保护资源的名称。
Skipped Reason	跳过 S3 对象恶意软件扫描的原因。
	潜在值
	<ul style="list-style-type: none"> • UnSupported • MissingPermissions

有关访问和查询这些指标的信息，请参阅[亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 指标](#)。

有关设置警报的信息，请参阅[亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 警报](#)。

使用 S3 对象标签进行监控

使用启用标记选项，GuardDuty 以便在完成恶意软件扫描后向您的 Amazon S3 对象添加标签。

启用标记的注意事项

- GuardDuty 标记您的 S3 对象时会产生相关的使用成本。有关更多信息，请参阅 [S3 恶意软件防护定价](#)。
- 您必须保留与该存储桶关联的首选 IAM 角色所需的标记权限；否则，GuardDuty 无法向扫描的对象添加标签。该 IAM 角色已经包含向扫描的 S3 对象添加标签的权限。有关更多信息，请参阅 [先决条件-创建或更新 IAM 角色策略](#)。
- 默认情况下，您最多可以将 10 个标签与一个 S3 对象关联。有关更多信息，请参阅 [使用基于标签的访问控制 \(\) TBAC](#)。

为 S3 存储桶或特定前缀启用标记后，任何新上传的扫描对象都将具有以下键值对格式的关联标签：

GuardDutyMalwareScanStatus:*Scan-Status*

有关潜在标签值的信息，请参见[使用基于标签的访问控制 \(\) TBAC](#)。

排除 S3 恶意软件防护中的 S3 对象扫描后标签故障

仅当您在受保护的存储桶[为扫描的对象启用标记](#)中时，本部分才适用于您。

GuardDuty 尝试向扫描的 S3 对象添加标签时，标记操作可能会导致失败。您的存储桶可能发生这种情况的潜在原因是ACCESS_DENIED和MAX_TAG_LIMIT_EXCEEDED。使用以下主题来了解这些扫描后标签失败原因的潜在原因并对其进行故障排除。

ACCESS_DENIED

以下列表提供了可能导致此问题的潜在原因：

- 用于此受保护的 S3 存储桶的IAM角色缺少AllowPostScanTag权限。验证关联IAM角色是否使用此存储桶策略。有关更多信息，请参阅[先决条件-创建或更新IAM角色策略](#)。
- 受保护的 S3 存储桶策略不允许 GuardDuty 向此对象添加标签。
- 扫描的 S3 对象已不存在。

MAX_TAG_LIMIT_EXCEEDED

默认情况下，您最多可以将 10 个标签与一个 S3 对象关联。有关更多信息，请参阅下的“GuardDuty 向 S3 对象添加标签的注意事项”[为扫描的对象启用标记](#)。

使用基于标签的访问控制 (TBAC) 和 S3 的恶意软件防护

为存储桶启用 S3 的恶意软件防护时，您可以选择启用标记。尝试扫描选定存储桶中新上传的 S3 对象后，向扫描的对象 GuardDuty 添加标签以提供恶意软件扫描状态。启用标记时会产生直接使用成本。有关更多信息，请参阅[S3 恶意软件防护定价](#)。

GuardDuty 使用预定义的标签，密钥为GuardDutyMalwareScanStatus，值作为恶意软件扫描状态之一。有关这些值的信息，请参见[S3 object potential scan result values](#)。

GuardDuty 向 S3 对象添加标签的注意事项：

- 默认情况下，您最多可以将 10 个标签与一个对象关联。有关更多信息，请参阅 Amazon S3 用户指南中的[使用标签对存储进行分类](#)。

如果所有 10 个标签都已在使用中，则 GuardDuty 无法将预定义的标签添加到扫描的对象。

GuardDuty 还会将扫描结果发布到您的默认 EventBridge 事件总线。有关更多信息，请参阅[使用 Amazon 进行监控 EventBridge](#)。

- 当所选IAM角色不包括标记 S3 对象的权限时，即使为受保护的存储桶启用了标记，GuardDuty 也无法向扫描的 S3 对象添加标签。GuardDuty 有关标记所需的IAM角色权限的更多信息，请参阅[先决条件-创建或更新IAM角色策略](#)。

GuardDuty 还会将扫描结果发布到您的默认 EventBridge 事件总线。有关更多信息，请参阅[使用 Amazon 进行监控 EventBridge](#)。

TBAC在 S3 存储桶上添加资源

您可以使用 S3 存储桶资源策略来管理 S3 对象的基于标签的访问控制 (TBAC)。您可以向特定用户提供访问和读取 S3 对象的访问权限。如果您的组织是通过使用创建的 AWS Organizations，则必须强制任何人都不能修改由添加的标签 GuardDuty。有关更多信息，请参阅《AWS Organizations 用户指南》中的[禁止修改标签，授权委托人除外](#)。链接主题中使用的示例提到ec2。使用此示例时，请替换 *ec2* 和s3。

以下列表说明了使用以下方法可以做什么TBAC：

- 阻止除 S3 恶意软件防护服务主体之外的所有用户读取尚未使用以下标签键值对标记的 S3 对象：

GuardDutyMalwareScanStatus:*Potential key value*

- 仅允许 GuardDuty 向扫描的 S3 对象添加GuardDutyMalwareScanStatus以值作为扫描结果的标签键。以下策略模板可以允许具有访问权限的特定用户有可能覆盖标签键值对。

S3 存储桶资源策略示例：

Replace (替换) *IAM-role-name* 使用您在存储桶中为 S3 配置恶意软件防护时使用的IAM角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NoReadExceptForClean",
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": [
          "arn:aws:iam::555555555555:root",
          "arn:aws:iam::555555555555:role/IAM-role-name",
          "arn:aws:iam::555555555555:assumed-role/IAM-role-name/GuardDutyMalwareProtection"
        ]
      }
    }
  ]
}
```

```

    },
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
"NO_THREATS_FOUND"
      }
    }
  },
  {
    "Sid": "OnlyGuardDutyCanTag",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:iam::555555555555:root",
        "arn:aws:iam::555555555555:role/IAM-role-name",
        "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
      ]
    },
    "Action": "s3:PutObjectTagging",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  }
]
}

```

有关为 S3 资源添加标签的更多信息，请参阅[标记和访问控制策略](#)。

为受保护存储桶编辑 S3 的恶意软件防护

使用以下步骤编辑受保护 S3 存储桶的现有设置：

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择 S3 恶意软件防护。
3. 在“受保护的存储桶”下，选择要编辑其现有配置的存储桶。
4. 选择编辑。
5. 更新存储桶的现有配置和设置并确认更改。有关每个部分的描述和步骤的信息，请参阅[为您的存储桶启用 S3 的恶意软件防护](#)。

监控此受保护存储桶的“状态”列。如果显示为“警告”或“错误”，请参阅[恶意软件防护计划故障排除状态详细信息](#)。

查看 S3 恶意软件防护的使用情况和费用

当您使用适用于 S3 的恶意软件防护超出免费套餐计划的特定限制或账户的 12 个月免费套餐计划到期时，您的账户就会开始产生使用费用。有关免费套餐计划的信息，请参阅[S3 恶意软件防护定价](#)。

要查看使用成本，请在 <https://console.aws.amazon.com/billing/> 控制台中导航到 Cost Explorer。有关 AWS 账户计费的信息，请参阅《[AWS Billing 用户指南](#)》。

为受保护的存储桶禁用 S3 的恶意软件防护

当您为受保护存储桶禁用 S3 的恶意软件防护时，GuardDuty 会删除与该存储桶关联的恶意软件防护计划 ID。GuardDuty 当新对象上传到此存储桶或其中一个选定的对象前缀时，将不再启动恶意软件扫描。

如果您已启用 GuardDuty 但现在想要暂停或禁用 GuardDuty，请参阅[暂停或禁用 GuardDuty](#)。由于 S3 恶意软件防护中没有探测器 ID 的概念，因此禁用或暂停 GuardDuty 不会影响您账户中受保护存储桶的状态。您可以继续单独使用适用于 S3 的恶意软件防护功能以及相关的标准定价。有关更多信息，请参阅[查看 S3 恶意软件防护的使用情况和费用](#)。要停止使用适用于 S3 的恶意软件防护，您需要为账户中的所有受保护存储桶禁用该功能。如果您想继续使用 GuardDuty 并仅对存储桶禁用 S3 的恶意软件防护，则以下步骤不会影响该 GuardDuty 服务的配置以及您可能已启用的其他保护计划。

为受保护存储桶禁用 S3 的恶意软件防护

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择 S3 的恶意软件防护。

3. 在“受保护的存储桶”下，选择要为其禁用 S3 恶意软件防护的存储桶。

您一次只能选择一个受保护的存储桶。要为多个存储桶禁用 S3 的恶意软件防护，请对另一个 S3 存储桶再次执行以下步骤。

4. 选择 禁用。

5. 选择“禁用”以确认选择。

亚马逊 S3 功能的可支持性

下表说明了 S3 恶意软件防护是否支持列出的 Amazon S3 功能。

支持是否可用？	描述
是	无需异步还原即可检索 S3 对象。

支持是否可用？	描述

支持是否可用？	描述
条件	<ul style="list-style-type: none">• 智能分层支持频繁、不频繁和存档实例访问层中的 S3 对象。• 不支持选择加入的存档和深度存档层。• 智能分层总是在频繁访问层中创建新对象。因此，支持在创建时扫描对象。• 未来的智能分层功能可能会从存档中的对象开始。因此，不支持此功能。
否	GuardDuty 仅支持 S3 恶意软件防护的通用存储桶。

支持是否可用？	描述
否	必须先恢复 S3 对象，然后才能对其进行访问。
否	Outposts 不支持 S3 的恶意软件防护。

支持是否可用？	描述
是	所有上传的 S3 对象都经过恶意软件扫描。如果您上传了文件版本 v1 的对象，并立即上传了另一个版本替换为 v2，则 GuardDuty 将同时扫描目标文件版本 v1 和 v2。但是，扫描开始时间的顺序可能不同。
是	如果目标存储桶是受保护的资源，则 GuardDuty 将扫描所有复制到受保护和监控的前缀的 S3 对象。
否	您无法根据扫描结果标签定义复制规则。Amazon S3 不支持对标签进行复制，但创建时除外。

支持是否可用？	描述
是	GuardDuty 支持对使用托管密钥和客户托管密钥加密的 S3 对象进行恶意软件扫描。确保该IAM角色包含使用密钥的权限。有关更多信息，请参阅 添加IAM策略权限 。

支持是否可用？	描述
否	S3 恶意软件防护不支持扫描使用不可访问的密钥加密的 S3 对象。
否	使用 Amazon S3 加密客户端对您的 S3 对象进行加密时，您的对象不会暴露给任何第三方，包括 AWS。有关不支持此功能的原因的更多信息，请参阅 Amazon S3 用户指南中的 使用客户端加密保护数据 。
是	锁定的 S3 对象的锁定基于 WORM-一次写入多次读取。适用于 S3 的恶意软件防护可以访问和扫描对象。
是	适用于 S3 的恶意软件防护可以扫描使用申请方付款设置的存储桶。请求者将为 S3 通话付费。有关更多信息，请参阅《Amazon S3 用户指南》中的 使用申请方付款存储桶进行存储传输和使用 。

支持是否可用？	描述
是	您可以根据扫描结果标签定义生命周期策略。例如，自动删除恶意对象。有关生命周期配置的更多信息，请参阅 Amazon S3 用户指南中的 管理存储生命周期 。
是	您可以基于 S3 对象扫描结果标签定义存储桶资源策略。例如，阻止访问尚未扫描的 S3 对象或 GuardDuty 检测到的威胁。有关更多信息，请参阅 使用基于标签的访问控制 (TBAC) 和 S3 的恶意软件防护 。

S3 恶意软件防护配额

本节提供默认配额，通常称为限制。除非指定，否则每个配额都是特定于区域的。要查看特定于使用基础（或核心）GuardDuty 服务的默认配额，请参阅[亚马逊 GuardDuty 配额](#)。

下表描述了适用于您的多个配额 AWS 账户。

AWS 默认配额值	它是否可以调节？	描述
5 GB	否	尝试扫描恶意软件的最大 S3 对象大小。 GuardDuty
5 GB	否	GuardDuty 可以从存档文件中提取和分析的最大数据量（以 GB 为单位）。即使存档文件包含的容量超过 5 GB，GuardDuty 也会跳过超过此值的内容。
1000	否	存档文件中 GuardDuty 可以提取和分析的最大文件数。如果文件包含 1,000 个以上的文件，GuardDuty 则必须跳过存档的文件。
5	否	GuardDuty 可以提取的最大嵌套存档级别。如果存档中包含嵌套超出此值的文件，则 GuardDuty 将跳过这些嵌套文件。

AWS 默认配额值	它是否可以调节？	描述
25	否	可以为 S3 启用恶意软件防护的 S3 存储桶的最大数量。此配额限制适用于每个地区的每个账户。
25	在地区层面	每个区域每秒可以启动的最大控制平面操作数。这些API操作包括创建、读取、更新和删除资源。此配额值适用于区域级别。

GuardDuty RDS保护

RDS亚马逊的保护功能 GuardDuty 会分析和分析您的亚马逊 Aurora 数据库（亚马逊 Aurora 我的兼容版和 Aurora Postgre SQL 兼容版）和亚马逊 Postgre 数据库（适用于 PostgreSQL）和亚马逊 RDS 的 PostgreSQL 数据库的潜在访问威胁。RDS SQL 此功能允许您识别潜在的可疑登录行为。RDS 保护不需要额外的基础架构；它的设计不影响数据库实例的性能。

当 P RDS protection 检测到表明您的数据库存在威胁的潜在可疑或异常登录尝试时，GuardDuty 会生成新的调查结果，其中包含有关可能受感染的数据库的详细信息。

您可以随时为任何账户启用或禁用 RDS 保护功能，AWS 区域 只要该功能在 Amazon GuardDuty 中可用。现有 GuardDuty 账户可以启用 30 天试用期的 RDS 保护。对于新 GuardDuty 帐户，RDS 保护已启用并包含在 30 天免费试用期内。有关更多信息，请参阅 [估算成本](#)。

Note

未启用“RDS 保护”功能时，GuardDuty 既不会收集您的 RDS 登录活动，也不会检测到异常或可疑的登录行为。

有关 where AWS 区域 e 尚 GuardDuty 不支持 RDS 保护的信息，请参阅 [特定于区域的功能可用性](#)。

支持的亚马逊 Aurora 和亚马逊 RDS 数据库

下表显示了支持的 Aurora 和 Amazon RDS 数据库版本。

亚马逊 Aurora 和亚马逊 RDS 数据库引擎	支持的引擎版本
Aurora My SQL	<ul style="list-style-type: none"> • 2.10.2 或更高版本 • 3.02.1 或更高版本
Aurora SQL	<ul style="list-style-type: none"> • 10.17 或更高版本 • 11.12 或更高版本 • 12.7 或更高版本 • 13.3 或更高版本 • 14.3 或更高版本

亚马逊 Aurora 和亚马逊RDS数据库引擎	支持的引擎版本
	<ul style="list-style-type: none"> • 15.2 或更高版本 • 16.1 或更高版本
RDS适用于 Postgr SQL	<ul style="list-style-type: none"> • 14.5 或更高版本 • 13.8 或更高版本 • 12.12 或更高版本 • 11.17 或更高版本 • 10.22 或更高版本 • RDS适用于 Postgre SQL 版本 15 • RDS适用于 Postgre SQL 版本 16

Prot RDS ection 如何使用RDS登录活动监控

RDS亚马逊的保护 GuardDuty 可帮助您保护账户中支持的亚马逊 Aurora (Aurora) 和 RDS Postgre SQL 数据库。启用RDS保护功能后，GuardDuty 立即开始监控您账户中来自 Aurora 数据库和 Amazon RDS 的RDS登录活动。GuardDuty 持续监控和分析RDS登录活动中是否存在可疑活动，例如，以前看不见的外部行为者未经授权访问您账户中的 Aurora 数据库。首次启用 P RDS rotection 或者您有新创建的数据库实例时，需要一段学习时间来确定正常行为的基准。因此，新启用或新创建的数据库实例可能在长达两周的时间内，没有关联的异常登录调查发现。有关更多信息，请参阅 [RDS登录活动监控](#)。

当 P RDS rotection 检测到潜在威胁（例如一系列成功、失败或不完整的登录尝试中的异常模式）时，GuardDuty 会生成新的调查结果，其中包含有关可能受损的数据库实例的详细信息。有关更多信息，请参阅 [RDS 保护查找类型](#)。如果您禁用“RDS保护”，则会 GuardDuty 立即停止监控RDS登录活动，并且无法检测到对您支持的数据库实例的任何潜在威胁。

Note

GuardDuty 不会管理您的活动[支持的数据库](#)或RDS登录活动，也不会向您提供RDS登录活动。

RDS保护功能

RDS登录活动监控

RDS登录活动会捕获您的 AWS 环境中成功和失败的[支持的亚马逊 Aurora 和亚马逊RDS数据库](#)登录尝试。为了帮助您保护数据库，Protecti GuardDuty RDS on 会持续监控登录活动，以发现可能存在可疑的登录尝试。例如，攻击者可能通过猜测 Amazon Aurora 数据库的密码，试图暴力破解访问该数据库。

启用RDS保护功能后，GuardDuty 会自动开始直接从 Aurora 和 Amazon RDS 服务监控数据库的RDS登录活动。如果有异常登录行为的迹象，则 GuardDuty 会生成一个调查结果，其中包含有关可能遭到入侵的数据库的详细信息。首次启用 P RDS rotection 或者您有新创建的数据库实例时，需要一段学习时间来确定正常行为的基准。因此，新启用或新创建的数据库实例可能在长达两周的时间内，没有关联的异常登录调查发现。

RDS保护功能不需要任何其他设置；它不会影响您的任何现有 Amazon Aurora 数据库或亚马逊RDS配置。GuardDuty 不会管理您支持的数据库或RDS登录活动，也不会向您提供RDS登录活动。

如果您选择在新成员帐户加入您的组织时自动启用RDS保护功能，则此操作会自动 GuardDuty 为这些新成员帐户启用。有关将RDS登录活动监控配置为一项功能的更多信息，请参阅[GuardDuty RDS保护](#)。

为独立账户配置RDS保护

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择“RDS保护”。
3. “RDS保护”页面显示您账户的当前状态。您可以随时通过选择启用或禁用，来启用或禁用此功能。确认您的选择。

API/CLI

使用您自己的区域探测器 ID 运行[updateDetector](#)API操作，并以ENABLED或的status形式传递features对象nameDISABLED。RDS_LOGIN_EVENTS

您也可以通过运行以下 AWS CLI 命令来启用或禁用RDS保护。请务必使用自己的有效证件 *detector ID*。

Note

以下示例代码启用RDS保护。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectorsAPI](#)。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

在多RDS账户环境中配置保护

在多账户环境中，只有委派的 GuardDuty 管理员账户可以选择为其组织中的成员账户启用或禁用RDS保护功能。GuardDuty成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理其成员账户 AWS Organizations。此委派的 GuardDuty 管理员账户可以选择在所有新账户加入组织时自动启用RDS登录活动监控。有关多账户环境的更多信息，请参阅在 [Amazon 中管理多个账户](#)。GuardDuty

为委派 GuardDuty 管理员账号配置RDS保护

选择您的首选访问方法，为委派的 GuardDuty 管理员帐户配置“RDS登录活动监控”。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

确保使用管理账户凭证。

2. 在导航窗格中，选择“RDS保护”。
3. 在“RDS保护”页面上，选择“编辑”。
4. 请执行以下操作之一：

使用对所有账户启用

- 选择为所有账户启用。这将为组织中的所有活跃 GuardDuty 账户（包括加入 AWS 组织的新账户）启用保护计划。
- 选择保存。

使用手动配置账户

- 要仅为委派 GuardDuty 管理员账户启用保护计划，请选择手动配置帐户。
- 在“委派 GuardDuty 管理员帐户（此帐户）”部分下选择“启用”。
- 选择保存。

API/CLI

使用您自己的区域探测器 ID 运行 [updateDetector](#) API 操作，并以 ENABLED 或的 status 形式传递 features 对象 name DISABLED。RDS_LOGIN_EVENTS

您可以通过运行以下 AWS CLI 命令来启用或禁用 RDS 保护。确保使用有效的委托 GuardDuty 管理员账号 *detector ID*。

Note

以下示例代码启用 RDS 保护。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区 detectorId 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

为所有成员账户自动启用 RDS 保护

选择您的首选访问方式，为所有成员账户启用 RDS 保护功能。包括现有成员账户和加入组织的新账户。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

使用“RDS保护”页面

1. 在导航窗格中，选择“RDS保护”。
2. 选择为所有账户启用。此操作会自动为组织中的现有帐户和新帐户启用RDS保护。
3. 选择保存。

Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在“管理自动启用首选项”窗口中，在“RDS登录活动监控”下选择“为所有帐户启用”。
4. 选择保存。

如果您无法使用为所有账户启用选项，请参阅 [有选择地启用或禁用对成员账户的RDS保护](#)。

API/CLI

- 要有选择地为您的成员账户启用或禁用RDS保护，请使用您自己的账户调用该[updateMemberDetectors](#)API操作 *detector ID*。
- 以下示例显示如何为单个成员账户启用RDS保护。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为所有现有活跃成员账户启用RDS保护

选择您的首选访问方式，为组织中所有现有的活跃成员账户启用RDS保护。

Console

为所有现有活跃成员账户配置RDS保护

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派 GuardDuty 管理员账户凭证登录。

2. 在导航窗格中，选择“RDS保护”。
3. 在“RDS保护”页面上，您可以查看配置的当前状态。在活跃成员账户部分下，选择操作。
4. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
5. 选择确认。

API/CLI

- 要有选择地为您的成员账户启用或禁用RDS保护，请使用您自己的账户调用该 [updateMemberDetectors](#) API 操作 *detector ID*。
- 以下示例显示如何为单个成员账户启用RDS保护。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找与您的账户和当前地区 detectorId 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

Note

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 UnprocessedAccounts 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为新成员账户自动启用RDS保护

选择您的首选访问方式，为加入组织的新账户启用RDS登录活动。

Console

委派的 GuardDuty 管理员账户可以通过控制台使用RDS保护或账户页面为组织中的新成员账户启用。

为新成员账户自动启用RDS保护

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

- 使用“RDS保护”页面：

1. 在导航窗格中，选择“RDS保护”。
2. 在“RDS保护”页面上，选择“编辑”。
3. 选择手动配置账户。
4. 选择为新成员账户自动启用。此步骤可确保每当有新账户加入您的组织时，系统都会自动为其账户启用RDS保护。只有组织委派的 GuardDuty 管理员帐户才能修改此配置。
5. 选择保存。

- 使用账户页面：

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项。
3. 在“管理自动启用首选项”窗口中，在“RDS登录活动监控”下选择“为新帐户启用”。
4. 选择保存。

API/CLI

- 要有选择地为您的成员账户启用或禁用RDS保护，请使用您自己的账户调用该[UpdateOrganizationConfiguration](#)API操作 *detector ID*。
- 以下示例显示如何为单个成员账户启用RDS保护。要将其禁用，请参阅 [有选择地启用或禁用对成员账户的RDS保护](#)。如果您不想为所有加入组织的新账户启用该功能，请将 `autoEnable` 设置为 `NONE`。

要查找与您的账户和当前地区 `detectorId` 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

- 成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

有选择地启用或禁用对成员账户的RDS保护

选择您的首选访问方式，有选择地启用或禁用对成员账户的RDS登录活动监控。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 在导航窗格中，选择账户。

在“帐户”页面上，查看RDS登录活动列，了解您的成员账户的状态。

3. 有选择地启用或禁用RDS登录活动

选择要为其配置RDS保护的帐户。您可以一次选择多个账户。在“编辑保护计划”下拉菜单中，选择“RDS登录活动”，然后选择相应的选项。


API/CLI

要有选择地为您的成员账户启用或禁用RDS保护，请使用您自己的账户调用该[updateMemberDetectors](#)API操作 *detector ID*。

以下示例显示如何为单个成员账户启用RDS保护。要将其禁用，请将 `ENABLED` 替换为 `DISABLED`。

要查找与您的账户和当前地区 `detectorId` 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 `ListDetectors` API。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
"ENABLED"}]'
```

 Note

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

GuardDuty Lambda 保护

当在您的 AWS 环境中调用 [AWS Lambda](#) 函数时，Lambda 保护可以帮助您识别潜在的安全威胁。启用 Lambda 保护后，GuardDuty 开始监控 Lambda 网络活动日志，从账户的[VPC 流日志](#)所有 Lambda 函数开始，包括那些不使用VPC联网的日志，并在调用 Lambda 函数时生成。如果 GuardDuty 发现可疑的网络流量，表明您的 Lambda 函数中存在潜在的恶意代码，则 GuardDuty 会生成调查结果。

Note

Lambda 网络活动监控不包括 [Lambda@Edge 函数](#)的日志。

您可以随时为任何账户或可用 AWS 区域账户配置 Lambda 保护。默认情况下，现有 GuardDuty 账户可以启用 Lambda 保护，试用期为 30 天。对于新 GuardDuty 账户，Lambda 保护已启用并包含在 30 天的试用期内。有关使用情况统计数据的更多信息，请参阅 [估算成本](#)。

GuardDuty 监控通过调用 Lambda 函数生成的网络活动日志。目前，Lambda 网络活动监控包括来自您账户所有 Lambda 函数的 Amazon VPC 流日志，包括那些不使用VPC联网的日志，并且可能会发生变化，包括扩展到其他网络活动，例如通过调用 Lambda 函数生成的DNS查询数据。扩展到其他形式的网络活动监控将增加 Lambda Protection GuardDuty 处理的数据量。这将直接影响 Lambda 保护的使用成本。每当 GuardDuty 开始监控其他网络活动日志时，它都会在发布前至少 30 天向已开启 Lambda Protection 的账户发出通知。

Lambda 保护中的功能

Lambda 网络活动监控

启用 Lambda 保护后，会监控调用与您的账户关联的 Lambda 函数时生成的 Lambda 网络活动日志。这可以帮助您检测 Lambda 函数面临的潜在安全威胁。GuardDuty 监控来自所有 Lambda 函数的VPC流日志，包括那些不使用VPC网络的函数。对于配置为使用VPC网络的 Lambda 函数，您无需为 Lambda 为创建的弹性网络接口 (ENI) 启用VPC流日志。GuardDuty 仅对为生成调查结果而处理的 Lambda 网络活动日志数据量（以 GB 为单位）收费。GuardDuty 通过应用智能筛选器并分析与威胁检测相关的 Lambda 网络活动日志子集来优化成本。有关定价的信息，请参阅 [Amazon GuardDuty 定价](#)。

GuardDuty 不会管理您的 Lambda 网络活动日志（包括VPC和非VPC流日志），也不会让这些日志可以在您的账户中访问。

配置 Lambda 保护

为独立账户配置 Lambda 保护

对于与之关联的账户 AWS Organizations，您可以通过 GuardDuty 控制台或 API 说明自动执行此过程，如下一节所述。

选择您的首选访问方法，为独立账户启用或禁用 Lambda 保护。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中的设置下，选择 Lambda 保护。
3. Lambda 保护页面显示您账户的当前状态。您可以随时通过选择启用或禁用，来启用或禁用此功能。
4. 选择保存。

API/CLI

使用您自己的区域探测器 ID 运行 [updateDetector](#) API 操作，并以 ENABLED 或的 status 形式传递 features 对象 name DISABLED。LAMBDA_NETWORK_LOGS

您还可以通过运行以下 AWS CLI 命令来启用或禁用 Lambda 网络活动监控。请务必使用自己的有效证件 *detector ID*。

Note

以下示例代码可启用 Lambda 网络活动监控。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]
```

在多账户环境中配置 Lambda 保护

在多账户环境中，只有委派的 GuardDuty 管理员账户可以选择为其组织中的成员账户启用或禁用 Lambda Protection。GuardDuty 成员账户无法通过其账户修改此配置。委托 GuardDuty 管理员账户使用管理成员账户 AWS Organizations。委托 GuardDuty 管理员账户可以选择在所有新账户加入组织时自动启用 Lambda 网络活动监控。有关多账户环境的更多信息，请参阅[在 Amazon GuardDuty 中管理多个账户](#)。

为委托 GuardDuty 管理员账户配置 Lambda 保护

选择您的首选访问方法，为委派的 GuardDuty 管理员账户启用或禁用 Lambda 网络活动监控。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

确保使用管理账户凭证。

2. 在导航窗格中的设置下，选择 Lambda 保护。
3. 在 Lambda 保护页面上，选择编辑。
4. 请执行以下操作之一：

使用对所有账户启用

- 选择为所有账户启用。这将为组织中的所有活跃 GuardDuty 账户（包括加入 AWS 组织的新账户）启用保护计划。
- 选择保存。


使用手动配置账户

- 要仅为委派 GuardDuty 管理员账户启用保护计划，请选择手动配置帐户。
- 在“委派 GuardDuty 管理员帐户（此帐户）”部分下选择“启用”。
- 选择保存。

API/CLI

使用您自己的区域探测器 ID 运行[updateDetector](#)API操作，并以ENABLED或的status形式传递features对象nameDISABLED。LAMBDA_NETWORK_LOGS

您可以通过运行以下 AWS CLI 命令来启用或禁用 Lambda 网络活动监控。确保使用有效的委托 GuardDuty 管理员账号 *detector ID*。

 Note

以下示例代码可启用 Lambda 网络活动监控。要将其禁用，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行 `ListDetectors` API。 `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

为所有成员账户自动启用 Lambda 网络活动监控

选择您的首选访问方法，为所有成员账户启用 Lambda 网络活动监控功能。包括现有成员账户和加入组织的新账户。

Console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

使用 Lambda 保护页面

1. 在导航窗格中，选择 Lambda 保护。
2. 选择为所有账户启用。此操作会自动为组织中的现有账户和新账户启用 Lambda 网络活动监控。
3. 选择保存。

Note

更新成员账户的配置可能最长需要 24 小时。

使用账户页面

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项，然后选择通过邀请添加账户。
3. 在管理自动启用首选项窗口中，在 Lambda 网络活动监控下选择为所有账户启用。

Note

默认情况下，此操作会自动打开“GuardDuty 为新成员帐户自动启用”选项。

4. 选择保存。

如果您无法使用为所有账户启用选项，请参阅 [有选择地为成员账户启用或禁用 Lambda 网络活动监控](#)。

API/CLI

- 要有选择地为您的成员账户启用或禁用 Lambda 网络活动监控，请使用您自己的账户调用 [updateMemberDetectors](#) API 该操作 *detector ID*。
- 以下示例显示如何为单个成员账户启用 Lambda 网络活动监控。要禁用成员账户，请将 ENABLED 替换为 DISABLED。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。detectorId

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

您也可以传递用空格IDs分隔的账户列表。

- 成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为所有现有活跃成员账户启用 Lambda 网络活动监控

选择您的首选访问方法，为组织中的所有现有活跃成员账户启用 Lambda 网络活动监控。

Console

要为所有现有活跃成员账户启用 Lambda 网络活动监控

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

使用委派 GuardDuty 管理员账户凭证登录。

2. 在导航窗格中，选择 Lambda 保护。
3. 在 Lambda 保护页面上，您可以查看配置的当前状态。在活跃成员账户部分下，选择操作。
4. 从操作下拉菜单中，选择为所有现有活跃成员账户启用。
5. 选择确认。

API/CLI

- 要有选择地为您的成员账户启用或禁用 Lambda 网络活动监控，请使用您自己的账户调用 `updateMemberDetectors` API 该操作 *detector ID*。
- 以下示例显示如何为单个成员账户启用 Lambda 网络活动监控。要禁用成员账户，请将 `ENABLED` 替换为 `DISABLED`。

要查找您的账户和当前区域的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 `ListDetectors` API。 `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

您也可以传递用空格 IDs 分隔的账户列表。

- 成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

为新成员账户自动启用 Lambda 网络活动监控

选择您的首选访问方法，为加入组织的新账户启用 Lambda 网络活动监控。

Console

委派的 GuardDuty 管理员账户可以使用 Lambda 保护或账户页面为组织中的新成员账户启用 Lambda 网络活动监控。

要为新成员账户自动启用 Lambda 网络活动监控

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 请执行以下操作之一：

- 使用 Lambda 保护页面：

1. 在导航窗格中，选择 Lambda 保护。
2. 在 Lambda 保护页面上，选择编辑。
3. 选择手动配置账户。
4. 选择为新成员账户自动启用。此步骤可确保每当有新账户加入您的组织时，系统都会自动为其账户启用 Lambda 保护。只有组织委派的 GuardDuty 管理员帐户才能修改此配置。
5. 选择保存。

- 使用账户页面：

1. 在导航窗格中，选择账户。
2. 在账户页面上，选择自动启用首选项。
3. 在管理自动启用首选项窗口中，在 Lambda 网络活动监控下选择为新账户启用。
4. 选择保存。

API/CLI

- 要为新成员账户启用或禁用 Lambda 网络活动监控，请使用您自己的账户调用该 [UpdateOrganizationConfiguration](#) API 操作 *detector ID*。

- 以下示例显示如何为单个成员账户启用 Lambda 网络活动监控。要将其禁用，请参阅 [有选择地为成员账户启用或禁用 Lambda 网络活动监控](#)。如果您不想为所有加入组织的新账户启用该功能，请将 `AutoEnable` 设置为 `NONE`。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。 `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

- 成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

有选择地为成员账户启用或禁用 Lambda 网络活动监控

选择您的首选访问方法，有选择地为成员账户启用或禁用 Lambda 网络活动监控。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

请务必使用委派 GuardDuty 管理员账户证书。

2. 在导航窗格中的设置下，选择账户。

在账户页面上，查看 Lambda 网络活动监控列。此列指示是否启用 Lambda 网络活动监控。

3. 选择您要为其配置 Lambda 保护的账户。您可以一次选择多个账户。
4. 从编辑保护计划下拉菜单中，选择 Lambda 网络活动监控，然后选择相应的操作。

API/CLI

[updateMemberDetectors](#)API使用你自己的调用 *detector ID*。

以下示例显示如何为单个成员账户启用 Lambda 网络活动监控。要将其禁用，请将 `ENABLED` 替换为 `DISABLED`。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。 `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":  
"ENABLED"}]'
```

您也可以传递用空格IDs分隔的账户列表。

成功执行代码后，会返回 `UnprocessedAccounts` 的空列表。如果更改账户的检测器设置时出现任何问题，则会列出该账户 ID 和问题摘要。

保护 AI 工作负载 GuardDuty

Amazon GuardDuty [基础威胁检测](#) 和 [Lambda Protection](#) 可帮助您更好地保护和检测基于人工智能工作负载的威胁。AWS

[基础 GuardDuty 威胁检测](#) 可监控 AWS CloudTrail 管理事件，以检测使用 AWS 服务（包括 Amazon Bedrock 和 Amazon SageMaker）创建的生成式 AI 工作负载中的可疑和恶意活动。例如，GuardDuty 可以识别以下活动：

- 异常拆除 Amazon Bedrock 安全护栏
- 更改可能导致数据中毒攻击的模型训练数据源
- 可疑 Amazon Bedrock 模型被调用
- 不寻常的笔记本实例或在 SageMaker 中创建训练作业
- 被泄露的亚马逊弹性计算云凭证可能被用来调用 Amazon Bedrock、Amazon APIs 或 EC2 实例 SageMaker、EKS 集群或任务上的自我管理的 AI 工作负载。ECS

GuardDuty Lambda Protection 可以帮助检测与 Amazon Bedrock 代理相关的潜在威胁。这可能包括可疑的网络活动，例如加密挖矿，以及与可能由供应链攻击或复杂提示引起的恶意命令和控制服务器的通信。

以下视频显示了相关发现的样子。

以下视频显示了相关发现的样子。[使用 Amazon GuardDuty 监控和保护您构建的 AI 工作负载 AWS](#)

在 Amazon 中管理多个账户 GuardDuty

当您的 AWS 环境有多个帐户时，您可以通过将一个帐户指定为管理员帐户来管理它们。然后，您可以将多个 AWS 帐户与该管理员帐户关联为其成员帐户。使用此配置，指定的 GuardDuty 管理员帐户可以评估和监控组织的整体安全性。管理员帐户还可以执行帐户管理任务，例如查看所有生成的调查结果并在其中配置保护计划 GuardDuty。

在中 GuardDuty，组织由一个委派的 GuardDuty 管理员帐户和一个或多个关联的成员帐户组成。您可以通过两种方式关联帐户：与帐户集成 AWS Organizations，或者使用 GuardDuty 控制台中发送和接受会员邀请的传统方法。GuardDuty 建议您与集成 AWS Organizations。

AWS Organizations 是一项全球帐户管理服务，使 AWS 管理员能够整合和集中管理多个帐户 AWS 帐户。它提供帐户管理和整合账单功能，这些功能旨在满足预算、安全性和合规性需求。它不收取额外费用，并且可以与包括 Macie 和 Amazon AWS 服务 GuardDuty 在内的多种 AWS Security Hub 产品集成。有关更多信息，请参阅 [用户指南。AWS Organizations](#)

内容

- [了解 GuardDuty 管理员帐户和成员帐户之间的关系](#)
- [使用管理 GuardDuty 帐户 AWS Organizations](#)
- [通过邀请管理 GuardDuty 帐户](#)

了解 GuardDuty 管理员帐户和成员帐户之间的关系

当您在多帐户环境 GuardDuty 中使用，管理员帐户可以代表成员帐户管理某些方面。GuardDuty 管理员帐户可以执行以下主要功能：

- 添加和删除关联的成员帐户。管理员帐户可以执行此操作的流程因您管理帐户的方式而异（通过组织或通过邀请）。
- 在 GuardDuty 管理帐户 GuardDuty 中启用委托管理员帐户

如果 AWS Organizations 管理帐户禁用 GuardDuty，则委派 GuardDuty 管理员帐户可以在管理帐户 GuardDuty 中启用。但是，要求管理帐户必须未明确删除的[服务相关角色权限 GuardDuty](#)。

- 管理关联成员帐户 GuardDuty 内的状态，包括启用和暂停 GuardDuty。

Note

在添加为成员的账户 GuardDuty 中，使用 AWS Organizations 自动启用来管理的委托管理
员帐户。

- 通过创建和管理抑制规则、可信 IP 列表和威胁列表，自定义 GuardDuty 网络内部的调查结果。在多
账户环境中，这些功能的配置仅适用于委派的 GuardDuty 管理员帐户。成员账户无法更新此配置。

下表详细说明了 GuardDuty 管理员账户和成员账户之间的关系。

在此表中：

- Self — 账户只能为自己的账户执行列出的操作。
- 任意-账户可以对任何关联账户执行列出的操作。
- 全部 — 一个账户可以执行列出的操作，它适用于所有关联的账户。通常，执行此操作的帐户是指定
的 GuardDuty 管理员帐户

带有短划线 (—) 的表格单元格表示该账户无法执行列出的操作。

操作	通过 AWS Organizations		通过邀请	
	委派 GuardDuty 管理员账号	关联的成员账户	委派 GuardDuty 管理员账号	关联的成员账户
启用 GuardDuty	任何	—	自身	自身
为整个组织 GuardDuty 自动启用 (ALL、NEW、NONE)	全部	—	—	—
查看所有 Organizations 成 员账户，无论其 GuardDuty 状态 如何	任何	—	—	—

生成示例发现结果	自身	自身	自身	自身
查看所有 GuardDuty 发现	任何	自身	任何	自身
存档 GuardDuty 调查结果	任何	—	任何	—
应用禁止规则	全部	—	全部	—
创建可信 IP 列表或威胁列表	全部	—	全部	—
更新可信 IP 列表或威胁列表	全部	—	全部	—
删除可信 IP 列表或威胁列表	全部	—	全部	—
设置 EventBridge 通知频率	全部	—	全部	自身
设置用于导出调查发现的 Amazon S3 位置	全部	—	全部	自身
为整个组织启用一个或多个可选保护计划 (ALL、NEW、NONE)	全部	—	—	—

这不包括 S3 的恶意软件防护。

为个人账户启用任何 GuardDuty 保护计划	任何	—	任何	—
这不包括 S3 的恶意软件防护 EC2 和恶意软件防护。				
恶意软件防护 EC2	任何	—	自身	自身
S3 恶意软件防护	—	自身	—	自身
取消关联成员账户	任何	—	任何	—
取消与管理员账户账户的关联	—	自我 ⁺	—	自身
删除已取消关联的成员账户	任何	—	任何	—
暂停 GuardDuty	任何 [*]	—	任何 [*]	—
禁用 GuardDuty	任何 [*]	—	任何 [*]	—

⁺ 表示只有在委派的 GuardDuty 管理员帐户尚未为组织成员设置自动启用首选项时，该帐户才能 ALL 执行此操作。

^{*} 表示委托 GuardDuty 管理员帐户不能直接 GuardDuty 在成员帐户中禁用。委托 GuardDuty 管理员帐号必须先解除关联成员帐号，然后再将其删除。之后，每个成员帐户都可以在自己的帐户 GuardDuty 中禁用。有关在组织中执行这些任务的更多信息，请参阅[在内部维护您的组织 GuardDuty](#)。

使用管理 GuardDuty 账户 AWS Organizations

在 AWS 组织中，管理帐户可以将该组织内的任何帐户指定为委派 GuardDuty 管理员帐户。对于此管理员帐户，GuardDuty 仅在当前帐户中自动启用 AWS 区域。默认情况下，管理员帐户可以启用和管理 GuardDuty 该区域内组织中的所有成员帐户。管理员帐户可以查看该 AWS 组织并向其添加成员。

以下各节将引导您完成作为委派 GuardDuty 管理员帐户可能执行的各种任务。

与 GuardDuty 一起使用的注意事项和建议 AWS Organizations

以下注意事项和建议可以帮助您了解委派 GuardDuty 管理员账户在中的运作方式 GuardDuty :

一个委托 GuardDuty 管理员账号最多可以管理 50,000 个成员。

每个委托 GuardDuty 管理员账户的成员账户上限为 50,000 个。这包括通过添加的成员账户 AWS Organizations 或接受 GuardDuty 管理员账户邀请加入其组织的成员账户。但是，您的 AWS 组织中可能有超过 50,000 个帐户。

如果您超过了 50,000 个成员账户的限制，您将收到来自 CloudWatch AWS Health Dashboard、的通知以及发送给指定委托 GuardDuty 管理员账户的电子邮件。

委托 GuardDuty 管理员账户为区域账户。

与之不同 GuardDuty 的是 AWS Organizations，是区域服务。必须在您已 GuardDuty 启用的每个所需区域 AWS Organizations 中添加委托 GuardDuty 管理员帐户及其成员帐户。如果组织管理帐户仅在美国东部（弗吉尼亚北部）指定委托 GuardDuty 管理员账户，则委派 GuardDuty 管理员账户将仅管理添加到该地区组织的成员账户。有关可用区域中功能对等性的 GuardDuty 更多信息，请参阅[区域和端点](#)。

选择加入区域的特殊情况

- 当委托 GuardDuty 管理员账户选择退出选择加入区域时，即使您的组织将 GuardDuty 自动启用配置设置为仅限新成员账户 (NEW) 或所有成员账户 (ALL)，也 GuardDuty 无法为组织中当前已禁用的任何成员账户启用自动启用配置。GuardDuty 有关您的成员账户配置的信息，请在[GuardDuty 控制台](#) 导航窗格中打开账户或使用[ListMembers](#) API。
- 使用设置为的 GuardDuty 自动启用配置时 NEW，请确保满足以下顺序：
 1. 成员账户选择加入可选区域。
 2. 在中将成员帐户添加到您的组织 AWS Organizations。

如果您更改这些步骤的顺序，则 GuardDuty 自动启用设置在特定的选择加入区域 NEW 将不起作用，因为该组织已不再是成员账户的新用户。GuardDuty 提供了两种备选解决方案：

- 将 GuardDuty 自动启用配置设置为 ALL，包括新的和现有的成员帐户。在这种情况下，这些步骤的顺序无关紧要。
- 如果成员账户已经是您组织的一部分，请使用 GuardDuty 控制台或，在特定的选择加入区域中单独管理该账户的 GuardDuty 配置。API

AWS 组织必须拥有相同的委托 GuardDuty 管理员帐户 AWS 区域。

您必须将一个成员帐户指定为所有启用 AWS 区域 位置 GuardDuty 的委托 GuardDuty 管理员帐户。例如，如果您指定了成员帐户 `111122223333` in *Europe (Ireland)*，您不能指定其他成员帐户 `555555555555` in *Canada (Central)*。在所有其他区域，您必须使用与委托 GuardDuty 管理员帐户相同的帐户。

您可以随时指定新的委派 GuardDuty 管理员帐户。有关删除现有委派 GuardDuty 管理员帐户的更多信息，请参阅[更改委派 GuardDuty 管理员账号](#)。

不建议将贵组织的管理账号设置为委派 GuardDuty 管理员账号。

您组织的管理账号可以是委派的 GuardDuty 管理员账号。但是，AWS 安全最佳实践遵循最低权限原则，不建议使用此配置。

更改委派 GuardDuty 管理员帐户不会 GuardDuty 对成员帐户禁用。

如果您移除委派 GuardDuty 管理员账号，则 GuardDuty 会移除与该委派 GuardDuty 管理员账号关联的所有成员账号。GuardDuty 所有这些成员帐户仍保持启用状态。

指定委派 GuardDuty 管理员账号所需的权限

要开始 GuardDuty 使用 Amazon AWS Organizations，该组织的 AWS Organizations 管理帐户会将一个帐户指定为委托 GuardDuty 管理员帐户。这可以 GuardDuty 作为可信的服务在中启用 AWS Organizations。它还 GuardDuty 支持委派 GuardDuty 管理员帐户，还允许委派管理员帐户启用和管理 GuardDuty 当前区域组织中的其他帐户。有关如何授予这些权限的信息，请参阅[与其他 AWS 服务 AWS Organizations 一起使用](#)。

作为 AWS Organizations 管理帐户，在为组织指定委派 GuardDuty 管理员帐户之前，请确认您可以执行以下 GuardDuty 操作：`guardduty:EnableOrganizationAdminAccount`。此操作允许您使用为您的组织指定委派 GuardDuty 管理员帐户 GuardDuty。您还必须确保允许您执行有助于检索组织信息的 AWS Organizations 操作。

要授予这些权限，请在帐户的 AWS Identity and Access Management (IAM) 策略中加入以下声明：

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
```

```

    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}

```

如果您想将自己的 AWS Organizations 管理账号指定为委派 GuardDuty 管理员账号，您的账户还需要 IAM 执行以下操作：`CreateServiceLinkedRole`。此操作允许您为管理账户 GuardDuty 进行初始化。但是，在继续添加权限与 [GuardDuty 一起使用的注意事项和建议 AWS Organizations](#) 之前，请先进行查看。

要继续将管理账号指定为委派 GuardDuty 管理员账户，请在 IAM 策略中添加以下语句并替换 **111122223333** 使用贵组织管理账户的 AWS 账户 ID：

```

{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "guarddduty.amazonaws.com"
    }
  }
}

```

指定委派 GuardDuty 管理员账号

选择首选访问方法，为您的组织指定委派 GuardDuty 管理员帐户。只有管理账户才能执行此步骤。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guarddduty/>。

要登录，请使用贵 AWS Organizations 组织的管理账户凭证。

2. 使用页面右上角的 AWS 区域选择器，选择要为组织指定委派 GuardDuty 管理员帐户的区域。
3. 根据您的管理账户在当前区域 GuardDuty 是否已启用，执行以下任一操作：
 - 如果已启 GuardDuty 用，请选择 Amazon GuardDuty -所有功能，然后选择入门。此操作将带您进入“欢迎来到 GuardDuty”页面。
 - 如果已启 GuardDuty 用，请在导航窗格中选择“设置”。
4. 在“委托管理员”下，输入要指定为组织委派 GuardDuty 管理员帐户的帐户的 12 位 AWS 帐户 ID。

请务必 GuardDuty 为您新指定的委派 GuardDuty 管理员账户启用，否则它将无法执行任何操作。

5. 选择 Delegate (委派) 。
6. (推荐) 重复上述步骤，在每个已 GuardDuty 启用的 AWS 区域 位置指定委派 GuardDuty 管理员帐户。

API/CLI

1. [enableOrganizationAdminAccount](#)使用组织管理账户 AWS 账户 的凭据运行。
 - 或者，您可以使用 AWS Command Line Interface 来执行此操作。以下 AWS CLI 命令仅为您当前的区域指定委派 GuardDuty 管理员帐户。运行以下 AWS CLI 命令并确保替换 **111111111111** 使用您要指定为委派 GuardDuty 管理员帐户的帐户 AWS 帐户 ID：

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

要为其他区域指定委派 GuardDuty 管理员帐户，请在 AWS CLI 命令中指定区域。以下示例演示如何在美国西部 (俄勒冈) 启用委托 GuardDuty 管理员账户。请务必更换 **us-west-2** 以及您要为其分配委派 GuardDuty 管理员帐户的区域。

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

有关 AWS 区域 何 GuardDuty 处可用的信息，请参见[区域和端点](#)。

GuardDuty 如果您的委托 GuardDuty 管理员账户未启用，它将无法执行任何操作。如果尚未启用，请确保 GuardDuty 为新指定的委派 GuardDuty 管理员帐户启用。

2. (推荐) 重复上述步骤，在已 GuardDuty 启用的每个 AWS 区域 位置指定委派 GuardDuty 管理员帐户。

更新组织自动启用首选项

中的自动启用组织功能 GuardDuty 可帮助您在单个步骤中为组织中的ALL现有帐户或NEW成员帐户设置相同的 GuardDuty 保护计划状态。同样，您可以通过选择来指定何时不想对成员帐户采取任何操作NEW。以下步骤说明了这些设置，并指明了何时需要使用特定设置。

选择首选访问方法以更新组织的自动启用首选项。

Console

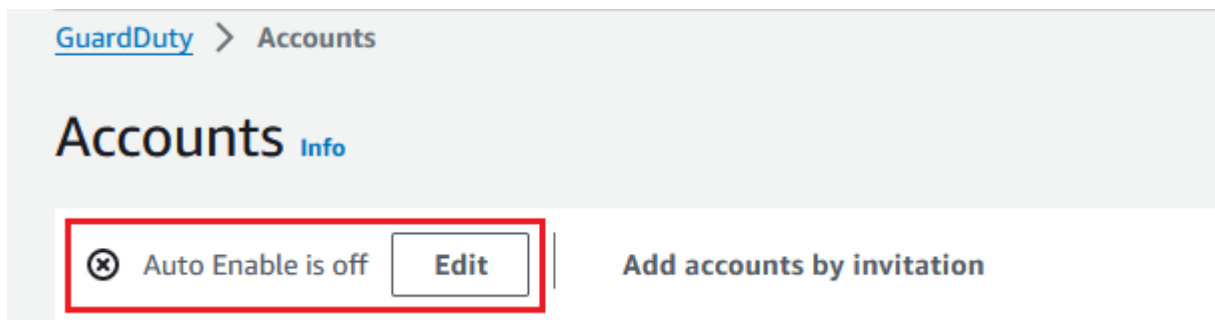
1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

要登录，请使用 GuardDuty 管理员帐户凭据。

2. 在导航窗格中，选择帐户。

“帐户”页面为 GuardDuty 管理员帐户提供要自动启用的配置选项，GuardDuty 以及代表属于该组织的成员帐户的可选保护计划。

3. 要更新现有的自动启用设置，请选择编辑。



此支持可用于配置 GuardDuty 以及您的所有受支持的可选保护计划 AWS 区域。您可以代表您的成员账户选择以下配置选项之一：GuardDuty

- 为所有帐户启用 (ALL)-选择此选项可为组织中的所有帐户启用相应的选项。这包括加入组织的新账户，以及可能已被暂停或从组织中删除的账户。这还包括委派 GuardDuty 管理员帐户。

Note

更新所有成员账户的配置最多可能需要 24 小时。

- 为新帐户自动启用 (**NEW**)-选择仅在新成员帐户加入您的组织时自动启用 GuardDuty 或可选的保护计划。
- 请勿启用 (**NONE**)-选择该选项可防止为组织中的新帐户启用相应的选项。在这种情况下，GuardDuty 管理员帐户将单独管理每个帐户。

当您将自动启用设置从ALL或更新NEW为时NONE，此操作不会禁用现有账户的相应选项。此配置将应用于加入组织的新帐户。更新自动启用设置后，任何新帐户都不会启用相应的选项。

Note

当委托 GuardDuty 管理员账户选择退出选择加入区域时，即使您的组织将 GuardDuty 自动启用配置设置为仅限新成员账户 (NEW) 或所有成员账户 (ALL)，也 GuardDuty无法为组织中当前已禁用的任何成员账户启用自动启用配置。GuardDuty 有关您的成员账户配置的信息，请在[GuardDuty 控制台](#)导航窗格中打开账户或使用[ListMembers](#)API。

4. 选择 Save changes (保存更改)。
5. (可选) 如果您想在每个地区使用相同的首选项，请分别更新每个受支持区域的首选项。

某些可选的保护计划可能并非在所有可用 AWS 区域 的地方都可 GuardDuty 用。有关更多信息，请参阅 [区域和端点](#)。


API/CLI

1. 使用[UpdateOrganizationConfiguration](#)委派 GuardDuty 管理员账户的凭据运行，在该区域为您的组织自动配置保护计划 GuardDuty 和可选保护计划。有关各种自动启用配置的信息，请参阅[autoEnableOrganization成员](#)。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

要为您所在区域中任何受支持的可选保护计划设置自动启用首选项，请按照每个保护计划的相应文档部分中提供的步骤进行操作。

- 您可以验证当前区域中组织的首选项。运行 [describeOrganizationConfiguration](#)。请务必指定委派 GuardDuty 管理员账户的检测器 ID。

 Note

更新所有成员账户的配置可能最长需要 24 小时。

- 或者，运行以下 AWS CLI 命令将首选项设置为 GuardDuty 在该区域自动启用或禁用加入组织的新帐户 (NEW)、组织中的所有帐户 (ALL) 或不包含任何帐户 (NONE)。有关更多信息，请参阅[autoEnableOrganization成员](#)。根据您的首选项，可能需要将 NEW 替换为 ALL 或 NONE。如果您使用配置保护计划 ALL，则还会为委派的 GuardDuty 管理员帐户启用保护计划。请务必指定管理组织配置的委派 GuardDuty 管理员帐户的检测器 ID。


要查找与您的账户和当前地区 detectorId 对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

- 您可以验证当前区域中组织的首选项。使用委派 GuardDuty 管理员帐户的检测器 ID 运行以下 AWS CLI 命令。

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(推荐) 使用委派 GuardDuty 管理员账户检测器 ID 在每个区域重复前面的步骤。

 Note

当委托 GuardDuty 管理员账户选择退出选择加入区域时，即使您的组织将 GuardDuty 自动启用配置设置为仅限新成员账户 (NEW) 或所有成员账户 (ALL)，也 GuardDuty 无法为组织中当前已禁用的任何成员账户启用自动启用配置。GuardDuty 有关您的成员账户配置的信息，请在[GuardDuty 控制台](#)导航窗格中打开账户或使用[ListMembers](#) API。

向组织添加成员

选择首选访问方式，将成员添加到您的组织。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

要登录，请使用委派的 GuardDuty 管理员账户证书。

2. 在导航窗格中，选择账户。

账户表显示了通过组织 (AWS Organizations) 或通过邀请添加的所有账户。如果成员账户未与组织的 GuardDuty 管理员账户关联，则该成员账户的状态为非成员。

3. 选择一个或多个 IDs 要添加为成员的帐户。这些账户的类型 IDs 必须为 Via Organizations。

通过邀请添加的账户不属于您的组织。您可以单独管理此类账户。有关更多信息，请参阅 [通过邀请管理账户](#)。

4. 选择操作下拉列表，然后选择添加成员。将此账户添加为成员后，将应用自动启用 GuardDuty 配置。根据中的设置 [更新组织自动启用首选项](#)，这些帐户的 GuardDuty 配置可能会发生变化。
5. 您可以选择“状态”列的向下箭头，按非成员状态对账户进行排序，然后选择当前区域中未 GuardDuty 启用的每个账户。

如果尚未将账户表中列出的账户添加为成员，则可以在当前区域 GuardDuty 中为所有组织账户启用。在页面顶部的横幅中选择启用。此操作会自动开启自动启用 GuardDuty 配置，GuardDuty 以便为任何加入组织的新账户启用该配置。

6. 选择确认，添加账户作为成员。此操作还 GuardDuty 适用于所有选定的帐户。账户的状态将变为已启用。
7. (推荐) 在每个步骤中重复这些步骤 AWS 区域。这样可以确保委派 GuardDuty 管理员账户可以在您 GuardDuty 启用的所有区域中管理成员账户的发现结果和其他配置。

自动启用功能 GuardDuty 适用于组织中的所有 future 成员。这样，您的委托 GuardDuty 管理员帐户就可以管理在组织内创建或添加到组织中的任何新成员。当成员账户数量达到 50,000 的上限时，自动启用功能将自动关闭。如果您删除了一个成员帐户，并且成员总数减少到少于 50,000，则自动启用功能将重新开启。

API/CLI

- 使用上一步中指定的委派 GuardDuty 管理员账户的凭据运行 [CreateMembers](#)。

您必须指定委派 GuardDuty 管理员账户的区域检测器 ID 以及要添加为 GuardDuty 成员的账户的账户详细信息 (AWS 账户 IDs 和相应的电子邮件地址)。您可以使用此 API 操作创建一个或多个成员。

当您在组织 CreateMembers 中运行时，新成员的自动启用首选项将在新成员帐户加入您的组织时适用。当您 CreateMembers 使用现有成员帐户运行时，组织配置也将应用于现有成员。这可能会更改现有成员帐户的当前配置。

[ListAccounts](#) 在“参 AWS Organizations API 考”中运行，查看 AWS 组织中的所有帐户。

Important

当您添加帐户为 GuardDuty 成员时，该帐户将在该地区自动 GuardDuty 启用。组织管理帐户有一个例外。在将管理帐户添加为 GuardDuty 成员之前，必须将其 GuardDuty 启用。

- 或者，您可以使用 AWS Command Line Interface。运行以下 AWS CLI 命令，并确保使用您自己的有效检测器 ID、AWS 帐户 ID 以及与帐户 ID 关联的电子邮件地址。

要查找与您的帐户和当前地区 detectorId 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

您可以通过运行以下 AWS CLI 命令来查看所有组织成员的列表：

```
aws organizations list-accounts
```

将此帐户添加为成员后，将应用自动启用 GuardDuty 配置。

(可选) 为现有成员帐户启用保护计划

以下步骤包括使用“帐户”页面为现有成员帐户启用保护计划的步骤。有关使用 API 或执行此操作的步骤 AWS CLI，请参阅与特定保护计划相关的文档。

您可以通过“账户”页面为个人账户启用保护计划。

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
使用委派 GuardDuty 管理员账户证书。
2. 在导航窗格中，选择账户。
3. 选择要为其配置保护计划的一个或多个账户。对要配置的每个保护计划重复以下步骤：
 - a. 选择编辑保护计划。
 - b. 从保护计划列表中，选择您要配置的一个保护计划。
 - c. 选择要为此保护计划执行的操作之一，然后选择确认。
 - d. 对于选定账户，与配置的保护计划对应的列将显示更新的配置为已启用或未启用。

在内部维护您的组织 GuardDuty

作为委托 GuardDuty 管理员帐户，您负责维护组织中每个受支持的帐户的配置 GuardDuty 及其可选保护计划 AWS 区域。以下各节提供了有关维护其 GuardDuty 任何可选保护计划的配置状态的选项：

维护每个区域中整个组织的配置状态

- 使用 GuardDuty 控制台为整个组织设置 GuardDuty 自动启用首选项 — 您可以为组织中的所有 (ALL) 成员或加入该组织的新 (NEW) 成员自动启用，也可以选择不 (NONE) 为组织中的任何成员自动启用首选项。

您也可以为其中的任何保护计划配置相同或不同的设置 GuardDuty。

更新组织中所有成员账户的配置最多可能需要 24 小时。

- 使用 API — 运行来更新自动启用首选项 [UpdateOrganizationConfiguration](#)，为组织自动配置 GuardDuty 及其可选保护计划。当您在组织中 [CreateMembers](#) 添加新的成员账户时，配置的设置将自动应用。当您 [CreateMembers](#) 使用现有成员帐户运行时，组织配置也将应用于现有成员。这可能会更改现有成员账户的当前配置。

要查看组织中的所有账户，请在“AWS Organizations API 参考” [ListAccounts](#) 中运行。

在每个区域中单独维护成员账户的配置状态

- 要查看组织中的所有账户，请在“AWS Organizations API 参考” [ListAccounts](#) 中运行。

- 如果您希望选定的成员帐户具有不同的配置状态，请分别[UpdateMemberDetectors](#)为每个成员帐户运行。

您可以通过导航到 GuardDuty 控制台中的“帐户”页面，使用 GuardDuty 控制台来执行相同的任务。

有关使用控制台或为个人账户启用保护计划的信息API，请参阅相应保护计划的配置页面。

更改委派 GuardDuty 管理员账号

您可以更改每个区域中贵组织的委托 GuardDuty 管理员帐户，然后在每个区域委派新的管理员。要保持组织在某个区域的成员账户的安全状态，您必须在该区域拥有委托 GuardDuty 管理员账户。

移除现有的委派 GuardDuty 管理员账号

第 1 步-删除每个区域中现有的委托 GuardDuty 管理员账户

1. 作为现有的委托 GuardDuty 管理员账户，列出与您的管理员账户关联的所有成员账户。[ListMembers](#)一起跑OnlyAssociated=false。
2. 如果将 GuardDuty 或任何可选保护计划的自动启用首选项设置为ALL，则运行[UpdateOrganizationConfiguration](#)将组织配置更新为NEW或NONE。此操作将防止您在下一步中取消关联所有成员帐户时出错。
3. 运行[DisassociateMembers](#)以取消与管理员帐户关联的所有成员帐户的关联。
4. 运行[DeleteMembers](#)删除管理员账户和成员账户之间的关联。
5. 以组织管理帐户的身份运行[DisableOrganizationAdminAccount](#)以删除现有的委派 GuardDuty 管理员帐户。
6. 在您拥有此委派 GuardDuty 管理员帐户的每个 AWS 区域 位置重复这些步骤。

第 2 步-在 AWS Organizations（一次性全局操作）中注销现有委派 GuardDuty 管理员账户

- [DeregisterDelegatedAdministrator](#)在“参AWS Organizations API考”中运行，注销中现有的委派 GuardDuty 管理员帐户。AWS Organizations

或者，你可以运行以下 AWS CLI 命令：

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --service-principal guardduty.amazonaws.com
```

请务必更换 **111122223333** 使用现有的委派 GuardDuty 管理员账户。

注销旧的委托 GuardDuty 管理员账号后，可以将其作为成员账号添加到新的委托 GuardDuty 管理员账号中。

在每个区域指定一个新的委托 GuardDuty 管理员账户

1. 使用您的首选访问方法（GuardDuty 控制台或API或），在每个区域指定一个新的委托 GuardDuty 管理员帐户 AWS CLI。有关更多信息，请参阅 [指定委派 GuardDuty 管理员账号](#)。
2. 运行 [DescribeOrganizationConfiguration](#) 以查看您的组织当前的自动启用配置。

Important

在向新的委派 GuardDuty 管理员账户添加任何成员之前，必须验证组织的自动启用配置。此配置特定于新的委派 GuardDuty 管理员账户和所选区域，与无关 AWS Organizations。当您在新的委派 GuardDuty 管理员账户下添加（新的或现有的）组织成员账户时，新的委派 GuardDuty 管理员账户的自动启用配置将在启用 GuardDuty 或其任何可选保护计划时适用。

使用您的首选访问方法（GuardDuty 控制台或API或）更改新委派 GuardDuty 管理员账户的组织配置 AWS CLI。有关更多信息，请参阅 [更新组织自动启用首选项](#)。

通过邀请管理 GuardDuty 账户

要管理您的组织外部的账户，可以使用传统邀请方法。使用此方法时，如果其他账户接受您的邀请成为成员账户，您的账户将被指定为管理员账户。

如果您的账户不是管理员帐户，则可以接受其他账户的邀请。接受邀请后，您的账户将成为成员账户。一个 AWS 账户不能同时是 GuardDuty 管理员账户和成员账户。

当你接受来自一个账户的邀请时，你不能接受来自另一个账户的邀请。要接受其他账户的邀请，您首先需要取消您的账户与现有管理员账户的关联。或者，管理员账户也可以取消关联您的账户并将其从其组织中移除。

通过邀请关联的账户与关联的账户具有相同的总体管理员 account-to-member 关系 AWS Organizations，如中所述 [了解 GuardDuty 管理员账户和成员账户之间的关系](#)。但是，邀请管理员账户

用户无法 GuardDuty 代表关联的成员账户启用，也不能查看其 AWS Organizations 组织内的其他非成员账户。

⚠ Important

使用此方法 GuardDuty 创建成员账户时，可能会发生跨区域数据传输。为了验证成员账户的电子邮件地址，请 GuardDuty 使用仅在美国东部（弗吉尼亚北部）地区运行的电子邮件验证服务。

通过邀请添加和管理账户

选择一种访问方法来添加和邀请帐户以 GuardDuty 管理员帐户的身份成为 GuardDuty 成员帐户。

Console

步骤 1：添加账户

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择账户。
3. 在顶部窗格中选择通过邀请添加账户。
4. 在“添加成员帐户”页面的“输入账户详细信息”下，输入与要添加的账户关联的 AWS 账户 ID 和电子邮件地址。
5. 要添加另一行，以便逐个输入账户详细信息，请选择添加其他账户。您也可以选择上传包含账户详细信息的.csv 文件来批量添加账户。

⚠ Important

csv 文件的第一行必须包含以下标头，如以下示例所示：Account ID,Email。随后的每一行都必须包含一个有效的 AWS 账户 ID 及其关联的电子邮件地址。如果一行仅包含一个 AWS 账户 ID 和用逗号分隔的关联电子邮件地址，则该行的格式有效。

```
Account ID,Email
```

```
555555555555,user@example.com
```

6. 添加所有账户的详细信息后，选择下一步。您可以在账户表中查看新添加的账户。这些账户的状态是未发送邀请。有关向一个或多个添加的账户发送邀请的信息，请参阅 [Step 2 - Invite an account](#)。

步骤 2：邀请账户

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择账户。
3. 选择一个或多个您想要邀请加入 Amazon 的账户 GuardDuty。
4. 选择操作下拉菜单，然后选择邀请。
5. 在 GuardDuty “邀请加入”对话框中，输入（可选）邀请消息。

如果受邀请的账户无法访问电子邮件，请选中同时向受邀者的 AWS 账户上的根用户发送电子邮件通知，并在受邀者的 AWS Health Dashboard 中生成警报。

6. 选择 Send invitation (发送邀请)。如果被邀请人有权访问指定的电子邮件地址，则他们可以通过打开 GuardDuty 控制台来查看邀请。 <https://console.aws.amazon.com/guardduty/>
7. 受邀者接受邀请后，状态列中的值将变为已邀请。有关接受邀请的信息，请参阅 [Step 3 - Accept an invitation](#)。

步骤 3：接受邀请

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

Important

必须 GuardDuty 先启用，然后才能查看或接受成员资格邀请。

2. 只有在 GuardDuty 尚未启用的情况下才执行以下操作；否则，可以跳过此步骤继续下一步。

如果您尚未启用 GuardDuty，请在 Amazon GuardDuty 页面上选择“开始”。

在“欢迎来到 GuardDuty”页面上，选择“启用” GuardDuty。

3. GuardDuty 为您的账户启用后，请按照以下步骤接受成员资格邀请：
 - a. 在导航窗格中，选择 Settings (设置)。
 - b. 选择 账户。
 - c. 在账户上，确保证您接受邀请的账户的所有者。打开接受以接受成员资格邀请。
4. 接受邀请后，您的账户将成为 GuardDuty 成员账户。所有者发送邀请的账户成为 GuardDuty 管理员账户。管理员账户就会知道您已接受邀请。他们账户中的 GuardDuty 账户表将会更新。状态列中与您的成员账户 ID 对应的值将更改为“已启用”。管理员账户所有者现在可以代表

您的账户查看 GuardDuty 、管理和保护计划配置。管理员账户还可以查看和管理为您的成员账户生成的 GuardDuty 调查结果。

API/CLI

您可以通过API操作指定 GuardDuty 管理员帐户，并通过邀请创建或添加 GuardDuty 成员帐户。运行以下 GuardDuty API操作以在中指定管理员帐户和成员帐户 GuardDuty。

使用要指定为 GuardDuty 管理员帐户 AWS 账户 的凭据完成以下过程。

创建或添加成员账户

1. 使用已 GuardDuty 启用的 AWS 账户的凭据运行[CreateMembers](#)API操作。这是您想要成为管理员帐户的 GuardDuty 帐户。

您必须指定当前 AWS 账户的检测器 ID 以及想要成为 GuardDuty 成员的账户的账户 ID 和电子邮件地址。您可以使用此API操作创建一个或多个成员。

您也可以使用 AWS 命令行工具通过运行以下CLI命令来指定管理员帐户。务必使用您自己的有效探测器 ID、账户 ID 和电子邮件。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. 使用已 GuardDuty 启用的 AWS 账户的凭据运行[InviteMembers](#)。这是您想要成为管理员帐户的 GuardDuty 帐户。

您必须指定当前 AWS 账户的检测器 ID 和要成为 GuardDuty 成员IDs的账户的账户。您可以通过此API操作邀请一个或多个成员。

Note

您也可以使用 message 请求参数指定可选的邀请消息。

您还可以通过运行以下命令 AWS Command Line Interface 来指定成员帐户。IDs对于要邀请的帐户，请务必使用自己的有效探测器 ID 和有效的帐户。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

接受邀请

使用要指定为 GuardDuty 成员账户的每个 AWS 账户的凭据完成以下过程。

1. 对每个受邀成为 GuardDuty 成员 AWS 账户并希望接受邀请的账户运行该[CreateDetector](#)API 操作。

您必须指定是否要使用该 GuardDuty 服务启用探测器资源。必须创建并启用探测器 GuardDuty 才能投入运行。GuardDuty 在接受邀请之前，必须先启用。

您也可以使用 AWS 命令行工具使用以下 CLI 命令来执行此操作。

```
aws guardduty create-detector --enable
```

2. 使用该 AWS 账户的凭证对每个要接受成员资格邀请的账户运行该[AcceptAdministratorInvitation](#)API 操作。

您必须为成员账户指定此 AWS 账户的探测器 ID、发送邀请的管理员账户的账户 ID 以及您正在接受的邀请的邀请 ID。您可以在邀请电子邮件中找到管理员帐户的帐户 ID，也可以使用[ListInvitations](#)操作来找到 API。

您可以通过运行以下 AWS CLI 命令使用命令行工具接受邀请。务必使用有效的检测器 ID、管理员账户 ID 和邀请 ID。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。detectorId

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
--administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

将 GuardDuty 管理员账户整合到单个组织委托 GuardDuty 管理员账户下

GuardDuty 建议使用关联 AWS Organizations 来管理委派 GuardDuty 管理员账户下的成员账户。您可以使用下面概述的示例流程，将组织中受邀关联的管理员帐户和成员整合到一个 GuardDuty 委派的 GuardDuty 管理员账户下。

Note

已由委派 GuardDuty 管理员账户管理的账户或与委派 GuardDuty 管理员账户关联的活跃成员账户无法添加到其他委托 GuardDuty 管理员账户。每个组织在每个区域只能有一个委托 GuardDuty 管理员账户，每个成员账户只能有一个委托 GuardDuty 管理员账户。

选择一种访问方法，将 GuardDuty 管理员帐户合并到单个委派 GuardDuty 管理员帐户下。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

若要登录，请使用组织的管理账户凭证。

2. 您要管理的所有账户都 GuardDuty 必须是您的组织的一部分。有关向组织添加账户的信息，请参阅 [邀请 AWS 账户 加入您的组织](#)。
3. 确保所有成员账户都与您想要指定为单一委派 GuardDuty 管理员账户的账户相关联。取消关联仍与原有管理员账户关联的成员账户。

以下步骤可帮助您取消成员账户与原有管理员账户的关联：

- a. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
 - b. 若要登录，请使用原有管理员账户凭证。
 - c. 在导航窗格中，选择账户。
 - d. 在账户页面上，选择一个或多个要与管理员账户取消关联的账户。
 - e. 选择操作，然后选择取消关联账户。
 - f. 选择确认以完成该步骤。
4. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

若要登录，请使用管理账户凭证。

5. 在导航窗格中，选择 Settings (设置)。在“设置”页面上，为组织指定委派 GuardDuty 管理员帐户。
6. 登录指定的委派 GuardDuty 管理员账号。
7. 添加组织中的成员。有关更多信息，请参阅 [使用管理 GuardDuty 账户 AWS Organizations](#)。

API/CLI

1. 您要管理的所有账户都 GuardDuty 必须是您的组织的一部分。有关向组织添加账户的信息，请参阅[邀请 AWS 账户 加入您的组织](#)。
2. 确保所有成员账户都与您想要指定为单一委派 GuardDuty 管理员账户的账户相关联。
 - a. 运行[DisassociateMembers](#)以取消仍与先前存在的管理员帐户关联的所有成员帐户的关联。
 - b. 或者，您可以使用 AWS Command Line Interface 运行以下命令并替换 `777777777777` 与您要取消关联成员帐户的先前存在的管理员帐户的探测器 ID。Replace (替换) `666666666666` 与您要取消关联的成员账户的 AWS 账户 ID。

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. 运行[EnableOrganizationAdminAccount](#)以委托 GuardDuty 管理员帐户的 AWS 账户 身份进行委托。

或者，您可以使用 AWS Command Line Interface 运行以下命令来委托委派 GuardDuty 管理员帐户：

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. 添加组织中的成员。有关更多信息，请参阅 [Create or add member member accounts using API](#)。

Important

为了最大限度地提高区域服务的效率，我们建议您指定您的委托 GuardDuty 管理员帐户，并在每个地区添加所有成员账户。GuardDuty

同时 GuardDuty 在多个账户中启用

使用以下方法同时 GuardDuty 在多个账户中启用。

使用 Python 脚本同时 GuardDuty 在多个账户中启用

您可以使用 [Amaz GuardDuty on 多账户脚本中示例存储库中的脚本自动启用或禁用 GuardDuty 多个账户](#)。使用本节中的流程启用 GuardDuty 使用 Amazon 的成员账户列表 EC2。有关使用禁用脚本或在本地设置脚本的信息，请参阅共享链接中的说明。

该 `enableguardduty.py` 脚本启用 GuardDuty、发送来自管理员账户的邀请，并接受所有成员账户中的邀请。结果是一个管理员帐户 GuardDuty 帐户，其中包含所有成员帐户的所有安全调查结果。由于按区域隔离，GuardDuty 因此每个成员帐户的搜索结果都会汇总到管理员帐户中的相应区域。例如，GuardDuty 您的管理员帐户中的 `us-east-1` 区域包含来自所有关联成员帐户的所有 `us-east-1` 发现的安全发现。

这些脚本依赖于与托管策略共享的 IAM 角色 — [AWS 托管策略：AmazonGuardDutyFullAccess](#)。此策略为实体提供访问权限，GuardDuty 并且必须存在于管理员帐户和您要启用的每个帐户中 GuardDuty。

默认情况下，以下过程 GuardDuty 将在所有可用区域启用。只有使用可选 `--enabled_regions` 参数并提供以逗号分隔的区域列表，才能在指定的区域中启用 GuardDuty。您还可以选择通过打开 `enableguardduty.py` 并编辑 `gd_invite_message` 字符串，自定义发送给成员帐户的邀请消息。

1. 在 GuardDuty 管理员帐户中创建 IAM 角色并附加要启用的 [AWS 托管策略：AmazonGuardDutyFullAccess](#) 策略 GuardDuty。
2. 在您希望由 GuardDuty 管理员帐户管理的每个成员帐户中创建一个 IAM 角色。此角色必须与步骤 1 中创建的角色同名，它应允许管理员帐户作为可信实体，并且其 `AmazonGuardDutyFullAccess` 托管策略应与前面描述的相同。
3. 启动具有附加角色的新的 Amazon Linux 实例，该角色具有允许实例代入服务角色的以下信任关系。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      }
    }
  ],
```

```
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

4. 登录到新实例，然后运行以下命令进行设置。

```
sudo yum install git python  
sudo yum install python-pip  
pip install boto3  
aws configure  
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git  
cd amazon-guardduty-multiaccount-scripts  
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. 创建一个CSV文件，其中包含您在步骤 2 中添加角色的成员账户的账户列表IDs和电子邮件。必须每行显示一个账户，账户 ID 和电子邮件地址必须用逗号分隔，如以下示例中所示。

```
111122223333,guardduty-member@organization.com
```

Note

该CSV文件必须与您的enableguardduty.py脚本位于同一位置。您可以使用以下方法将现有CSV文件从 Amazon S3 复制到当前目录。

```
aws s3 cp s3://my-bucket/my_key_name example.csv
```

6. 运行 Python 脚本。请务必提供您的 GuardDuty 管理员帐户 ID、在第一步中创建的角色名称以及您的CSV文件名作为参数。

```
python enableguardduty.py --master_account 444455556666 --assume_role  
roleName accountID.csv
```

了解亚马逊的 GuardDuty 调查结果

GuardDuty 发现的结果代表在您的网络中检测到的潜在安全问题。GuardDuty 每当它在您的 AWS 环境中检测到意外和潜在的恶意活动时，都会生成调查结果。

您可以在 GuardDuty 控制台的 Find GuardDuty findings 页面上或使用 AWS CLI 或 API 操作来查看和管理您的调查结果。有关管理调查发现的方法概述，请参阅 [管理 Amazon GuardDuty 调查结果](#)。

主题：

[GuardDuty 查找格式](#)

了解 GuardDuty 发现类型的格式以及跟踪的不同威胁目的 GuardDuty。

[示例发现结果](#)

尝试生成样本调查结果以测试和理解 GuardDuty 发现结果和相关细节。这些发现标有前缀 [SAMPLE]。

[专用账户中的测试 GuardDuty 结果](#)

在专用的非生产环境中运行 guardduty-tester 脚本 AWS 账户，在您的 AWS 环境中生成选定的 GuardDuty 结果。

[调查发现详细信息](#)

了解与您的账户中生成的 GuardDuty 调查结果相关的详细信息。

[调查发现类型](#)

按类型查看和搜索所有可用的 GuardDuty 查找结果。每个调查发现类型条目都包括该调查发现的说明以及补救的提示和建议。

GuardDuty 查找格式

当 AWS 在您的 AWS 环境中检测到可疑或意外行为时，它会生成一个调查结果。调查结果是一个通知，包含有关发现的潜在安全问题的详细信息。调查结果详细信息包括有关所发生情况、可疑活动涉及哪些 AWS 资源、此活动何时发生等信息及其他信息。

调查结果详细信息中最有用的一部分信息是调查结果类型。调查结果类型的目的是为潜在安全问题提供简明且可读的说明。例如，的 Recon:EC2/PortProbeUnprotectedPortAWS 调查结果类型快速通知您，在 AWS 环境中的某个位置，潜在攻击者正在探查某个 EC2 实例未受保护的端口。

为所生成的各种调查结果类型使用以下格式：

威胁目的：资源类型受影响/威胁家族名称。检测机制！ 构件

此格式的每个部分都代表查找类型的一个方面。这些方面有以下解释：

- ThreatPurpose – 描述威胁或潜在攻击的主要目标。有关 GuardDuty 威胁目的的完整列表，请参阅以下部分。
- ResourceTypeAffected – 描述在此调查结果中将哪些 AWS 资源确定为攻击的潜在目标。目前，GuardDuty 可以为 EC2、S3、IAM 和 EKS 资源生成调查结果。
- ThreatFamilyName – 描述正在检测的整体威胁或潜在恶意活动。例如，NetworkPortUnusual 值指示在调查结果中确定的 EC2 实例以前没有同样在该调查结果中确定的特定远程端口上进行通信的历史记录。
- 检测机制——描述了 GuardDuty 检测发现的方法。这可以用来表示常见发现类型的变体或 GuardDuty 使用特定机制来检测的发现。例如，backdoor: ec2/denialofService.tcp 表示在 TCP 上检测到拒绝服务 (DoS)。UDP 变体是 backdoor: ec2/denialofService.udp。

.Custom 值表示 GuardDuty 根据您的自定义威胁列表检测到了该发现，而 .Reputation 则表示 GuardDuty 使用域名信誉评分模型检测到了该发现。
- Artifact – 描述攻击中所用工具拥有的特定资源。例如，结果类型 CryptoCurrency:EC2/BitcoinTool.BIDNS 中的 DNS 表示 EC2 实例正在与已知的比特币相关域进行通信。

威胁目的

在 GuardDuty 中，威胁目的描述了威胁的主要目的、攻击类型或潜在攻击的阶段。例如，某些威胁目的（例如 Backdoor）表示一种攻击。但是，某些威胁目的，例如冲击，与 [MITRE ATT&CK](#) 战术一致。MITRE ATT&CK 战术表明了对手攻击周期的不同阶段。在当前版本中，ThreatPurpose 可以具有以下值：

后门

Backdoor – 此值表示攻击盗用了 AWS 资源并可以与其主命令和控制 (C&C) 服务器通信，用于进一步接收恶意活动的指令。

行为

此值表示 GuardDuty 检测到的活动或活动模式与所涉资源的既定基准 AWS 不同。

凭证访问权限

此值表示 GuardDuty 已检测到活动模式，攻击者可能利用这些活动模式从您的环境中窃取账户 ID 或密码等凭证。这种威胁目的基于 [MITRE ATT&CK 战术](#)

加密货币

此值表示 GuardDuty 已检测到您的环境中的资源正在托管与加密货币（例如比特币）关联的软件。AWS

防御闪避

此值表示 GuardDuty 已检测到活动或活动模式，攻击者在渗透到您的环境时可能会使用这些活动或活动模式来避免被发现。这种威胁目的基于 [MITRE ATT&CK 战术](#)

探索

此值表示 GuardDuty 已检测到活动或活动模式，攻击者可能会利用这些活动或活动模式来扩展对您的系统和内部网络的了解。这种威胁目的基于 [MITRE ATT&C K 战术](#)。

执行

此值表示 GuardDuty 已检测到攻击者可能试图运行恶意代码来探索网络或窃取数据。这种威胁目的基于 [MITRE ATT&C K 战术](#)。

渗透

此值表示 GuardDuty 已检测到攻击者在尝试从您的网络中窃取数据时可能使用的活动或活动模式。这种威胁目的基于 [MITRE ATT&C K 战术](#)。

影响：

此值表示 GuardDuty 已检测到活动或活动模式，这些活动或活动模式表明对手正试图操纵、中断或破坏您的系统和数据。这种威胁目的基于 [MITRE ATT&CK 战术](#)

初始访问权限

这种威胁目的基于 [MITRE ATT&CK 战术](#)

PenTest

PentestAWS - 有时候 AWS 资源的所有者或其授权代表有意运行针对 AWS 应用程序的测试来查找漏洞，例如开放过于宽松的安全组或访问密钥等。进行这些渗透测试是为了尝试在攻击者发现之前确定和锁定易受攻击的资源。不过，授权渗透测试人员使用的一些工具免费提供，因此会由未经授权用户或攻击者用于运行探测测试。尽管不能识别这种活动背后的真实目的，但 Pentest 值指示正在检测此类活动，并且此类活动与已知渗透测试工具生成的活动类似。

持久性

此值表示 GuardDuty 已检测到活动或活动模式，即使他们的初始访问路径被切断，攻击者也可能使用这些活动或活动模式来尝试保持对系统的访问权限。例如，这可能包括在通过现有用户泄露的证书获得访问权限后创建新的 IAM 用户。删除现有用户的凭据后，攻击者将保留在原始事件中未被检测到的新用户的访问权限。这种威胁目的基于 [MITRE ATT&C K](#) 战术。

策略

Policy - 此值表示您 AWS 账户表现出的行为不符合建议的安全最佳实践。

PrivilegeEscalation

此值告诉您，您的AWS环境中涉及的主体表现出攻击者可能用来获取更高级别的网络权限的行为。这种威胁目的基于 [MITRE ATT&C K](#) 战术。

Recon

此值表示 GuardDuty 已检测到活动或活动模式，攻击者在对您的网络进行侦察时可能会使用这些活动或活动模式，以确定他们如何扩大访问范围或利用您的资源。例如，此活动可能包括通过探测端口、列出用户、数据库表等来确定AWS环境中的漏洞。

Stealth

此值表示对手正在积极试图隐瞒自己的行为。例如，他们可能使用匿名代理服务器，这使得衡量活动的真实性质变得极其困难。

木马

Trojan – 此值表示攻击使用了木马程序，悄无声息地运行恶意活动。有时候此软件貌似合法程序。有时候用户会意外运行此软件。另一些时候，此软件会自动通过利用漏洞来运行。

UnauthorizedAccess

UnauthorizedAccess – 此值表示 正在检测未经授权个人的恶意活动或可疑活动。

GuardDuty 恶意软件检测扫描引擎

Amazon GuardDuty 拥有内部构建和管理的扫描引擎和[第三方供应商](#)。两者都使用来自各种内部 Feed 的入侵指标 (IoCs)，这些信息可以查看可能针对的不同类型的恶意软件 AWS。GuardDuty 还有基于我们的安全工程师添加的YARA规则的检测定义，以及基于启发式和机器学习 (ML) 模型的检测。基于签名的检测不仅包括字节匹配，还包括可能很复杂的代码片段，扫描器可以解析内容并做出决策。

恶意软件扫描引擎不执行实时行为分析，在这种分析中，恶意软件爆炸会监控样本在真实系统中的执行情况。GuardDuty 解决方案主要是基于文件的检测。为了检测无文件恶意软件，GuardDuty 提供了基于代理的解决方案，例如适用于[运行时监控](#)亚马逊、EKS亚马逊EC2和亚马逊ECS（包括）。AWS Fargate

它使用的扫描引擎对 GuardDuty 扫描恶意软件的文件格式没有限制，可以检测不同类型的恶意软件，例如加密矿工、勒索软件和网络外壳。完全托管的 GuardDuty 扫描引擎每 15 分钟持续更新一次恶意软件签名列表。

扫描引擎是 GuardDuty 威胁情报系统的一部分，它使用内部恶意软件引爆组件。这通过独立收集来自多个来源的恶意软件和良性样本来生成新的威胁情报。来自威胁情报系统的文件哈希 IoC 类型进一步输入恶意软件扫描引擎，以根据已知的错误文件哈希值检测恶意软件。

在中生成样本调查结果 GuardDuty

您可以使用 Amazon 生成样本调查结果，GuardDuty 以帮助您可视化和了解 GuardDuty 可能生成的各种调查结果类型。生成样本查找结果时，GuardDuty 会针对每种支持的查找结果类型使用一个样本查找结果填充当前查找结果列表。

生成的示例是用占位符值填充的近似值。这些样本可能与您环境的实际发现不同，但您可以使用它们来测试各种配置 GuardDuty，例如您的 EventBridge 事件或过滤器。有关查找类型可用值的列表，请参阅[调查发现类型](#)表。

通过 GuardDuty 控制台生成样本调查结果或 API

选择您的首选访问方法以生成示例调查发现。

Note

控制台方法生成每种调查发现类型中的一种。只能通过生成单个样本发现API。

Console

使用以下过程来生成示例调查发现。此过程为每种查找类型生成一个样本 GuardDuty 查找结果。

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择设置。
3. 在设置页面上的示例调查发现下，选择生成示例调查发现。

- 在导航窗格中，选择调查发现。样本发现结果显示在“当前查找结果”页面上，前缀为 [SAMPLE]。

API/CLI

您可以通过生成与任何查找类型匹配的单个样本 GuardDuty 查找结果 [CreateSampleFindingsAPI](#)，[调查发现类型](#)表格中列出了查找类型的可用值。

这对于测试 CloudWatch 事件规则或基于发现的自动化非常有用。以下示例展示了如何使用 AWS CLI生成 Backdoor:EC2/DenialOfService.Tcp 类型的单个示例调查发现。

要查找您的账户和当前区域的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectorsAPI](#)。detectorId

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

在控制台中，通过这些方法生成的样本发现的标题始终以 [SAMPLE] 开头。样本调查结果 "sample": true 在查找结果 JSON 详细信息 additionalInfo 部分的值为。

要根据您的环境中专用和隔离 AWS 账户 环境中的模拟活动生成一些常见发现，请参阅[专用账户中的测试 GuardDuty 结果](#)。

专用账户中的测试 GuardDuty 结果

使用本文档运行测试器脚本，该脚本生成您专门用于此目的的 GuardDuty 结果。AWS 账户 当您想了解和了解某些 GuardDuty 查找类型时，可以执行这些步骤。这种体验不同于生成[示例发现结果](#)。有关测试 GuardDuty 结果体验的更多信息，请参阅[注意事项](#)。

内容

- [注意事项](#)
- [GuardDuty 调查结果测试器脚本可以生成](#)
- [步骤 1-先决条件](#)
- [步骤 2-部署 AWS 资源](#)
- [步骤 3-运行测试器脚本](#)
- [步骤 4-清理 AWS 测试资源](#)
- [常见问题疑难解答](#)。

注意事项

在继续操作之前，请考虑以下注意事项：

- GuardDuty 建议在专用的非生产环境 AWS 账户 或隔离环境中部署测试器脚本。通过运行测试器脚本，GuardDuty 将在此账户中部署某些 AWS 资源。这也将帮助您识别这些模拟结果。
- 测试器脚本使用不同的 AWS 资源组合生成 100 多个 GuardDuty 调查结果。目前，这还不包括所有的。[调查发现类型](#)有关可使用此测试器脚本生成的查找类型列表，请参阅[GuardDuty 调查结果测试器脚本可以生成](#)。
- 测试器脚本会验证您的专用账户中的 GuardDuty 配置状态。如果此帐户尚未 GuardDuty 启用，则脚本将要求您在执行时将其启用[步骤 3-运行测试器脚本](#)。测试器脚本将请求您的许可，以启用生成发现结果所需的某些保护计划。

GuardDuty 首次启用

在 GuardDuty 特定地区首次在您的专用账户中启用后，您的账户将自动注册为期 30 天的免费试用。

GuardDuty 提供可选的保护计划。启用时 GuardDuty，某些保护计划也已启用，并包含在 GuardDuty 30 天免费试用版中。有关更多信息，请参阅 [使用 GuardDuty 30 天免费试用](#)。

GuardDuty 在运行测试器脚本之前，已在您的账户中启用

如果 GuardDuty 已启用，则测试器脚本将根据参数检查某些保护计划的配置状态以及生成调查结果所需的其他账户级别设置。

通过运行此测试脚本，某些保护计划可能会在您位于某个地区的专用账户中首次启用。这将开始该保护计划的 30 天免费试用。有关与每个保护计划相关的免费试用版的信息，请参阅[使用 GuardDuty 30 天免费试用](#)。

- 测试器脚本结束后，您的专用账户将恢复到其原始保护计划配置和设置。

GuardDuty 调查结果测试器脚本可以生成

目前，测试器脚本生成以下与亚马逊 EC2、亚马逊、Amazon EKS S3 和 EKS 审计日志相关的查找类型：IAM

- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Udp](#)

- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [PenTest:IAMUser/KaliLinux](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)

- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

步骤 1-先决条件

要准备测试环境，您需要以下物品：

- Git — 根据你使用的操作系统安装 git 命令行工具。这是克隆[amazon-guardduty-tester](#)存储库所必需的。
- AWS Command Line Interface— 一种开源工具，允许您使用命令行外壳中的命令进行交互。AWS 服务 有关更多信息，请参阅《AWS Command Line Interface 用户指南》AWS CLI中的“[入门](#)”。
- AWS Systems Manager— 要使用与托管节点启动会话管理器会话，AWS CLI 必须在本地计算机上安装会话管理器插件。有关更多信息，请参阅《AWS Systems Manager 用户指南》AWS CLI中的“[安装会话管理器插件](#)”。
- Node Package Manager (NPM)-安装NPM以安装所有依赖项。
- Docker — 你必须安装了 Docker。有关安装说明，请参阅 [Docker 网站](#)。

要验证是否已安装 Docker，请运行以下命令并确认是否有类似于以下输出的输出：

```
$ docker --version
Docker version 19.03.1
```

- 在中订阅 [Kali Linux](#) 镜像。AWS Marketplace

步骤 2-部署 AWS 资源

本节列出了在您的专用账户中部署某些 AWS 资源的关键概念和步骤。

概念

以下列表提供了与帮助您部署资源的命令相关的关键概念：

- AWS Cloud Development Kit (AWS CDK)— CDK 是一个开源软件开发框架，用于在代码中定义云基础架构并通过它进行配置 AWS CloudFormation。CDK支持几种编程语言来定义称为构造的可重复使用的云组件。你可以将它们组合成堆栈和应用程序。然后，您可以将CDK应用程序部署到 AWS CloudFormation 以配置或更新资源。有关更多信息，请参阅[什么是 AWS CDK?](#) 在《AWS Cloud Development Kit (AWS CDK) 开发人员指南》中。
- Bootstrapping — 这是准备您的 AWS 环境以供使用的过程。AWS CDK在将CDK堆栈部署到 AWS 环境中之前，必须先对环境进行引导。在您的环境中配置由使用的特定 AWS 资源的过程 AWS CDK 是您将在下一节中执行的步骤的一部分-[部署 AWS 资源的步骤](#)。

有关引导工作原理的更多信息，请参阅《开发人员指南》中的 [Bootstrapping](#)。AWS Cloud Development Kit (AWS CDK)

部署 AWS 资源的步骤

执行以下步骤开始部署资源：

1. 除非在bin/cdk-gd-tester.ts文件中手动设置了专用账户“区域”变量，否则请设置您的 AWS CLI 默认账户和区域。有关更多信息，请参阅《AWS Cloud Development Kit (AWS CDK) 开发人员指南》中的[环境](#)。
2. 运行以下命令部署资源：

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

最后一个命令 (cdk deploy) 代表你创建一个 AWS CloudFormation 堆栈。此堆栈的名称是GuardDutyTesterStack。

作为此脚本的一部分，GuardDuty 创建新资源以在您的账户中生成 GuardDuty调查结果。它还向 Amazon EC2 实例添加了以下标签键:值对：

CreatedBy:GuardDuty Test Script

Amazon EC2 实例还包括托管EKS节点和ECS集群的EC2实例。

实例类型

GuardDuty t3.micro为除 Amazon EKS 节点组之外的所有资源创建。由于至少EKS需要 2 个内核，因此该EKS节点具有t3.medium实例类型。有关实例类型的更多信息，请参阅 Amazon EC2 实例类型指南中的[可用大小](#)。

步骤 3-运行测试器脚本

这是一个分为两步的过程，首先需要启动与测试驱动程序的会话，然后运行脚本以生成具有特定资源组合的 GuardDuty 结果。

A 部分-与测试驱动程序开始会话

1. 部署资源后，将区域代码保存到当前终端会话中的变量中。使用以下命令并替换 *us-east-1* 使用您部署资源的区域代码：

```
$ REGION=us-east-1
```

2. 测试器脚本只能通过 AWS Systems Manager (SSM) 获得。要在测试器主机实例上启动交互式 shell，请查询主机 InstanceId。
3. 使用以下命令开始测试器脚本的会话：

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

B 部分-生成调查结果

测试器脚本是一个基于 Python 的程序，它动态构建 bash 脚本以根据您的输入生成结果。您可以根据一种或多种 AWS 资源类型、GuardDuty 保护计划 [威胁目的](#)（战术）或灵活地生成调查结果 [the section called “GuardDuty 调查结果测试器脚本可以生成”](#)。[基础数据来源](#)

使用以下命令示例作为参考，然后运行一个或多个命令来生成要探索的结果：

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
```

```
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

有关有效参数的更多信息，可以运行以下帮助命令：

```
python3 guardduty_tester.py --help
```

C 部分-审查生成的调查结果

选择首选方法在您的账户中查看生成的调查结果。

GuardDuty console

1. 登录 AWS Management Console 并打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择 调查发现。
3. 从调查结果表中，选择要查看其详细信息的调查结果。这将打开查找详细信息面板。有关信息，请参阅[了解亚马逊的 GuardDuty 调查结果](#)。
4. 如果要筛选这些结果，请使用资源标签键和值。例如，要筛选为 Amazon EC2 实例生成的结果，请使用CreatedBy:GuardDuty Test Script 标签键:值对作为实例标签密钥和实例标签密钥。

API

- 运行[ListFindings](#)以查看特定探测器 ID 的发现结果。您可以指定参数来筛选结果。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。

AWS CLI

- 运行以下 AWS CLI 命令查看生成的查找结果并替换 *us-east-1* 以及 *12abc34d567e8fa901bc2d34EXAMPLE* 使用合适的值：

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```


要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。

有关可用于筛选结果的参数的更多信息，请参阅《AWS CLI 命令参考》中的 [list-find ings](#)。

步骤 4-清理 AWS 测试资源

当测试器脚本结束时，账户级别的设置和其他配置状态在[步骤 3-运行测试器脚本](#)返回到原始状态期间所做的更新。

运行测试器脚本后，您可以选择清理 AWS 测试资源。您可以选择使用以下方法之一来执行此操作：

- 运行以下命令：

```
cdk destroy
```

- 删除名称为的 AWS CloudFormation 堆栈GuardDutyTesterStack。有关步骤的信息，请参阅在[AWS CloudFormation 控制台上删除堆栈](#)。

常见问题疑难解答。

GuardDuty 已确定常见问题并推荐了故障排除步骤：

- Cloud assembly schema version mismatch— 更新 AWS CDK CLI到与所需云装配版本兼容的版本，或更新到最新的可用版本。有关更多信息，请参阅[AWS CDK CLI兼容性](#)。
- Docker permission denied— 将专用帐户用户添加到 docker-users 中，以便专用帐户可以运行命令。有关步骤的更多信息，请参阅 [Docker 访问被拒绝](#)。
- Your requested instance type is not supported in your requested Availability Zone— 某些可用区不支持特定的实例类型。要确定哪些可用区支持您的首选实例类型并重新尝试部署 AWS 资源，请执行以下步骤：

1. 选择一种首选方法来确定哪些可用区支持您的实例类型：

Console

识别支持首选实例类型的可用区

1. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为<https://console.aws.amazon.com/ec2/>。

2. 使用页面右上角的 AWS 区域选择器，选择要启动实例的区域。
3. 在导航窗格中的实例下，选择实例类型。
4. 从实例类型表中，选择首选实例类型。
5. 在“网络”下，查看可用区域下列出的区域。

根据这些信息，您可能需要选择一个可以部署资源的新区域。

AWS CLI

运行以下命令查看可用区列表。请务必指定您的首选实例类型和区域 (*us-east-1*)。

```
aws ec2 describe-instance-type-offerings --location-type availability-zone --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

有关此命令的更多信息，请参阅《AWS CLI 命令参考》[describe-instance-type-offerings](#)中的。

运行此命令时，如果您收到错误，请确保使用的是最新版本的 AWS CLI。有关更多信息，请参阅《AWS Command Line Interface User Guide》中的 [Troubleshooting](#)。

2. 尝试再次部署 AWS 资源并指定支持您的首选实例类型的可用区。


重新尝试部署资源 AWS

1. 在bin/cdk-gd-tester.ts文件中设置默认区域。
2. 要指定可用区，请打开该amazon-guardduty-tester/lib/common/network/vpc.ts文件。
3. 在此文件中，maxAzs: 2, 替换为必须为您的实例类型指定可用区域availabilityZones: ['*us-east-1a*', '*us-east-1c*'], 的位置。
4. 继续执行其余步骤[部署 AWS 资源的步骤](#)。

GuardDuty 调查结果的严重性级别

根据我们的安全工程师的决定，每个 GuardDuty 发现都有指定的严重级别和值，反映了该发现可能给您的网络带来的潜在风险。严重性值可以是介于 1.0 和 8.9 之间的任何值，值越高，安全风险就越

大。为了帮助您确定对调查结果中突出显示的潜在安全问题的应对措施，请将此范围 GuardDuty 分为“高”、“中”和“低”严重级别。

 Note

值 0 以及介于 9.0 和 10.0 之间的值表示保留以供将来使用。

以下是目前为 GuardDuty调查结果定义的严重程度和值，以及每种严重程度的一般建议：

严重性级别	值范围
高	7.0-8.9
<p>严重级别为“高”表示相关资源（一个EC2实例或一组IAM用户登录凭证）已被泄露并被积极用于未经授权的目的。</p> <p>我们建议您优先处理任何“高”严重性的调查发现安全问题，并立即采取补救措施，以防止对您的资源进行其他未经授权的使用。例如，清理或终止您的EC2实例，或者轮换IAM证书。有关更多详细信息，请参阅补救措施。</p>	
中等	4.0-6.9
<p>“中”严重性级别表示偏离正常观察到的行为的可疑活动，根据您的使用案例，可能指示资源被盗用。</p> <p>我们建议您尽可能早调查牵涉的资源。补救措施因资源和调查发现系列而异，但通常情况下，您应寻求确认活动是否已获得授权并与您的使用案例一致。如果您无法确定原因，或者无法确认该活动是否得到授权，则应考虑资源已泄露，并采取补救措施来保护资源。</p> <p>查看“中”严重性级别的调查发现时，需要注意以下事项：</p> <ul style="list-style-type: none"> 检查是否有授权用户安装新的软件，更改了资源的行为（例如，允许高于正常流量，或者在新端口上启用了通信）。 检查是否有授权用户更改了控制面板设置，例如，修改了安全组设置。 在牵涉的资源上运行反病毒扫描，检测未经授权的软件。 验证附加到相关IAM角色、用户、组或一组凭据的权限。可能需要更改或轮换它们。 	
低	1.0-3.9

严重性级别	值范围
“低”严重性级别表示尝试进行的可疑活动未危及您的网络，例如端口扫描或失败的入侵尝试。	
不需要立即采取行动，但此信息值得注意，因为它可能表明有人正在寻找网络中的弱点。	

审查 GuardDuty调查结果

使用以下程序来查看和理解您的 GuardDuty 发现。

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 选择 调查结果，然后选择一个特定的调查发现以查看其详细信息。

每个调查发现的详细信息因调查发现类型、涉及的资源和活动的性质而异。有关可用的调查发现字段的更多信息，请参阅[调查发现详细信息](#)。

3. (可选) 如果要存档某个调查发现，请从调查发现列表中选择该调查发现，然后选择操作菜单。然后选择 Archive (存档)。

从当前下拉菜单中选择存档，即可查看存档的调查发现。

目前，来自 GuardDuty 成员账户的 GuardDuty 用户无法存档调查结果。

Important

如果您使用上述过程将调查发现手动存档，此调查发现的所有后续匹配项（存档完成后生成）将添加到当前调查发现的列表。如果您永远不希望在当前列表中看到此调查发现，可以将其自动存档。有关更多信息，请参阅[抑制规则](#)。

4. (可选) 要下载一个调查发现，请从调查发现列表中选择该调查发现，然后选择 操作 菜单。然后选择 Export (导出)。导出调查结果时，可以看到其完整JSON文档。

Note

在某些情况下，在某些发现生成后 GuardDuty 就会意识到这些发现是误报。GuardDuty 在查找结果中提供置信度字段JSON，并将其值设置为零。这样 GuardDuty 可以让你知道你可以放心地忽略这些发现。

调查发现详细信息

在 Amazon GuardDuty 控制台中，您可以在查找结果摘要部分查看查找详情。调查发现详细信息因调查发现类型而异。

有两类主要详细信息，用于确定哪些类型的信息可用于任何调查发现。第一个是资源类型，可以是 Instance、AccessKeyS3Bucket、S3Object、Kubernetes cluster、ECS cluster、ContainerRDSDBInstance、或 Lambda。决定调查发现信息的第二类详细信息是资源角色。资源角色可以是访问密钥的 Target，这意味着该资源是可疑活动的目标。对于实例类型的调查发现，资源角色也可以是 Actor，这意味着您的资源是进行可疑活动的行动者。本主题介绍调查发现的一些常见可用详细信息。

调查发现概览

调查发现的概览部分包含该调查发现最基本的识别特征，包括以下信息：

- 账户 ID — 发生活动并提示 GuardDuty 生成此调查结果的 AWS 账户的 ID。
- 计数-汇总 GuardDuty 与此发现 ID 匹配此模式的活动的次数。
- 创建时间：首次创建此调查发现的时间和日期。如果此值与更新时间不同，则表示该活动已多次发生，是一个持续的问题。

Note

GuardDuty 控制台中查找结果的时间戳以您的本地时区显示，而 JSON 导出和 CLI 输出显示的时间戳则显示在中。UTC

- 调查发现 ID：此调查发现类型和参数集的唯一标识符。与此模式匹配的新活动实例将聚合到同一 ID 中。
- 调查发现类型：表示触发调查发现的活动类型的格式化字符串。有关更多信息，请参阅 [GuardDuty 查找格式](#)。
- 区域-生成发现的 AWS 区域。有关支持的区域的更多信息，请参阅 [区域和端点](#)。
- 资源 ID — 活动所针对的 AWS 资源的 ID，提示生成 GuardDuty 此调查结果。
- 扫描 ID — 适用于启用 GuardDuty 恶意软件防护时的发现，这是在连接到可能受感染的 EC2 实例或容器工作负载的 EBS 卷上运行的恶意软件扫描的标识符。EC2 有关更多信息，请参阅 [用于 EC2 查找详细信息的恶意软件防护](#)。
- 严重性：为调查发现分配的严重性级别，可以为“高”、“中”或“低”。有关更多信息，请参阅 [GuardDuty 调查结果的严重性级别](#)。

- 更新时间 — 上次更新此发现的时间，新活动与提示生成此发现 GuardDuty的模式相匹配。

资源

“受影响的资源”提供了有关启动活动所针对的 AWS 资源的详细信息。可用信息因资源类型和操作类型而异。

资源角色-启动查找结果的 AWS 资源的角色。此值可以是TARGET或 ACTOR，表示您的资源是可疑活动的目标还是执行可疑活动的行为者。

资源类型：受影响资源的类型。如果涉及多个资源，则调查发现可能包括多种资源类型。资源类型包括实例、S3Bucket AccessKey、S3 Object、、Container KubernetesCluster和 Lambda ECSCluster RDSDBInstance。根据资源类型，将提供不同的调查发现详细信息。选择资源选项卡，了解该资源的可用详细信息。

Instance

实例详细信息：

Note

如果实例已经停止，或者在进行跨API区域调用时，底层API调用来自不同区域的实例，则可能缺少一些EC2实例详细信息。

- 实例 ID — 提示生成调查结果的活动所涉及 GuardDuty 的EC2实例的 ID。
- 实例类型-调查结果中涉及的EC2实例的类型。
- 启动时间：启动实例的日期和时间。
- 前哨基地 ARN — 的亚马逊资源名称 (ARN)。AWS Outposts仅适用于实 AWS Outposts 例。有关更多信息，请参阅[什么是 AWS Outposts ?](#)
- 安全组名称：附加到所涉及实例的安全组的名称。
- 安全组 ID：附加到所涉及实例的安全组的 ID。
- 实例状态：目标实例的当前状态。
- 可用区：相关实例所在的 AWS 区域可用区。
- 映像 ID：Amazon 系统映像的 ID，该系统映像用于构建活动中涉及的实例。
- 映像描述：Amazon 系统映像 ID 的描述，该系统映像用于构建活动中涉及的实例。

- 标签：附加到此资源的标签列表，格式为 key:value。

AccessKey

访问密钥详细信息：

- 访问密钥 ID — 参与提示 GuardDuty 生成调查结果的活动的用户的访问密钥 ID。
- 委托人 ID — 参与提示 GuardDuty 生成调查结果的活动的用户的主人 ID。
- 用户类型-参与活动并提示 GuardDuty 生成调查结果的用户类型。有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。
- 用户名-参与提示 GuardDuty 生成调查结果的活动的用户的姓名。

S3Bucket

Amazon S3 存储桶详细信息：

- 名称：存储桶的名称，在调查发现中包含该存储桶。
- ARN— 调查结果中涉及 ARN 的水桶中的一部分。
- 拥有者：用户的规范用户 ID，该用户拥有调查发现中涉及的存储桶。有关规范用户的更多信息，IDs 请参阅 [AWS 账户](#) 标识符。
- 类型：存储桶调查发现的类型，可以是目标或源。
- 默认服务器端加密：存储桶的加密详细信息。
- 存储桶标签：附加到此资源的标签列表，以 key:value 格式列出。
- 有效权限：评估存储桶上的所有有效权限和策略，指示涉及的存储桶是否公开。值可以是公开，也可以是非公开。

S3Object

- S3 对象详细信息-包括有关扫描的 S3 对象的以下信息：
 - ARN— 扫描的 S3 对象的亚马逊资源名称 (ARN)。
 - 密钥-在 S3 存储桶中创建文件时为其分配的名称。
 - 版本 ID — 启用存储桶版本控制后，此字段表示与扫描的 S3 对象的最新版本关联的版本 ID。有关更多信息，请参阅《Amazon S3 用户指南》中的 [在 S3 存储桶中使用版本控制](#)。
 - eTag— 表示扫描的 S3 对象的特定版本。

- 哈希 — 此发现中检测到的威胁的哈希值。
- S3 存储桶详情 — 包括与扫描的 S3 对象关联的 Amazon S3 存储桶的以下信息：
 - 名称 — 表示包含该对象的 S3 存储桶的名称。
 - ARN— S3 存储桶的亚马逊资源名称 (ARN)。
- 所有者-S3 存储桶所有者的规范 ID。

EKSCluster

Kubernetes 集群详情：

- 名称：Kubernetes 集群名称。
- ARN— 用于标识集群的。
- 创建时间：创建此集群的时间和日期。

Note

GuardDuty 控制台中查找结果的时间戳以您的本地时区显示，而JSON导出和CLI输出显示的时间戳则显示在中。UTC

- VPCID — 与您的集群关联VPC的 ID。
- 状态：集群的当前状态。
- 标签：您应用于集群以帮助您对其进行分类和组织的元数据。每个标签都由一个键和一个可选值组成，以 key:value 格式列出。您可以定义键和值。

集群标签不会应用到与集群关联的任何其他资源。

Kubernetes 工作负载详情：

- 类型：Kubernetes 工作负载的类型，例如容器组、部署和作业。
- 名称：Kubernetes 工作负载的名称。
- Uid：Kubernetes 工作负载的唯一 ID。
- 创建时间：创建此工作负载的日期和时间。
- 标签：附加到 Kubernetes 工作负载的键值对。
- 容器：容器的详细信息，该容器作为 Kubernetes 工作负载的一部分运行。
- 命名空间：工作负载所属的 Kubernetes 命名空间。

- 卷：Kubernetes 工作负载使用的卷。
 - 主机路径：表示卷映射的目标主机上预先存在的文件或目录。
 - 名称：卷的名称。
- 容器组安全上下文：定义容器组中所有容器的权限和访问控制设置。
- 主机网络：如果容器组包含在 Kubernetes 工作负载中，则设置为 true。

Kubernetes 用户详细信息：

- 群组 — 参与生成调查结果的活动所涉及的用户 KubernetesRBAC (基于角色访问权限的控制) 群组。
- ID：Kubernetes 用户的唯一 ID。
- 用户名：Kubernetes 用户的名称，该用户参与生成调查发现的发现。
- 会话名称-以 Kubernetes RBAC 权限担任该IAM角色的实体。

ECSCluster

ECS集群详情：

- ARN— 用于标识ARN识集群的。
- 名称：集群的名称。
- 状态：集群的当前状态。
- 活动服务计数：处于 ACTIVE 状态的集群上运行的服务数量。您可以通过以下方式查看这些服务 [ListServices](#)
- 已注册的容器实例计数：注册到集群中的容器实例数量，包括同时处于 ACTIVE 和 DRAINING 状态的容器实例。
- 正在运行的任务计数：集群中处于 RUNNING 状态的任务数。
- 标签：您应用于集群以帮助您对其进行分类和组织的元数据。每个标签都由一个键和一个可选值组成，以 key:value 格式列出。您可以定义键和值。
- 容器：与任务关联的容器的详细信息：
 - 容器名称：容器的名称。
 - 容器映像：容器的映像。
- 任务详情：集群中任务的详细信息。
 - ARN— 任务的 Amazon 资源名称 (ARN)。

- 定义 ARN — 创建任务的任务定义的 Amazon 资源名称 (ARN)。
- 版本：任务的版本计数器。
- 任务创建时间：创建任务时的 Unix 时间戳。
- 任务开始时间：任务开始时的 Unix 时间戳。
- 任务启动者：任务开始时指定的标签。

Container

容器详细信息：

- 容器运行时：用于运行容器的容器运行时（例如 docker 或 containerd）。
- ID — 容器实例 ID 或容器实例的完整 ARN 条目。
- 名称：容器的名称。

如果可用，该字段将显示标签 `io.kubernetes.container.name` 的值。

- 映像：容器实例的映像。
- 卷挂载：容器卷挂载列表。容器可以在其文件系统下挂载卷。
- 安全上下文：容器安全上下文定义容器的权限和访问控制设置。
- 进程详细信息：描述与调查发现关联的进程的详细信息。

RDSDBInstance

RDSDBInstance 细节：

Note

此资源可在与数据库实例相关的 RDS 保护结果中找到。

- 数据库实例 ID-与 GuardDuty 调查结果中涉及的数据库实例关联的标识符。
- 引擎：数据库实例的数据库引擎名称，在调查发现中包含该实例。可能的值是 Aurora 我的 SQL 兼容或兼容 Aurora Postgre。SQL
- 引擎版本- GuardDuty 调查结果中涉及的数据库引擎的版本。
- 数据库集群 ID-包含 GuardDuty 调查结果中涉及的数据库实例 ID 的数据库集群的标识符。

- 数据库实例 ARN-用于标识 GuardDuty查找结果中涉及的数据库实例。ARN

Lambda

Lambda 函数详细信息

- 函数名称：Lambda 函数的名称，在调查发现中包含该函数。
- 函数版本：Lambda 函数的版本，在调查发现中包含该函数。
- 函数描述：对 Lambda 函数的描述，在调查发现中包含该函数。
- 函数 ARN — 调查结果中涉及的 Lambda 函数的亚马逊资源名称 (ARN)。
- 修订 ID：Lambda 函数版本的修订 ID。
- 角色：Lambda 函数的执行角色，在调查发现中包含该函数。
- VPC配置 — Amazon VPC 配置，包括与您的 Lambda 函数IDs关联的 VPC ID、安全组和子网。
- VPCID — 与调查结果中涉及VPC的 Lambda 函数关联的亚马逊 ID。
- 子网 IDs-与您的 Lambda 函数关联的子网的 ID。
- 安全组：附加到相关 Lambda 函数的安全组。这包括安全组名称和组 ID。
- 标签：附加到此资源的标签列表，以 key:value 格式列出。

RDS数据库 (DB) 用户详细信息

Note

本节适用于在中启用“RDS保护”功能时的发现 GuardDuty。有关更多信息，请参阅 [GuardDuty RDS保护](#)。

GuardDuty 调查结果提供了可能遭到入侵的数据库的以下用户和身份验证详细信息。

- 用户：用于进行异常登录尝试的用户名。
- 应用程序：用于进行异常登录尝试的应用程序名称。
- 数据库：数据库实例的名称，在异常登录尝试中包含此实例。
- SSL— 用于网络的安全套接字层 (SSL) 的版本。
- 身份验证方法：用户使用的身份验证方法，在调查发现中包括该用户。

运行时监控查找详细信息

Note

这些详细信息只有在 GuardDuty 生成其中一个时才可用[运行时监控查找类型](#)。

本节包含运行时详细信息，例如进程详细信息和任何必需的上下文。进程详细信息描述了有关观察到的进程的信息，运行时上下文描述了有关潜在可疑活动的任何其他信息。

进程详细信息

- 名称：进程的名称。
- 可执行文件路径：进程可执行文件的绝对路径。
- 可执行文件 SHA -256-进程可执行文件的SHA256哈希值。
- 命名空间 PID — 除主机级PID命名空间之外的辅助PID命名空间中进程的进程 ID。对于容器内的进程，命名空间 PID 是容器内观察到的进程 ID。
- 当前工作目录：进程的当前工作目录。
- 进程 ID：操作系统分配给进程的 ID。
- startTime— 流程开始的时间。这是UTC日期字符串格式 (2023-03-22T19:37:20.168Z)。
- UUID— 分配给进程的唯一 ID GuardDuty。
- 父进程 UUID-父进程的唯一 ID。此 ID 由分配给父进程 GuardDuty。
- 用户：执行进程的用户。
- 用户 ID：执行进程的用户 ID。
- 有效用户 ID：事件发生时进程的有效用户 ID。
- 谱系：有关进程原级的信息。
 - 进程 ID：操作系统分配给进程的 ID。
 - UUID— 分配给进程的唯一 ID GuardDuty。
 - 可执行文件路径：进程可执行文件的绝对路径。
 - 有效用户 ID：事件发生时进程的有效用户 ID。
 - 父进程 UUID-父进程的唯一 ID。此 ID 由分配给父进程 GuardDuty。
 - 开始时间：进程启动的时间。
 - 命名空间 PID — 除主机级PID命名空间之外的辅助PID命名空间中进程的进程 ID。对于容器内的进程，命名空间 PID 是容器内观察到的进程 ID。

- 用户 ID：执行进程用户的用户 ID。
- 名称：进程的名称。

运行时上下文

在以下字段中，生成的调查发现可能仅包含与调查发现类型相关的字段。

- 挂载源：被容器挂载的主机上的路径。
- 挂载目标：容器中映射到主机目录的路径。
- 文件系统类型：表示已挂载文件系统的类型。
- 标志：表示控制事件行为的选项，在此调查发现中包含该事件。
- 修改进程：有关运行时在容器内创建或修改二进制文件、脚本或库的进程的信息。
- 修改时间：进程运行时在容器内创建或修改二进制文件、脚本或库的时间戳。此字段采用UTC日期字符串格式 (2023-03-22T19:37:20.168Z)。
- 库路径：已加载的新库的路径。
- LD 预加载值：LD_PRELOAD 环境变量的值。
- 套接字路径：被访问的 Docker 套接字的路径。
- Runc 二进制文件路径：runc 二进制文件的路径。
- 版本代理路径：cgroup 版本代理文件的路径。
- 命令行示例-潜在可疑活动所涉及的命令行示例。
- 工具类别-工具所属的类别。其中一些示例包括后门工具、Pentest 工具、网络扫描器和网络嗅探器。
- 工具名称-可能可疑的工具的名称。
- 脚本路径-生成结果的已执行脚本的路径。
- 威胁文件路径-找到威胁情报详细信息的可疑路径。
- 服务名称-已禁用的安全服务的名称。

EBS卷扫描详细信息

Note

本节适用于开启 GuardDuty启动的恶意软件扫描时发现的结果。[恶意软件防护 EC2](#)

EBS卷扫描提供有关连接到可能受损的EC2实例或容器工作负载的EBS卷的详细信息。

- 扫描 ID：恶意软件扫描的标识符。
- 扫描开始时间：开始恶意软件扫描的日期和时间。
- 扫描完成时间：完成恶意软件扫描的日期和时间。
- 触发器查找 ID — 启动此恶意软件扫描的 GuardDuty 发现的查找 ID。
- 来源-潜在值为Bitdefender和Amazon。
- 扫描检测：每次恶意软件扫描的详细信息和结果的完整视图。
 - 已扫描项目数：已扫描文件的总数。提供例如 totalGb、files 和 volumes 的详细信息。
 - 检测到的威胁项目数：扫描期间检测到的恶意 files 总数。
 - 最高严重性威胁详细信息：扫描期间检测到的最高严重性威胁的详细信息，以及恶意文件数量。提供例如 severity、threatName 和 count 的详细信息。
 - 检测到的威胁（按名称）：对所有严重性级别的威胁进行分组的容器元素。提供例如 itemCount、uniqueThreatNameCount、shortened 和 threatNames 的详细信息。

用于EC2查找详细信息的恶意软件防护

Note

本节适用于开启 GuardDuty启动的恶意软件扫描时发现的结果。[恶意软件防护 EC2](#)

当用于EC2扫描的恶意软件防护检测到恶意软件时，您可以通过在<https://console.aws.amazon.com/guardduty/>控制台的“发现”页面上选择相应的发现结果来查看扫描详细信息。用于EC2发现的恶意软件防护的严重程度取决于 GuardDuty发现的严重程度。

Note

GuardDutyFindingDetected 标签指定快照包含恶意软件。

详细信息面板的检测到的威胁部分，提供以下信息。

- 名称：威胁的名称，该名称通过将文件按检测结果分组获得。
- 严重性：检测到的威胁的严重性。

- 哈希 — 文件的 SHA -256。
- 文件路径-EBS 卷中恶意文件的位置。
- 文件名称：检测出威胁的文件的名称。
- 体积 ARN-扫描ARN的EBS卷。

详细信息面板的恶意软件扫描详细信息部分，提供以下信息。

- 扫描 ID：恶意软件扫描的扫描 ID。
- 扫描开始时间：开始扫描的日期和时间。
- 扫描完成时间：完成扫描的日期和时间。
- 扫描的文件：扫描的文件和目录的总数。
- 扫描总量 (GB)：扫描过程中扫描的存储量。
- 触发查找 ID — 启动此恶意软件扫描的 GuardDuty 发现的查找 ID。
- 详细信息面板的卷详细信息部分，提供以下信息。
 - 卷 ARN-卷的亚马逊资源名称 (ARN)。
 - 快照 ARN-EBS 卷快照ARN的快照。
 - 状态：卷的扫描状态，例如 Running、Skipped 和 Completed。
 - 加密类型：用于给卷加密的加密类型。例如，CMCMK。
 - 设备名称：设备的名称。例如，/dev/xvda。

S3 恶意软件防护查找详情

当您在中同时启用 S3 GuardDuty 和“恶意软件防护”时，以下恶意软件扫描详细信息可用 AWS 账户：

- 威胁-恶意软件扫描期间检测到的威胁列表。

有关调查结果可能包含的威胁数量的信息，请参阅[S3 恶意软件防护配额](#)。

- 项目路径-已扫描 S3 对象的嵌套项目路径和哈希详细信息的列表。
 - 嵌套项目路径-检测到威胁的已扫描 S3 对象的项目路径。

只有当顶级对象是档案并且在档案内检测到威胁时，此字段的值才可用。

- 哈希 — 此发现中检测到的威胁的哈希值。
- 来源-潜在值为Bitdefender和Amazon。

操作

调查发现的操作提供触发调查发现的活动类型的详细信息。可用信息因操作类型而异。

操作类型：调查发现活动类型。此值可以是 NETWORKPORT_CONNECTION_PROBE、DNS_REQUEST、AWSAPI_CALL、_ 或 RDSLOGIN_ATTEMPT。可用信息因操作类型而异：

- NETWORK_CONNECTION — 表示已识别的EC2实例和远程主机之间交换了网络流量。此操作类型具有以下额外信息：
 - 连接方向-在提示生成结果的活动中观察到 GuardDuty 的网络连接方向。它可以是以下值之一：
 - INBOUND— 表示远程主机启动了与您账户中已识别EC2实例上的本地端口的连接。
 - OUTBOUND— 表示已识别的EC2实例启动了与远程主机的连接。
 - UNKNOWN— 表示 GuardDuty 无法确定连接方向。
 - 协议-在提示生成调查结果的活动中观察 GuardDuty 到的网络连接协议。
 - 本地 IP：触发调查发现的流量的原始源 IP 地址。此信息可用于区分流量流经的中间层的 IP 地址与触发调查发现的流量的原始源 IP 地址。例如，EKSPod 的 IP 地址与运行 Po EKS d 的实例的 IP 地址对比。
 - 已阻止：指示目标端口是否被阻止。
- PORT_PROBE — 表示远程主机在多个打开的端口上探测了已识别的EC2实例。此操作类型具有以下额外信息：
 - 本地 IP：触发调查发现的流量的原始源 IP 地址。此信息可用于区分流量流经的中间层的 IP 地址与触发调查发现的流量的原始源 IP 地址。例如，EKSPod 的 IP 地址与运行 Po EKS d 的实例的 IP 地址对比。
 - 已阻止：指示目标端口是否被阻止。
- DNS_REQUEST — 表示已识别的EC2实例查询了域名。此操作类型具有以下额外信息：
 - 协议-在提示生成调查结果的活动中观察 GuardDuty 到的网络连接协议。
 - 已阻止：指示目标端口是否被阻止。
- AWS_API_CALL — 表示 AWS API已调用。此操作类型具有以下额外信息：
 - API— 被调用并因此被提示生成此结果 GuardDuty 的API操作的名称。

Note

这些操作还可能包括由捕获的非API事件 AWS CloudTrail。有关更多信息，请参阅[捕获的非API事件 CloudTrail](#)。

- 用户代理-API 发出请求的用户代理。此值告诉您呼叫是从 AWS Management Console、AWS 服务 AWS SDKs、还是 AWS CLI。
- ERRORCODE— 如果发现是由失败的API呼叫触发的，则会显示该呼叫的错误代码。
- 服务名称-尝试拨打触发查找结果的API呼叫的服务的DNS名称。
- RDS_LOGIN _ ATTEMPT — 表示有人尝试从远程 IP 地址登录到可能受到威胁的数据库。
- IP 地址：用于进行潜在可疑登录尝试的远程 IP 地址。

行动者或目标

如果资源角色是 TARGET，则调查发现会有行动者部分。这表示您的资源是可疑活动的目标，并且行动者部分包含针对您资源的实体的详细信息。

如果资源角色是 ACTOR，则调查发现会有目标部分。这表示您的资源参与了针对远程主机的可疑活动，且该部分包含有关资源所针对的 IP 或域的信息。

行动者或目标部分中可用的信息包括以下内容：

- 附属机构-有关远程API呼叫者的 AWS 帐户是否与您的 GuardDuty 环境相关的详细信息。如果此值为 true，则表示API来电者以某种方式关联到您的帐户；如果 false，API来电者来自您的环境之外。
- 远程帐户 ID — 拥有用于访问最终网络资源的出站 IP 地址的帐户 ID。
- IP 地址-提示 GuardDuty 生成调查结果的活动中的涉及的 IP 地址。
- 位置-提示 GuardDuty 生成调查结果的活动所涉及的 IP 地址的位置信息。
- ISP组织 — 提示 GuardDuty 生成调查结果的活动所涉及的 IP 地址的组织信息。
- 端口 — 提示 GuardDuty 生成查找结果的活动所涉及的端口号。
- 域-提示 GuardDuty 生成调查结果的活动所涉及的域。
- 带后缀的域-可能提示 GuardDuty 生成调查结果的活动中的涉及的第二和顶级域名。有关顶级和二级域名的列表，请参阅[公共后缀](#)列表。

其他信息

调查发现的额外信息部分，包括以下信息：

- 威胁列表名称-威胁列表的名称，其中包括提示 GuardDuty 生成发现的活动所涉及的 IP 地址或域名。

- 示例：true 或 false 值，指示此项否为示例调查发现。
- 已存档：true 或 false 值，指示此调查发现是否已存档。
- 不常见：过去未观察到的活动详细信息。这些可能包括异常（以前未观察到的）用户、位置、时间、存储桶、登录行为或ASN组织。
- 异常协议-提示生成调查结果的活动过程中涉及 GuardDuty 的网络连接协议。
- 代理详细信息-有关当前部署在您的EKS集群上的安全代理的详细信息 AWS 账户。这仅适用于“EKS运行时监控”查找类型。
 - 代理版本- GuardDuty 安全客户端的版本。
 - 代理 ID- GuardDuty 安全代理的唯一标识符。

证据

基于威胁情报的调查发现包括证据部分，其中包含以下信息：

- 威胁情报详细信息-Threat name 显示已识别的威胁列表的名称。
- 威胁名称-恶意软件系列的名称或与威胁相关的其他标识符。
- 威胁文件 SHA256 — SHA256 生成发现的文件。

异常行为

结尾为的发现类型AnomalousBehavior表示发现是由 GuardDuty 异常检测机器学习 (ML) 模型生成的。机器学习模型会评估对您账户的所有API请求，并识别与对手使用的策略相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的地点以及请求API的具体内容。

有关请求中哪些因素对于调用该API请求的 CloudTrail 用户身份来说不寻常的详细信息，可以在调查结果详细信息中找到。恒等式由 [CloudTrail userIdentity 元素](#) 定义，可能的值为：Root、IAMUser、AssumedRoleFederatedUser、AWSAccount、或AWSService。

除了与API活动相关的所有 GuardDuty 发现的详细信息外，AnomalousBehavior调查结果还有其他详细信息，将在下一节中概述。这些详细信息可以在控制台中查看，也可以在调查结果中找到JSON。

- Anomalous APIs — 用户身份在与调查结果关联的主要API请求附近调用的请求列表。API此窗格通过以下方式进一步细分了API事件的详细信息。
 - API列出的第一个是主API请求API，即与观察到的风险最高的活动相关的请求。这是触发API发现的原因，并且与发现类型的攻击阶段相关。这也是控制台的“操作”部分和调查结果中详细介绍的JSON。API

- APIs列出的任何其他用户身份都是在主要用户附近观察APIs到的列出用户身份中的其他异常情况。API如果列表中只有一个API，则机器学习模型不会将来自该用户身份的任何其他API请求识别为异常请求。
- 列表APIs是根据调用成功还是调用失败（即API已收到错误响应）来划分的。API接收到的错误响应类型列在每个未成功调用的API错误响应的上方。可能的错误响应类型有：`access denied`、`access denied exception`、`auth failure`、`instance limit exceeded`、`invalid permission - duplicate`、`invalid permission - not found`、和 `operation not permitted`。
- APIs按其相关服务分类。
- APIs要了解更多背景信息，请选择 `Historical` 以查看有关顶部APIs内容的详细信息，最多 20 个，通常同时显示用户身份和账户内所有用户。根据您的账户中的使用频率，分别标记为“稀APIs有”（每月少于一次）、“不频繁”（每月几次）或“频繁”（从每天到每周）。
- 异常行为（账户）：本部分提供有关您账户的已剖析行为的更多详细信息。

已分析的行为

GuardDuty 根据已交付的事件持续了解您账户中的活动。这些活动及其观察到的频率被称为剖析行为。

此面板中跟踪的信息包括：

- ASN组织 — 发出异常API呼叫的ASN组织。
- 用户名-发出异常API呼叫的用户的姓名。
- 用户代理 — 用于进行异常呼叫的用户代理。API用户代理是用于发出调用的方法，例如 `aws-cli` 或 `Botocore`。
- 用户类型-发出异常API呼叫的用户类型。可能的值为 `AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER` 或 `ROLE`。
- 存储桶：正在经受访问的 S3 存储桶的名称。
- 异常行为（用户身份）：本部分提供了有关调查发现所涉及的用户身份剖析行为的更多详细信息。当某项行为未被识别为历史行为时，这意味着 GuardDuty ML 模型以前没有看到此用户身份在训练期间以这种方式进行API调用。有关用户身份的以下其他详细信息可用：
 - ASN组织 — 发出异常API呼叫的ASN组织。
 - 用户代理 — 用于进行异常呼叫的用户代理。API用户代理是用于发出调用的方法，例如 `aws-cli` 或 `Botocore`。

- 存储桶：正在经受访问的 S3 存储桶的名称。
- 不常见行为（存储桶）：本部分提供与调查发现关联的 S3 存储桶已剖析行为的更多详细信息。当某项行为未被识别为历史行为时，这意味着 GuardDuty ML 模型以前在训练期内从未见过以这种方式对该存储桶进行的API调用。此部分中跟踪的信息包括：
 - ASN组织 — 发出异常API呼叫的ASN组织。
 - 用户名-发出异常API呼叫的用户的姓名。
 - 用户代理 — 用于进行异常呼叫的用户代理。API用户代理是用于发出调用的方法，例如 `aws-cli` 或 `Botocore`。
 - 用户类型-发出异常API呼叫的用户类型。可能的值为 `AWS_SERVICE`、`ASSUMED_ROLE`、`IAM_USER` 或 `ROLE`。

Note

有关历史行为的更多上下文，请在不常见行为（账户）、用户 ID 或存储桶部分中，选择历史行为，查看有关您账户中以下每个类别的预期行为的详细信息：稀有（每月少于一次）、不频繁（每月几次）或频繁（每天到每周），具体取决于在您账户中的使用频率。

- 不常见行为（数据库）：本部分提供有关数据库实例剖析行为的更多详细信息，该实例与调查发现相关联。如果某项行为未被识别为历史行为，则意味着 GuardDuty ML 模型在训练期内未曾尝试以这种方式登录该数据库实例。在调查发现面板中针对此部分跟踪的信息包括：
 - 用户名：用于进行异常登录尝试的用户名。
 - ASN组织 — 进行异常登录尝试的ASN组织。
 - 应用程序名称：用于进行异常登录尝试的应用程序名称。
 - 数据库名称：数据库实例的名称，在异常登录尝试中包含该实例。

“历史行为”部分提供了有关先前观察到的关联数据库的用户名、ASN组织、应用程序名称和数据库名称的更多背景信息。每个唯一值都有一个关联的计数，表示在成功登录事件中观察到该值的次数。

- 异常行为（账户 Kubernetes 集群、Kubernetes 命名空间和 Kubernetes 用户名）— 本节提供了有关与发现结果关联的 Kubernetes 集群和命名空间的分析行为的更多详细信息。如果某项行为未被识别为历史行为，则意味着 GuardDuty ML 模型以前未以这种方式观察到此账户、集群、命名空间或用户名。在调查发现面板中针对此部分跟踪的信息包括：
 - 用户名 — 调用与搜索结果API关联的 Kubernetes 的用户。
 - 冒充的用户名-被冒充的用户。username
 - 命名空间 — 发生操作的亚马逊EKS集群中的 Kubernetes 命名空间。

- 用户代理 — 与 Kubernetes API 调用关联的用户代理。用户代理是用于进行呼叫的方法，例如 `kubectl`。
- API — 在亚马逊集群中 API 调用的 Kubernetes username。EKS
- ASN 信息 - 与进行此呼叫的用户的 IP 地址相关的 ASN 信息，例如组织和 ISP。
- 一周中的某一天 — 一周中发出 Kubernetes API 调用的那一天。
- 权限 — 正在检查访问权限的 Kubernetes 动词和资源，以指示他们是否 username 可以使用 Kubernetes。API
- 服务帐户名称 — 与 Kubernetes 工作负载关联的服务帐户，为工作负载提供身份。
- 注册表 — 与 Kubernetes 工作负载中部署的容器镜像关联的容器注册表。
- 镜像 — 部署在 Kubernetes 工作负载中的容器镜像，不带相关标签和摘要。
- Image Prefix Config — 使用镜像的容器启用了容器和工作负载安全配置的镜像前缀 `privileged`，例如 `hostNetwork` 或。
- 主题名称 - 绑定到或 `serviceAccountName` 中参考角色的主题，例如 `group`、`RoleBinding` 或 `ClusterRoleBinding`。user
- 角色名称 - 创建或修改角色所涉及的角色名称或 `roleBindingAPI`。

基于 S3 卷的异常

本节详细介绍基于 S3 卷的异常的上下文信息。基于卷的发现 ([Exfiltration:S3/AnomalousBehavior](#)) 监视用户对 S3 存储桶发出的异常数量的 S3 API 调用，这表明存在潜在的数据泄露。监控以下 S3 API 调用以进行基于卷的异常检测。

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

以下指标将有助于建立 IAM 实体访问 S3 存储桶时的通常行为的基准。为了检测数据泄露，基于卷的异常检测调查发现会根据常见的行为基准评估所有活动。在不常见行为 (用户身份)、观测到的卷 (用户身份) 和观测到的卷 (存储桶) 部分中，选择历史行为，以分别查看以下指标。

- 在过去 24 小时内，与受影响的 S3 存储桶关联的 IAM 用户或 IAM 角色 `s3-api-name` API 调用的次数 (取决于发出的是哪个调用)。
- 在过去 24 小时内，IAM 用户或 IAM 角色 `s3-api-name` API 调用的与所有 S3 存储桶关联的呼叫数 (取决于发出的呼叫是哪个)。

- 过去 24 小时内所有 IAM 用户或 IAM 角色中与受影响的 S3 存储桶关联的 s3-api-name API 调用数量（取决于发出的呼叫是哪一个）。

RDS 基于登录活动的异常

本节详细说明了不常见行动者执行的登录尝试次数，并按登录尝试的结果进行分组。[RDS 保护查找类型](#) 通过监控登录事件中是否存在 `successfulLoginCount`、`failedLoginCount` 和 `incompleteConnectionCount` 的不常见模式，来识别异常行为。

- `successfulLoginCount`— 此计数器表示异常行为者成功连接到数据库实例的总和（登录属性的正确组合）。登录属性包括用户名、密码和数据库名称。
- `failedLoginCount`— 此计数器表示为建立与数据库实例的连接而进行的失败（失败）登录尝试的总和。这表明登录组合的一个或多个属性（例如用户名、密码或数据库名称）不正确。
- `incompleteConnectionCount`— 此计数器表示无法归类为成功或失败的连接尝试次数。这些连接在数据库提供响应之前就已关闭。例如，在端口扫描中已连接数据库端口，但没有向数据库发送任何信息，或者在成功或失败的尝试中，连接在登录完成前中止。

GuardDuty 查找聚合

所有发现都是动态的，这意味着，如果 GuardDuty 检测到与相同安全问题相关的新活动，它将使用新信息更新原始发现结果，而不是生成新的发现。此行为可使您能够识别正在发生的问题，而无需浏览多个类似报告，并减少来自您已发现的安全问题的总体噪音。

例如，对于 `UnauthorizedAccess:EC2/SSHBruteForce` 调查发现，针对实例的多次访问尝试将聚合到同一调查发现 ID，从而增加调查发现详细信息中的计数。这是因为该发现代表了一个安全问题，该实例表明该实例上的 SSH 端口没有得到适当的保护，无法抵御此类活动。但是，如果在您的环境中 GuardDuty 检测到针对新实例的 SSH 访问活动，它将创建一个带有唯一查找 ID 的新发现，提醒您存在与新资源相关的安全问题。

聚合调查发现后，系统会根据该活动最近一次发生的信息进行更新。这意味着，在上面的示例中，如果您的实例是新攻击者的暴力攻击目标，则调查发现的详细信息将会更新，以反映最新源的远程 IP 信息，并且旧信息将被替换。您的 CloudTrail 或 VPC Flow Logs 中仍将提供有关个人活动尝试的完整信息。

提醒 GuardDuty 生成新查找结果而不是汇总现有查找结果的标准取决于查找结果类型。每种调查发现类型的聚合标准均由我们的安全工程师确定，以便为您提供账户中各种安全问题的最佳概述。

调查发现类型

有关对 GuardDuty 查找结果类型进行重要更改（包括新添加或已停用的查找类型）的信息，请参见 [Amazon 的文档历史记录 GuardDuty](#)。

有关查找现已停用的类型的信息，请参阅 [停用调查结果类型](#)。

GuardDuty EC2 查找类型

以下调查发现专门针对 Amazon EC2 资源，以及始终具有 Instance 的资源类型。调查发现的严重性和详细信息因资源角色而异，指示 EC2 资源是可疑活动的目标还是执行活动的威胁行为者。

此处列出的调查发现包括用于生成该调查发现类型的数据来源和模型。有关数据来源和模型的更多信息，请参阅 [GuardDuty 基础数据源](#)。

Note

如果实例已经终止，或者底层 API 调用是跨区域 API 调用（源自不同区域的 EC2 实例）的一部分，则某些 EC2 调查发现可能缺失实例详细信息。

对于所有 EC2 调查发现，建议您检查相关资源以确定其行为是否符合预期。如果活动已获得授权，则可以使用抑制规则或可信 IP 列表，来防止该资源的误报通知。如果活动是意外活动，则安全的最佳实践是假定实例已被盗用，并执行 [修复可能遭到入侵的 Amazon 实例 EC2](#) 中详述的操作。

主题

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.BIDNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)

- [Behavior:EC2/NetworkPortUnusual](#)
- [Behavior:EC2/TrafficVolumeUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)
- [Recon:EC2/PortProbeEMRUnprotectedPort](#)
- [Recon:EC2/PortProbeUnprotectedPort](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/MetadataDNSRebind](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)

- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)

Backdoor:EC2/C&CActivity.B

EC2 实例正在查询与已知命令和控制服务器关联的 IP。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的实例，正在查询与已知命令和控制（C&C）服务器关联的 IP。列出的实例可能被盗用。命令和控制服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是感染了相同类型恶意软件，并受其控制的一组连接到互联网的设备（其中可能包括 PC、服务器、移动设备和物联网设备）。僵尸网络通常用于分发恶意软件和收集不当信息，例如信用卡号。根据僵尸网络的用途和结构，命令和控制服务器也可以发布命令来启动分布式拒绝服务（DDoS）攻击。

Note

如果查询的 IP 与 log4j 相关，则相关调查发现的字段将包含以下值：

- 服务。附加信息。threatListName = 亚马逊
- service.additionalInfo.threatName = Log4j Related

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Backdoor:EC2/C&CActivity.B!DNS

EC2 实例正在查询与已知命令和控制服务器关联的域名。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的实例，正在查询与已知命令和控制 (C&C) 服务器关联的域名。列出的实例可能被盗用。命令和控制服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是感染了相同类型恶意软件，并受其控制的一组连接到互联网的设备（其中可能包括 PC、服务器、移动设备和物联网设备）。僵尸网络通常用于分发恶意软件和收集不当信息，例如信用卡号。根据僵尸网络的用途和结构，命令和控制服务器也可以发布命令来启动分布式拒绝服务 (DDoS) 攻击。

Note

如果查询的域名与 log4j 相关，则相关调查发现的字段将包含以下值：

- 服务。附加信息。threatListName = 亚马逊
- service.additionalInfo.threatName = Log4j Related

Note

要测试如何 GuardDuty 生成此发现类型，您可以针对测试域从您的实例（使用 dig 适用于 Linux 或 nslookup Windows）发出 DNS 请求 guarddutyec2activityb.com。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。


Backdoor:EC2/DenialOfService.Dns

EC2 实例的行为方式可能表明该实例正被用于使用 DNS 协议执行拒绝服务 (DoS) 攻击。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在生成大量出站 DNS 流量。这可能表明列出的实例已遭到入侵，并被用来使用 DNS 协议执行 denial-of-service (DoS) 攻击。

 Note

此调查发现仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。


Backdoor:EC2/DenialOfService.Tcp

EC2 实例的行为方式表明该实例正被用于使用 TCP 协议执行拒绝服务 (DoS) 攻击。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您的 AWS 环境中列出的 EC2 实例，正在生成大量出站 TCP 流量。这可能表明该实例已遭到入侵并被用来使用 TCP 协议执行 denial-of-service (DoS) 攻击。

 Note

此调查发现仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。


Backdoor:EC2/DenialOfService.Udp

EC2 实例的行为方式表明该实例正被用于使用 UDP 协议执行拒绝服务 (DoS) 攻击。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在生成大量出站 UDP 流量。这可能表明列出的实例已遭到入侵，并被用来使用 UDP 协议执行 denial-of-service (DoS) 攻击。

 Note

此调查发现仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。


Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 实例的行为方式可能表明该实例正被用于在 TCP 端口上使用 UDP 协议执行拒绝服务 (DoS) 攻击。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在生成大量出站 UDP 流量，该流量针对通常用于 TCP 通信的端口。这可能表明列出的实例已遭到入侵，并被用来在 TCP 端口上使用 UDP 协议执行 denial-of-service (DoS) 攻击。

 Note

此调查发现仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 实例的行为方式可能表明该实例正被用于使用不寻常协议执行拒绝服务 (DoS) 攻击。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例正在生成大量来自异常协议类型的出站流量，EC2 实例通常不会使用该协议类型，例如 Internet 组管理协议。这可能表明该实例已遭到入侵，并被用来使用异常协议执行 denial-of-service (DoS) 攻击。此调查发现仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Backdoor:EC2/Spambot

EC2 实例表现出不正常的行为，在端口 25 上与远程主机通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例在端口 25 上与远程主机通信。这是异常行为，因为此 EC2 实例以前没有在端口 25 上通信的历史记录。端口 25 通常由电子邮件服务器用于 SMTP 通信。此调查结果表明 EC2 实例可能已遭盗用，并被用于发送垃圾邮件。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Behavior:EC2/NetworkPortUnusual

EC2 实例在异常服务器端口上与远程主机通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例表现出的行为，偏离了所建立的基准。此 EC2 实例以前没有在该远程端口上通信的历史记录。

Note

如果 EC2 实例通过端口 389 或端口 1389 进行通信，则关联的调查发现严重级别将修改为“高”，并且调查发现字段将包含以下值：

- `service.additionalInfo.context = Possible log4j callback`

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Behavior:EC2/TrafficVolumeUnusual

EC2 实例正在生成异常大量的网络流量到远程主机。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例表现出的行为，偏离了所建立的基准。此 EC2 实例以前没有发送这种大量流量到该远程主机的历史记录。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

CryptoCurrency:EC2/BitcoinTool.B

EC2 实例正在查询与加密货币相关活动关联的 IP 地址。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在查询与比特币或其他加密货币相关活动关联的 IP 地址。比特币是一种全球性的加密货币和数字支付系统，可以兑换成其他货币、产品和服务。比特币是比特币挖矿的奖励，受到威胁行为者的高度追捧。

修复建议：

如果您使用此 EC2 实例挖掘或管理加密货币，或此实例涉及区块链活动，则该调查发现可能是您环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 CryptoCurrency:EC2/BitcoinTool.B。第二个筛选条件应是实例的实例 ID，该实例涉及区块链活动。要了解有关创建抑制规则的更多信息，请参阅 [抑制规则](#)。

如果此活动是意外活动，则您的实例可能被盗用，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 实例正在查询与加密货币相关活动关联的域名。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在查询与比特币或其他加密货币相关活动关联的域名。比特币是一种全球性的加密货币和数字支付系统，可以兑换成其他货币、产品和服务。比特币是比特币挖矿的奖励，受到威胁行为者的高度追捧。

修复建议：

如果您使用此 EC2 实例挖掘或管理加密货币，或此实例涉及区块链活动，则该调查发现可能是您环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 `CryptoCurrency:EC2/BitcoinTool.B!DNS`。第二个筛选条件应是实例的实例 ID，该实例涉及区块链活动。要了解有关创建抑制规则的更多信息，请参阅 [抑制规则](#)。

如果此活动是意外活动，则您的实例可能被盗用，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

DefenseEvasion:EC2/UnusualDNSResolver

Amazon EC2 实例正在与异常的公有 DNS 解析器通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例表现出的行为，偏离了基准行为。此 EC2 实例最近没有与该公有 DNS 解析器通信的历史记录。GuardDuty 控制台中查找详细信息面板中的“异常”字段可以提供有关所查询的 DNS 解析器的信息。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 实例正在执行异常的 DNS over HTTPS (DoH) 通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例表现出的行为，偏离了所建立的基准。此 EC2 实例没有任何与该公共 DoH 服务器进行 DNS over HTTPS (DoH) 通信的最新历史记录。调查发现详细信息中的异常字段，可提供有关所查询的 DoH 服务器的信息。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 实例正在执行异常的 DNS over TLS (DoT) 通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例表现出的行为，偏离了所建立的基准。此 EC2 实例没有任何与该公共 DoT 服务器进行 DNS over TLS (DoT) 通信的最新历史记录。调查发现详细信息面板中的异常字段，可提供有关所查询的 DoT 服务器的信息。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/AbusedDomainRequest.Reputation

EC2 实例正在查询与已知滥用域关联的低信誉域名。

默认严重级别：中

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例，正在查询与已知滥用域或滥用 IP 地址相关联的低信誉域。滥用域的示例：提供免费子域注册的顶级域名 (TLD) 和二级域名 (2LD)，以及动态 DNS 提供商。威胁行为者往往利用这些服务免费或低成本注册域名。这类低信誉域也可能是解析到注册商 Parking IP 地址的过期域，因此可能不再处于活跃状态。Parking IP 是注册商为未链接到任何服务的域引导流量的位置。由于威胁行为者通常使用这些注册商或服务进行 C&C 和恶意软件分发，因此列出的 Amazon EC2 实例可能会被盗用。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 实例正在查询与加密货币相关活动关联的低信誉域名。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例，正在查询与比特币或其他加密货币相关活动相关联的低信誉域名。比特币是一种全球性的加密货币和数字支付系统，可以兑换成其他货币、产品和服务。比特币是比特币挖矿的奖励，受到威胁行为者的高度追捧。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

修复建议：

如果您使用此 EC2 实例挖掘或管理加密货币，或此实例涉及区块链活动，则该调查发现可能表示您环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 Impact:EC2/BitcoinDomainRequest.Reputation。第二个筛选条件应是实例的实例 ID，该实例涉及区块链活动。要了解有关创建抑制规则的更多信息，请参阅 [抑制规则](#)。

如果此活动是意外活动，则您的实例可能被盗用，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 实例正在查询与已知恶意域关联的低信誉域。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例，正在查询与已知恶意域或恶意 IP 地址相关联的低信誉域。例如，域可能与已知的陷穴 IP 地址相关联。Sinkholed 域是以前由威胁行为者控制的域，如果向该域发出请求则可能表明该实例已被盗用。这些域也可能与已知的恶意活动或域生成算法相关。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/PortSweep

EC2 实例正在探测大量 IP 地址上的端口。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在探测大量公开可路由 IP 地址上的端口。此类活动通常用于查找易受攻击的主机。在 GuardDuty 控制台的查找详细信息面板中，仅显示最新的远程 IP 地址

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 实例正在查询低信誉域名，该域名由于过时或受欢迎程度低而具有可疑性。

默认严重级别：低

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 Amazon EC2 实例，正在查询疑似恶意的低信誉域名。我们注意到该域的特征与之前观察到的恶意域一致，但我们的信誉模型无法将其与已知威胁明确关联起来。这些域通常是新近观察到的，或者接收到的流量较少。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Impact:EC2/WinRMBruteForce

EC2 实例正在执行出站 Windows 远程管理暴力攻击。

默认严重级别：低*

Note

如果您的 EC2 实例是暴力攻击的目标，则此调查发现的严重级别为“低”。如果您的 EC2 实例是用于执行暴力攻击的攻击者，则此调查发现的严重级别为“高”。

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在执行 Windows 远程管理 (WinRM) 暴力攻击，目的是在基于 Windows 的系统上访问 Windows 远程管理服务。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Recon:EC2/PortProbeEMRUnprotectedPort

已知恶意主机在探测 EC2 实例的一个未受保护的 EMR 相关端口。

默认严重级别：高

- 数据来源：VPC 流日志

这一发现告诉您，列出的 EC2 实例上与 EMR 相关的敏感端口是 AWS 您环境中集群的一部分，未被安全组、访问控制列表 (ACL) 或主机上的防火墙（例如 Linux IPTables）阻止。这一发现还表明，Internet 上的已知扫描仪正在积极探测此端口。可触发此调查发现的端口可能被用于远程代码执行，例如端口 8088（YARN Web UI 端口）。

修复建议：

您应阻止集群上的端口接受来自 Internet 的公开访问，并将访问限制为必须访问这些端口的特定 IP 地址。有关更多信息，请参阅 [EMR 集群的安全组](#)。

Recon:EC2/PortProbeUnprotectedPort

已知恶意主机在探测 EC2 实例的一个未受保护端口。

默认严重级别：低*

Note

此调查发现的默认严重级别为“低”。但是，如果 Elasticsearch 使用正在探测的端口（9200 或 9300），则发现的严重性为“高”。

- 数据来源：VPC 流日志

此调查发现通知您，您的 AWS 环境中列出的 EC2 实例上的端口，未受到安全组、访问控制列表（ACL）或主机上防火墙（例如，Linux IPTables）的阻止，Internet 上的已知扫描程序正在积极地探测该端口。

如果确定的未受保护端口为 22 或 3389，并且您正在使用这些端口来连接到您的实例，则您仍可以将对这些端口的访问限制为您公司网络 IP 地址范围内的 IP 地址，从而限制暴露。要在 Linux 上限制对端口 22 的访问，请参阅[为您的 Linux 实例授权入站流量](#)。要在 Windows 上限制对端口 3389 的访问，请参阅[Windows 实例授权入站流量](#)。

GuardDuty 不会为端口 443 和 80 生成此结果。

修复建议：

这可能是有意暴露实例的情况，例如，在它们托管 Web 服务器时。如果您的 AWS 环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 Recon:EC2/PortProbeUnprotectedPort。第二个筛选条件应与用作堡垒主机的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工具的实例可识别哪些条件。有关创建抑制规则的更多信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的实例可能被盗用，请参阅[修复可能遭到入侵的 Amazon 实例 EC2](#)。

Recon:EC2/Portscan

EC2 实例正在执行对远程主机的出站端口扫描。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，参与到可能的端口扫描攻击中，因为此实例在短时间内尝试连接到多个端口。端口扫描攻击的目的是找出开放端口，用于发现机器运行何种服务以及确定其操作系统。

修复建议：

当漏洞评估应用程序部署在您环境中的 EC2 实例上时，此调查发现可能是误报的，因为这些应用程序会执行端口扫描，以提醒您注意错误配置的开放端口。如果您的 AWS 环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 Recon:EC2/Portscan。第二个筛选条件应与托管这些漏洞评估工具的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工具的实例可识别哪些条件。有关创建抑制规则的更多信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的实例可能被盗用，请参阅[修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/BlackholeTraffic

EC2 实例正在尝试与作为已知黑洞的远程主机的 IP 地址进行通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例可能被盗用，因为此实例正在与黑洞（或陷穴）的 IP 地址通信。黑洞是网络中的一些位置，在这些位置中会将传入或传出流量静默丢弃，而不向源通知数据未达到源目标接收方。黑洞 IP 地址指定没有运行的主机或者未分配主机的地址。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/BlackholeTraffic!DNS

EC2 实例正在查询重定向到黑洞 IP 地址的域名。

默认严重级别：中

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例可能被盗用，因为此实例正在查询重定向到黑洞 IP 地址的域名。黑洞是网络中的一些位置，在这些位置中会将传入或传出流量静默丢弃，而不向源通知数据未达到源目标接收方。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DGADomainRequest.B


EC2 实例正在查询通过算法生成的域。此类域通常由恶意软件使用，并且可能表示 EC2 实例被盗用。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在尝试查询域生成算法 (DGA) 域。您的 EC2 实例可能被盗用。

DGA 用于定期生成大量的域名，可由其命令和控制 (C&C) 服务器用作汇聚点。命令和控制服务器是向僵尸网络的成员发布命令的计算机，僵尸网络是感染了相同类型恶意软件，并受其控制的一组连接到 Internet 的设备。大量潜在汇聚点的存在，使得有效关闭僵尸网络非常困难，因为受感染的计算机尝试每天与这样一些域名联系来接收更新或命令。

 Note

这此调查发现基于使用高级探试程序的域名分析，可能会发现在威胁情报源中不存在的新 DGA 域。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DGADomainRequest.C!DNS

EC2 实例正在查询通过算法生成的域。此类域通常由恶意软件使用，并且可能表示 EC2 实例被盗用。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例，正在尝试查询域生成算法 (DGA) 域。您的 EC2 实例可能被盗用。

DGA 用于定期生成大量的域名，可由其命令和控制 (C&C) 服务器用作汇聚点。命令和控制服务器是向僵尸网络的成员发布命令的计算机，僵尸网络是感染了相同类型恶意软件，并受其控制的一组连接到

Internet 的设备。大量潜在汇聚点的存在，使得有效关闭僵尸网络非常困难，因为受感染的计算机尝试每天与这样一些域名联系来接收更新或命令。

Note

这一发现基于威胁情报源中已知 GuardDuty 的 DGA 域名。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DNSDataExfiltration

EC2 实例通过 DNS 查询泄露数据。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例正在运行恶意软件，使用 DNS 查询用于出站数据传输。这种类型的数据传输表示实例已被盗用，并可能导致数据泄露。防火墙通常不会阻止 DNS 流量。举例而言，遭盗用 EC2 实例中的恶意软件可以将数据（例如，您的信用卡号）编码到 DNS 查询中，并将其发送到由攻击者控制的远程 DNS 服务器。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 实例正在查询某个远程主机的域名，该远程主机是路过式下载攻击的已知来源。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中列出的 EC2 实例可能被盗用，因为此实例正在查询某个远程主机的域名，该远程主机是路过式下载攻击的已知来源。这些是来自 Internet 的恶意计算机软件下载，可能会触发自动安装病毒、间谍软件或恶意软件。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DropPoint

EC2 实例正在尝试与已知持有凭证和恶意软件捕获的其他被盗数据的远程主机的 IP 地址进行通信。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例正在尝试与某个远程主机的 IP 地址进行通信，该主机持有由恶意软件捕获的凭证和其他被盗数据。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/DropPoint!DNS

EC2 实例正在查询持有由恶意软件捕获的凭证和其他被盗数据的远程主机的域名。

默认严重级别：中

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中的 EC2 实例正在查询远程主机的域名，该主机持有由恶意软件捕获的凭证和其他被盗数据。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Trojan:EC2/PhishingDomainRequest!DNS

EC2 实例正在查询涉及网络钓鱼攻击的域。您的 EC2 实例可能被盗用。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中的某个 EC2 实例，正在尝试查询参与网络钓鱼攻击的域。网络钓鱼域由冒充合法机构的人设置，其目的是引诱个人提供敏感数据，如个人可识别信息、银行和信用卡信息、密码等。您的 EC2 实例可能正在尝试检索存储在网络钓鱼网站上的敏感数据，或者可能正在尝试设置网络钓鱼网站。您的 EC2 实例可能被盗用。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

EC2 实例正在与自定义威胁列表上的 IP 地址建立连接。

默认严重级别：中

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例，正在与您上传的威胁列表中的 IP 地址通信。在 GuardDuty 中，威胁列表包含已知的恶意 IP 地址。GuardDuty 将根据已上传的威胁列表生成调查结果。用于生成此调查发现的威胁列表将在调查发现的详细信息中列出。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 实例正在执行解析到实例元数据服务的 DNS 查找。

默认严重级别：高

- 数据来源：DNS 日志

此调查发现通知您，您 AWS 环境中的某个 EC2 实例，正在查询一个解析为 EC2 元数据 IP 地址 (169.254.169.254) 的域。此类 DNS 查询可能表明该实例是 DNS 重新绑定技术的目标。此技术可用于从 EC2 实例获取元数据，包括与该实例关联的 IAM 凭证。

DNS 重新绑定需要引诱在 EC2 实例上运行的应用程序，以加载从 URL 返回的数据，该 URL 中的域名解析到 EC2 元数据 IP 地址 (169.254.169.254)。这会导致应用程序访问 EC2 元数据，并可能使其为攻击者所用。

如果该 EC2 实例正在运行允许注入 URL 的应用程序，且该应用程序存在漏洞；或者如果某用户在该 EC2 实例上运行的 Web 浏览器中，访问该 URL，则可以使用 DNS 重新绑定来访问 EC2 元数据。

修复建议：

为了解决此调查发现，您应该考虑 EC2 实例上是否运行有漏洞的应用程序，或者某用户是否使用浏览器来访问调查发现中识别的域。如果根本原因在于有漏洞的应用程序，您应该修复漏洞。如果是由于某用户已浏览识别的域，则应阻止该域或阻止用户进行访问。如果您确定调查发现属于以上任一种情况，则[撤销与 EC2 实例相关联的会话](#)。

某些 AWS 客户有意将元数据 IP 地址映射到其授权 DNS 服务器的域名。如果您的环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 UnauthorizedAccess:EC2/MetaDataDNSRebind。第二个筛选条件应为 DNS 请求域，并且值应与已映射到元数据 IP 地址 (169.254.169.254) 的域匹配。有关创建隐藏规则的更多信息，请参阅[抑制规则](#)。

UnauthorizedAccess:EC2/RDPBruteForce

EC2 实例涉及到 RDP 暴力攻击中。

默认严重级别：低*

Note

如果您的 EC2 实例是暴力攻击的目标，则此调查发现的严重级别为“低”。如果您的 EC2 实例是用于执行暴力攻击的攻击者，则此调查发现的严重级别为“高”。

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例参与到暴力攻击中，旨在获取基于 Windows 系统的 RDP 服务密码。这种情况可能表明有人未经授权访问您的 AWS 资源。

修复建议：

如果您实例的资源角色为 ACTOR，则表示实例已用于执行 RDP 暴力攻击。除非此实例有正当理由联系作为 Target 列出的 IP 地址，否则建议您假定实例已被盗用，并执行 [修复可能遭到入侵的 Amazon 实例 EC2](#) 中列出的操作。

如果您实例的资源角色为 TARGET，则可以通过安全组、ACL 或防火墙，将您的 RDP 端口限定为仅受信任的 IP，来纠正此调查发现。有关更多信息，请参阅[有关保护您的 EC2 实例 \(Linux\) 的提示](#)。

UnauthorizedAccess:EC2/SSHBruteForce

EC2 实例已涉及到 SSH 暴力攻击中。

默认严重级别：低*

Note

如果暴力攻击的目标是您的一个 EC2 实例，则此调查发现的严重程度较低。如果您的 EC2 实例用于执行暴力攻击，则此调查发现的严重程度为“高”。

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例涉及到暴力攻击中，旨在获取基于 Linux 系统的 SSH 服务密码。这种情况可能表明有人未经授权访问您的 AWS 资源。

Note

此调查发现仅通过在端口 22 上监控流量生成。如果 SSH 服务配置为使用其他端口，则不会生成此调查发现。

修复建议：

如果此次暴力攻击的目标是堡垒主机，这可能代表了 AWS 环境的预期行为。如果是这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 `UnauthorizedAccess:EC2/SSHBruteForce`。第二个筛选条件应与用作堡垒主机的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工具的实例可识别哪些条件。有关创建抑制规则的更多信息，请参阅 [抑制规则](#)。

如果您的环境不需要此活动，并且实例的资源角色为 `TARGET`，则可以通过安全组、ACL 或防火墙，将您的 SSH 端口限定为仅受信任的 IP，来纠正此调查发现。有关更多信息，请参阅 [有关保护您的 EC2 实例 \(Linux\) 的提示](#)。

如果您实例的资源角色为 `ACTOR`，则表示该实例已用于执行 SSH 暴力攻击。除非此实例有正当理由联系作为 Target 列出的 IP 地址，否则建议您假定实例已被盗用，并执行 [修复可能遭到入侵的 Amazon 实例 EC2](#) 中列出的操作。

UnauthorizedAccess:EC2/TorClient

EC2 实例正在连接到一个 Tor Guard 或 Authority 节点。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例，正在连接到一个 Tor Guard 或 Authority 节点。Tor 是用于实现匿名通信的软件。Tor Guard 和 Authority 节点充当 Tor 网络的初始网关。此流量可能指示此 EC2 实例已被盗用，正充当 Tor 网络上的客户端。此调查发现可能指示有人未经授权访问您的 AWS 资源，并意图隐藏攻击者的真实身份。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

UnauthorizedAccess:EC2/TorRelay

EC2 实例正在以 Tor 中继身份连接到 Tor 网络。

默认严重级别：高

- 数据来源：VPC 流日志

此调查发现通知您，您 AWS 环境中的 EC2 实例，正在以一种暗示其充当 Tor 中继的方式与 Tor 网络建立连接。Tor 是用于实现匿名通信的软件。Tor 通过将客户端可能的非法流量从一个 Tor 中继转发到另一个 Tor 中继，来提高通信的匿名程度。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

GuardDuty IAM查找类型

以下发现特定于IAM实体和访问密钥，并且资源类型始终为AccessKey。调查发现的严重性和详细信息因调查发现类型而异。

此处列出的调查发现包括用于生成该调查发现类型的数据来源和模型。有关更多信息，请参阅 [GuardDuty 基础数据源](#)。

对于所有IAM相关发现，我们建议您检查相关实体，并确保其权限遵循最低权限的最佳实践。如果此活动是意外活动，则凭证可能已泄露。有关修复调查发现的信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

主题

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)

- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [PenTest:IAMUser/KaliLinux](#)
- [PenTest:IAMUser/ParrotLinux](#)
- [PenTest:IAMUser/PentoolLinux](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [Policy:IAMUser/RootCredentialUsage](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Recon:IAMUser/MaliciousIPCaller](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

CredentialAccess:IAMUser/AnomalousBehavior

以异常方式调用了API用于访问 AWS 环境的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。当攻击者试图为您的环境收集密码、用户名和访问密钥时，API观察到的情况通常与攻击的凭证访问阶段有关。此类别APIs中的是GetPasswordData、GetSecretValueBatchGetSecretValue、和GenerateDbAuthToken。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

DefenseEvasion:IAMUser/AnomalousBehavior

以一种反常的方式援引了API用来逃避防御措施的手段。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与防御逃避战术有关，在这种策略中，对手试图掩盖自己的踪迹并逃避侦查。APIs此类别中通常包括删除、禁用或停止操作，例如DeleteFlowLogs、DisableAlarmActions、或StopLogging。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Discovery:IAMUser/AnomalousBehavior

API通常用于发现资源的方法被异常调用。

默认严重级别：低

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与攻击的发现阶段有关，即攻击者正在收集信息以确定您的 AWS 环境是否容易受到更广泛的攻击。APIs此类别中通常是获取、描述或列出操作，例如DescribeInstances、GetRolePolicy、或ListAccessKeys。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Exfiltration:IAMUser/AnomalousBehavior

API通常用于从 AWS 环境中收集数据的方法被异常调用。

默认严重级别：高

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与泄露策略有关，在这种策略中，对手试图使用打包和加密从您的网络收集数据以避免被发现。APIs此查找类型仅为管理（控制平面）操作，通常与 S3、快照和数据库相关，例如、PutBucketReplicationCreateSnapshot、或。RestoreDBInstanceFromDBSnapshot

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Impact:IAMUser/AnomalousBehavior

API通常用于在 AWS 环境中篡改数据或进程的方法被以异常方式调用。

默认严重级别：高

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与冲击策略有关，在这种策略中，对手试图破坏运营并操纵、中断或销毁您账户中的数据。APIs对于此查找类型，通常是删除、更新或放置操作，例如DeleteSecurityGroup、UpdateUser、或PutBucketPolicy。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

InitialAccess:IAMUser/AnomalousBehavior

API通常用于未经授权访问 AWS 环境的方法被异常调用。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与攻击的初始访问阶段有关，即攻击者试图建立对您环境的访问权限。APIs此类别中通常有 get token 或会话操作，例如GetFederationToken、StartSession、或GetAuthorizationToken。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如

发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用该API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅[修复可能被泄露的凭证AWS](#)。

PenTest:IAMUser/KaliLinux

API是从 Kali Linux 计算机上调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，一台运行 Kali Linux 的计算机正在使用属于您环境中列出的 AWS 账户的凭据进行 API 呼叫。Kali Linux 是一种流行的渗透测试工具，安全专业人员使用它来识别需要修补的 EC2 实例中的漏洞。攻击者还使用此工具来发现 EC2 配置漏洞，并获得对您的 AWS 环境的未经授权的访问权限。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅[修复可能被泄露的凭证AWS](#)。

PenTest:IAMUser/ParrotLinux

API是从 Parrot Security Linux 计算机上调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，一台运行 Parrot Security Linux 的计算机正在使用属于您环境中列出的 AWS 账户的凭据进行 API 呼叫。Parrot Security Linux 是一种流行的渗透测试工具，安全专业人员使用它来识别需要修补的 EC2 实例中的漏洞。攻击者还使用此工具来发现 EC2 配置漏洞，并获得对您的 AWS 环境的未经授权的访问权限。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

PenTest:IAMUser/PentooLinux

API是从 Pentoo Linux 计算机上调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，一台运行 Pentoo Linux 的计算机正在使用属于你环境中列出的 AWS 账户的凭据进行API呼叫。Pentoo Linux 是一种流行的渗透测试工具，安全专业人员使用它来识别需要修补的EC2实例中的漏洞。攻击者还使用此工具来发现EC2配置漏洞，并获得对您的 AWS 环境的未经授权的访问权限。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Persistence:IAMUser/AnomalousBehavior

API通常用于维护对 AWS 环境的未经授权访问的方法被异常调用。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与持久性策略有关，在这种策略中，对手已获得对您的环境的访问权限并试图保持该访问权限。APIs此类别中通常是创建、导入或修改操作，例如CreateAccessKey、ImportKeyPair、或ModifyInstanceAttribute。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Policy: IAMUser/RootCredentialUsage

API是使用根用户登录凭据调用的。

默认严重级别：低

- 数据源：CloudTrail 管理事件或 CloudTrail 数据事件

此调查发现通知您，正在利用您环境中列出的 AWS 账户 根用户登录凭证，向 AWS 服务发出请求。建议用户切勿使用 root 用户登录凭据来访问 AWS 服务。相反，应使用来自 AWS Security Token Service (STS) 的最低权限临时证书访问 AWS 服务。AWS STS 对于不支持的情况，建议IAM使用用户证书。有关更多信息，请参阅[IAM最佳实践](#)。

Note

如果为该账户启用了 S3 威胁检测，则可能会生成此调查发现，以响应使用 AWS 账户的根用户登录凭证对 S3 资源运行 S3 数据面板操作的尝试。使用的API呼叫将在查找详细信息中列出。如果未启用 S3 威胁检测，则只能由事件日志触发此发现APIs。有关 S3 威胁检测的更多信息，请参阅 [S3 保护](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

PrivilegeEscalation: IAMUser/AnomalousBehavior

API通常用于获取 AWS 环境高级权限的方法被异常调用。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，在你的账户中发现了一个异常API请求。这一发现可能包括单个[用户身份](#)在附近提出的单个API或一系列相关API请求。API观察到的情况通常与权限升级策略有关，在这种策略中，攻击者试图获得更高级别的环境权限。APIs此类别中通常涉及更改IAM策略、角色和用户的操作，例如、AssociateIamInstanceProfileAddUserToGroup、或PutUserPolicy。

该API请求被 GuardDuty异常检测机器学习 (ML) 模型识别为异常。机器学习模型会评估您账户中的所有API请求，并识别与对手使用的技术相关的异常事件。机器学习模型跟踪API请求的各种因素，例如发出请求的用户、发出请求的位置以及请求API的具体内容。有关请求中哪些因素对调用API请求的用户身份不寻常的详细信息，可以在[调查结果详细信息中找到](#)。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅[修复可能被泄露的凭证AWS](#)。

Recon:IAMUser/MaliciousIPCaller

API是从已知的恶意 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，可以列出或描述您环境中账户中 AWS 资源的API操作是从威胁列表中包含的 IP 地址调用的。攻击者可能会使用被盗的凭据对您的 AWS 资源进行此类侦察，以找到更有价值的凭据或确定他们已经拥有的凭据的功能。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅[修复可能被泄露的凭证AWS](#)。

Recon:IAMUser/MaliciousIPCaller.Custom

API是从已知的恶意 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，可以列出或描述您环境中账户中 AWS 资源的 API 操作是从自定义威胁列表中包含的 IP 地址调用的。使用的威胁列表将在调查发现的详细信息中列出。攻击者可能会使用被盗的凭据对您的 AWS 资源进行此类侦察，以便找到更有价值的凭据或确定他们已经拥有的凭据的功能。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Recon:IAMUser/TorIPCaller

API 是从 Tor 退出节点 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉你，可以列出或描述环境中账户中 AWS 资源的 API 操作是从 Tor 出口节点 IP 地址调用的。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。攻击者会使用 Tor 来掩盖他们的真实身份。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail 日志记录已禁用。

默认严重级别：低

- 数据源：CloudTrail 管理事件

此发现告知您 AWS 环境中的一条 CloudTrail 跟踪已被禁用。这可能是攻击者尝试禁用日志记录，通过消除其活动的任何痕迹来掩盖其踪迹，同时出于恶意目的获取对您 AWS 资源的访问权限。成功地删除或更新跟踪会触发此调查发现。成功删除存储与之关联的跟踪中的日志的 S3 存储桶也可能触发此发现 GuardDuty。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

Stealth:IAMUser/PasswordPolicyChange

账户密码策略受损。

默认严重级别：低*

Note

此调查发现的严重性可以是“低”、“中”或“高”，具体取决于对密码策略所做更改的严重性。

- 数据源：CloudTrail 管理事件

您的 AWS 环境中列出的 AWS 账户的账户密码策略已被削弱。例如，策略已删除或者进行了更新，要求较少的字符、无需符号和数字或者要求延长密码有效期。尝试更新或删除您的 AWS 账户密码策略也可能触发此发现。AWS 账户密码策略定义了管理可以为您的 IAM 用户设置哪些类型的密码的规则。较弱的密码策略允许创建易于记住同时也可能更容易被猜到的密码，因而造成安全风险。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

发现多个全球范围内的成功控制台登录。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，大约在同一时间在不同的地理位置观察到同一 IAM 用户多次成功登录控制台。这种异常且有风险的访问位置模式表明您的 AWS 资源可能遭到未经授权的访问。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

通过EC2实例启动角色专为实例创建的证书正在从其中的另一个账户中使用 AWS。

默认严重级别：高*

Note

此调查发现的默认严重级别为“高”。但是，如果是由与您的 AWS 环境关联的账户调用的，则严重性为“中”。API

- 数据源：CloudTrail 管理事件或 S3 数据事件

当您的EC2实例证书被用于APIs从与关联EC2实例运行的 AWS 账户不同的账户拥有的 IP 地址进行调用时，该发现会通知您。

AWS 不建议在创建临时证书的实体（例如 AWS 应用程序或 Lambda）之外重新分配临时证书。EC2但是，授权用户可以从其EC2实例中导出证书以进行合法API呼叫。如果该remoteAccountDetails.Affiliated字段为True，则API是从与您的 AWS 环境关联的账户调用的。要排除潜在的攻击并验证活动的合法性，请联系分配了这些凭据的IAM用户。

Note

如果 GuardDuty 观察到来自远程账户的持续活动，则其机器学习 (ML) 模型会将其识别为预期行为。因此，GuardDuty 将停止为来自该远程账户的活动生成此调查结果。GuardDuty 将继续从其他远程帐户生成有关新行为的调查结果，并将随着时间的推移行为发生变化而重新评估已学习的远程帐户。

修复建议：

针对此调查发现，您可以使用以下工作流程来确定行动方案：

1. 从 `service.action.awsApiCallAction.remoteAccountDetails.accountId` 字段识别涉及的远程账户。
2. 接下来，从 `service.action.awsApiCallAction.remoteAccountDetails.affiliated` 现场确定该账户是否与您的 GuardDuty 环境有关联。
3. 如果该账户是关联账户，请联系远程账户所有者和 EC2 实例凭证的所有者进行调查。
4. 如果该账户没有关联账户，首先要评估该账户是否与您的组织相关联，但不是您的 GuardDuty 多账户设置的一部分，或者该账户是否 GuardDuty 尚未启用。否则，请联系 EC2 凭证的所有者，以确定是否存在远程账户使用这些凭据的用例。
5. 如果凭证的所有者无法识别远程账户，则该凭证可能已被在 AWS 中操作的威胁行为者窃取。您应该采取 [修复可能遭到入侵的 Amazon 实例 EC2](#) 中建议的步骤来保护您的环境。

此外，您可以向 [AWS 信任与安全团队提交滥用报告](#)，开始对远程账户进行调查。向 AWS Trust and Safety 提交报告时，请附上调查结果的全部 JSON 细节。

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

通过 EC2 实例启动角色专为实例创建的证书正在从外部 IP 地址使用。

默认严重级别：高

- 数据源：CloudTrail 管理事件或 S3 数据事件

这一发现告诉您，外部的 AWS 主机试图使用在您 AWS 环境中的 EC2 实例上创建的临时 AWS 证书来运行 AWS API 操作。列出的 EC2 实例可能已被泄露，并且该实例的临时证书可能已被泄露到外部的远程主机。AWS 不建议在创建临时证书的实体（例如 AWS 应用程序或 Lambda）之外重新分配临时证书。EC2 但是，授权用户可以从其 EC2 实例中导出证书以进行合法 API 呼叫。要排除潜在的攻击并验证活动的合法性，请验证是否应在调查发现中使用来自远程 IP 的实例凭证。

Note

如果 GuardDuty 观察到来自远程账户的持续活动，则其机器学习 (ML) 模型会将其识别为预期行为。因此，GuardDuty 将停止为来自该远程账户的活动生成此调查结果。GuardDuty 将继续从其他远程帐户生成有关新行为的调查结果，并将随着时间的推移行为发生变化而重新评估已学习的远程帐户。

修复建议：

当网络配置为路由 Internet 流量，使其从本地网关而不是从 Internet Gateway (IGW) 流出时，VPC 就会生成此结果。常用配置（例如使用[AWS Outposts](#)或VPCVPN连接）可能会导致流量以这种方式路由。如果这是预期行为，我们建议您使用抑制规则，并创建一个包含两个过滤条件的规则。第一个标准是 finding type（调查发现类型），它应是 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS。第二个筛选条件是API呼叫者IPv4地址，其中包含本地互联网网关的 IP 地址或CIDR范围。要了解有关创建抑制规则的更多信息，请参阅[抑制规则](#)。

Note

如果 GuardDuty 观察到来自外部来源的持续活动，则其机器学习模型将将其识别为预期行为，并停止为来自该来源的活动生成此发现。GuardDuty 将继续从其他来源得出有关新行为的调查结果，并将随着时间的推移行为发生变化而重新评估所学来源。

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅[修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/MaliciousIPCaller

API是从已知的恶意 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

此发现告诉您，某项API操作（例如，尝试启动EC2实例、创建新IAM用户或修改您的 AWS 权限）是从已知的恶意 IP 地址调用的。这可能表示对您环境中的 AWS 资源进行了未经授权的访问。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

API是从自定义威胁列表上的 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

此发现告诉您，某项API操作（例如，尝试启动EC2实例、创建新IAM用户或修改 AWS 权限）是从您上传的威胁列表中包含的 IP 地址调用的。在中，威胁列表包含已知的恶意 IP 地址。这可能表示对您环境中的 AWS 资源进行了未经授权的访问。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/TorIPCaller

API是从 Tor 退出节点 IP 地址调用的。

默认严重级别：中

- 数据源：CloudTrail 管理事件

这一发现告诉您，从 Tor 出口节点 IP 地址调用了一项API操作（EC2例如，尝试启动实例、创建新IAM用户或修改您的 AWS 权限）。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这种情况可能表明有人未经授权访问您的 AWS 资源，并意图隐藏攻击者的真实身份。

修复建议：

如果此活动是意外活动，则您的凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。

GuardDuty S3 查找类型

以下发现特定于 Amazon S3 资源，S3Bucket如果数据源是 S3 的数据事件，或者CloudTrail 数据源是CloudTrail 管理事件，AccessKey则其资源类型将为。调查发现的严重性和详细信息将因调查发现类型和与存储桶关联的权限而异。

此处列出的调查发现包括用于生成该调查发现类型的数据来源和模型。有关数据来源和模型的更多信息，请参阅 [GuardDuty 基础数据源](#)。

Important

只有在启用了 S3 保护后，才会生成具有 S3 CloudTrail 数据事件数据源的调查结果 GuardDuty。2020 年 7 月 31 日之后创建的所有账户均默认启用 S3 保护。有关如何启用或禁用 S3 保护的信息，请参阅 [GuardDuty S3 防护](#)。

对于所有 S3Bucket 类型的调查发现，建议您检查相关存储桶的权限以及调查发现中涉及的任何用户权限，如果活动是不正常的，请参阅 [修复可能遭到入侵的 S3 存储桶](#) 中详细介绍的修复建议。

主题

- [Discovery:S3/AnomalousBehavior](#)
- [Discovery:S3/MaliciousIPCaller](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:S3/MaliciousIPCaller](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/MaliciousIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [PenTest:S3/ParrotLinux](#)
- [PenTest:S3/Pentoolinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)

- [UnauthorizedAccess:S3/TorIPCaller](#)

Discovery:S3/AnomalousBehavior

常用于发现 S3 对象的 API 被异常调用。

默认严重级别：低

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，IAM 实体已调用 S3 API 来发现您环境中的 S3 存储桶，例如 ListObjects。此类活动与攻击的发现阶段相关，在该阶段攻击者收集信息以确定您的 AWS 环境是否容易受到更广泛的攻击。此活动之所以可疑，是因为 IAM 实体调用 API 的方式异常。例如，以前没有历史记录 IAM 实体调用了 S3 API，或者 IAM 实体从异常位置调用 S3 API。

此 API 被 GuardDuty 异常检测机器学习 (ML) 模型确定为异常。机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者使用的技术相关的异常事件。还会跟踪 API 请求的各种因素，例如发出请求的用户、发出请求的位置、请求的特定 API、请求的存储桶，以及发出的 API 调用次数。如需了解对于调用 API 请求的用户身份而言具体的异常因素，请参阅[查找详细信息](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Discovery:S3/MaliciousIPCaller

通常用于在 AWS 环境中发现资源的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，与已知恶意活动关联的 IP 地址调用了 S3 API 操作。观察到的 API 通常与攻击的发现阶段相关联，即攻击者正在收集有关您的 AWS 环境的信息。示例包括 GetObjectAcl 和 ListObjects。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Discovery:S3/MaliciousIPCaller.Custom

自定义威胁列表中的 IP 地址调用了 S3 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，您上传的威胁列表中的 IP 地址调用了 S3 API（例如 GetObjectAcl 或 ListObjects）。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。此类活动与攻击的发现阶段有关，攻击者会在该阶段收集信息，以确定您的 AWS 环境是否容易受到更广泛的攻击。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Discovery:S3/TorIPCaller

Tor 出口节点 IP 地址调用了 S3 API。

默认严重级别：中

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，Tor 出口节点 IP 地址调用了 S3 API（例如 GetObjectAcl 和 ListObjects）。此类活动与攻击的发现阶段有关，攻击者正在收集信息以确定您的 AWS 环境是否容易受到更广泛的攻击。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这可能表示未经授权访问您的 AWS 资源，目的是隐藏攻击者的真实身份。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Exfiltration:S3/AnomalousBehavior

IAM 实体以可疑的方式调用了 S3 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，IAM 实体正在进行涉及 S3 存储桶的 API 调用，并且此活动与该实体的既定基准不同。此活动中使用的 API 调用在攻击的渗透阶段进行，攻击者在该阶段试图收集数据。此活动之所以可疑，是因为 IAM 实体调用 API 的方式异常。例如，以前没有历史记录 IAM 实体调用了 S3 API，或者 IAM 实体从异常位置调用 S3 API。

此 API 被 GuardDuty 异常检测机器学习 (ML) 模型确定为异常。机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者使用的技术相关的异常事件。还会跟踪 API 请求的各种因素，例如发出请求的用户、发出请求的位置、请求的特定 API、请求的存储桶，以及发出的 API 调用次数。如需了解对于调用 API 请求的用户身份而言具体的异常因素，请参阅[查找详细信息](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Exfiltration:S3/MaliciousIPCaller

通常用于从 AWS 环境中收集数据的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，与已知恶意活动关联的 IP 地址调用了 S3 API 操作。API 通常与攻击者试图从您的网络收集数据的泄露策略相关联。示例包括 GetObject 和 CopyObject。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Impact:S3/AnomalousBehavior.Delete

IAM 实体以可疑的方式调用了试图删除数据的 S3 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉您，您 AWS 环境中的一个 IAM 实体正在进行涉及 S3 存储桶的 API 调用，这种行为与该实体的既定基准不同。此活动中使用的 API 调用与试图删除数据的攻击相关联。此活动之所以可疑，是因为 IAM 实体调用 API 的方式异常。例如，以前没有历史记录 IAM 实体调用了 S3 API，或者 IAM 实体从异常位置调用 S3 API。

此 API 被 GuardDuty 异常检测机器学习 (ML) 模型确定为异常。机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者使用的技术相关的异常事件。还会跟踪 API 请求的各种因素，例如发出请求的用户、发出请求的位置、请求的特定 API、请求的存储桶，以及发出的 API 调用次数。如需了解对于调用 API 请求的用户身份而言具体的异常因素，请参阅[查找详细信息](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

我们建议您对 S3 存储桶的内容进行审计，以确定是否可以或应该恢复之前的对象版本。

Impact:S3/AnomalousBehavior.Permission

异常调用了常用于设置访问控制列表 (ACL) 权限的 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉您，您 AWS 环境中的一个 IAM 实体更改了列出的 S3 存储桶上的存储桶策略或 ACL。此更改可能会向所有经过身份验证的 AWS 用户公开您的 S3 存储桶。

此 API 被 GuardDuty 异常检测机器学习 (ML) 模型确定为异常。机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者使用的技术相关的异常事件。还会跟踪 API 请求的各种因素，例如发出请

求的用户、发出请求的位置、请求的特定 API、请求的存储桶，以及发出的 API 调用次数。如需了解对于调用 API 请求的用户身份而言具体的异常因素，请参阅[查找详细信息](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

我们建议对您的 S3 存储桶的内容进行审计，以确保没有对象被意外允许公开访问。

Impact:S3/AnomalousBehavior.Write

IAM 实体调用了试图以可疑方式写入数据的 S3 API。

默认严重级别：中

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉您，您 AWS 环境中的一个 IAM 实体正在进行涉及 S3 存储桶的 API 调用，这种行为与该实体的既定基准不同。此活动中使用的 API 调用与尝试写入数据的攻击相关联。此活动之所以可疑，是因为 IAM 实体调用 API 的方式异常。例如，以前没有历史记录 IAM 实体调用了 S3 API，或者 IAM 实体从异常位置调用 S3 API。

此 API 被 GuardDuty 异常检测机器学习 (ML) 模型确定为异常。机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者使用的技术相关的异常事件。还会跟踪 API 请求的各种因素，例如发出请求的用户、发出请求的位置、请求的特定 API、请求的存储桶，以及发出的 API 调用次数。如需了解对于调用 API 请求的用户身份而言具体的异常因素，请参阅[查找详细信息](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

我们建议您对 S3 存储桶的内容进行审计，以确保此 API 调用未写入恶意或未经授权的数据。

Impact:S3/MaliciousIPCaller

通常用于在 AWS 环境中篡改数据或进程的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，与已知恶意活动关联的 IP 地址调用了 S3 API 操作。观察到的 API 通常与冲击策略相关联，在这种策略中，对手试图操纵、中断或销毁您的 AWS 环境中的数据。示例包括 PutObject 和 PutObjectAcl。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

PenTest:S3/KaliLinux

运行有 Kali Linux 的计算机调用了 S3 API。

默认严重级别：中

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉你，一台运行 Kali Linux 的计算机正在使用属于你 AWS 账户的凭据进行 S3 API 调用。您的凭证可能遭到盗用。Kali Linux 是一种流行的渗透测试工具，安全专家用它来确定需要修补的 EC2 实例中的漏洞。攻击者还使用此工具来发现 EC2 配置漏洞，并获得对您的 AWS 环境的未经授权的访问权限。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

PenTest:S3/ParrotLinux

运行有 Parrot Security Linux 的计算机调用了 S3 API。

默认严重级别：中

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉你，一台运行 Parrot Security Linux 的计算机正在使用属于你 AWS 账户的凭据进行 S3 API 调用。您的凭证可能遭到盗用。Parrot Security Linux 是一种流行的渗透测试工具，安全专家用它来确定需要修补的 EC2 实例中的漏洞。攻击者也会使用此工具来寻找 EC2 配置漏洞和获取对您 AWS 环境未经授权的访问。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

PenTest:S3/PentooLinux

运行有 Pentoo Linux 的计算机调用了 S3 API。

默认严重级别：中

- 数据源：S3 CloudTrail 的数据事件

这一发现告诉你，一台运行 Pentoo Linux 的计算机正在使用属于你 AWS 账户的凭据进行 S3 API 调用。您的凭证可能遭到盗用。Pentoo Linux 是一种流行的渗透测试工具，安全专家用它来确定需要修补的 EC2 实例中的漏洞。攻击者还使用此工具来发现 EC2 配置漏洞，并获得对您的 AWS 环境的未经授权的访问权限。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Policy:S3/AccountBlockPublicAccessDisabled

IAM 实体调用了用于禁用账户上 S3 屏蔽公共访问权限的 API。

默认严重级别：低

- 数据源：CloudTrail 管理事件

此调查发现通知您，Amazon S3 屏蔽公共访问权限已在账户级别禁用。启用 S3 屏蔽公共访问权限设置后，将用于筛选存储桶的策略或访问控制列表（ACL），作为防止意外公开暴露数据的安全措施。

通常情况下，会关闭账户的 S3 屏蔽公共访问权限，以允许公开访问存储桶或存储桶中的对象。禁用账户的 S3 屏蔽公共访问权限后，对存储桶的访问权限将由应用于个人存储桶的策略、ACL 或存储桶级屏蔽公共访问权限设置来控制。这并不一定意味着将公开共享存储桶，但应审计应用于存储桶的权限，以确认这些权限提供了适当的访问级别。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Policy:S3/BucketAnonymousAccessGranted

IAM 主体已通过更改存储桶策略或 ACL 向 Internet 授予对 S3 存储桶的访问权限。

默认严重级别：高

- 数据源：CloudTrail 管理事件

此调查发现通知您，由于 IAM 实体更改了所列出的 S3 存储桶的策略或 ACL，因此该存储桶已可在 Internet 上公开访问。检测到策略或 ACL 变更后，使用由 [Zelkova](#) 支持的自动推理来确定存储桶是否可公开访问。

Note

如果将存储桶的 ACL 或存储桶策略配置为明确拒绝或全部拒绝，则此调查发现可能无法反映存储桶的当前状态。此调查发现不会反映任何可能已为您的 S3 存储桶启用的 [S3 屏蔽公共访问权限](#) 设置。在这种情况下，调查发现中的 effectivePermission 值将标记为 UNKNOWN。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Policy:S3/BucketBlockPublicAccessDisabled

IAM 主体调用了禁用存储桶 S3 屏蔽公共访问权限的 API。

默认严重级别：低

- 数据源：CloudTrail 管理事件

此调查发现通知您已禁用列出的 S3 存储桶的屏蔽公开访问权限。启用 S3 屏蔽公共访问权限设置后，将用于筛选存储桶的策略或访问控制列表（ACL），作为防止意外公开暴露数据的安全措施。

通常情况下，会关闭存储桶的 S3 屏蔽公共访问权限，以允许公开访问该存储桶或其中的对象。由于禁用了存储桶的 S3 屏蔽公共访问权限，因此对该存储桶的访问权限将由其策略或 ACL 控制。这并不意味着将公开共享存储桶，但应审计应用于该存储桶的策略和 ACL，以确认应用适当的权限。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Policy:S3/BucketPublicAccessGranted

IAM 委托人已通过更改存储桶策略或 ACL 向所有 AWS 用户授予对 S3 存储桶的公共访问权限。

默认严重级别：高

- 数据源：CloudTrail 管理事件

这一发现告诉您，列出的 S3 存储桶已向所有经过身份验证的 AWS 用户公开，因为 IAM 实体更改了该 S3 存储桶的存储桶策略或 ACL。检测到策略或 ACL 变更后，使用由 [Zelkova](#) 支持的自动推理来确定存储桶是否可公开访问。

Note

如果将存储桶的 ACL 或存储桶策略配置为明确拒绝或全部拒绝，则此调查发现可能无法反映存储桶的当前状态。此调查发现不会反映任何可能已为您的 S3 存储桶启用的 [S3 屏蔽公共访问权限](#) 设置。在这种情况下，调查发现中的 effectivePermission 值将标记为 UNKNOWN。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

Stealth:S3/ServerAccessLoggingDisabled

已为存储桶禁用 S3 服务器访问日志记录。

默认严重级别：低

- 数据源：CloudTrail 管理事件

这一发现告诉您，您的 AWS 环境中的存储桶已禁用 S3 服务器访问日志记录。如果禁用，则不会为访问已识别的 S3 存储桶的任何尝试创建 Web 请求日志，但是，仍会跟踪对该存储桶的 S3 管理 API 调用（例如 [DeleteBucket](#)）。如果通过 CloudTrail 为该存储桶启用 S3 数据事件记录，则仍将跟踪对存储桶内对象的 Web 请求。禁用日志记录是未经授权的用户为逃避检测而使用的一种技术。要了解有关 S3 日志的更多信息，请参阅 [S3 服务器访问日志记录](#) 和 [S3 日志记录选项](#)。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

自定义威胁列表中的 IP 地址调用了 S3 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，您上传的威胁列表中的 IP 地址调用了 S3 API 操作（例如 `PutObject` 或 `PutObjectAcl`）。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

UnauthorizedAccess:S3/TorIPCaller

Tor 出口节点 IP 地址调用了 S3 API。

默认严重级别：高

- 数据源：S3 CloudTrail 的数据事件

此调查发现通知您，Tor 出口节点 IP 地址调用了 S3 API 操作（例如 PutObject 和 PutObjectAcl）。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这一发现可能表明有人未经授权访问您的 AWS 资源，目的是隐藏攻击者的真实身份。

修复建议：

如果此活动对于关联主体来说是意外活动，则可能表明凭证已暴露或 S3 权限不够严格。有关更多信息，请参阅 [修复可能遭到入侵的 S3 存储桶](#)。

EKS审核日志查找类型

以下是针对 Kubernetes 资源的调查发现，并且 resource_type 为 EKSCluster。调查发现的严重性和详细信息将因调查发现类型而异。

对于所有 Kubernetes 类型的调查发现，我们建议您检查相关资源，以确定该活动是正常的活动还是潜在的恶意活动。有关修复发现的受损的 Kubernetes 资源的指南，GuardDuty 请参阅 [修复 EKS 审计日志监控调查发现](#)

Note

如果生成这些调查发现的活动的活动是正常的活动，则应考虑添加 [抑制规则](#) 以防将来发出警报。

主题

- [CredentialAccess:Kubernetes/MaliciousIPCaller](#)
- [CredentialAccess:Kubernetes/MaliciousIPCaller.Custom](#)
- [CredentialAccess:Kubernetes/SuccessfulAnonymousAccess](#)

- [CredentialAccess:Kubernetes/TorIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom](#)
- [DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess](#)
- [DefenseEvasion:Kubernetes/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Impact:Kubernetes/SuccessfulAnonymousAccess](#)
- [Impact:Kubernetes/TorIPCaller](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Persistence:Kubernetes/MaliciousIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/SuccessfulAnonymousAccess](#)
- [Persistence:Kubernetes/TorIPCaller](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated](#)
- [Execution:Kubernetes/AnomalousBehavior.ExecInPod](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer](#)
- [Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount](#)
- [Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed](#)

- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated](#)
- [Discovery:Kubernetes/AnomalousBehavior.PermissionChecked](#)

Note

在 Kubernetes 版本 1.14 之前，该 `system:unauthenticated` 群组与默认关联且处于关联状态。 `system:discovery` `system:basic-user` ClusterRoles 这种关联可能导致匿名用户意外访问。更新集群不会撤消这些权限。即使您将集群更新到版本 1.14 或更高版本，这些权限仍可能处于启用状态。我们建议您取消这些权限与 `system:unauthenticated` 组的关联。有关撤消这些权限的指导，请参阅《亚马逊EKS用户指南》EKS中的[亚马逊安全最佳实践](#)。

CredentialAccess:Kubernetes/MaliciousIPCaller

API通常用于访问 Kubernetes 集群中的凭据或机密的方法是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API操作是从与已知恶意活动关联的 IP 地址调用的。API观察到的情况通常与证书访问策略有关，在这种策略中，攻击者试图为您的 Kubernetes 集群收集密码、用户名和访问密钥。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是 `system:anonymous`，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤消权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤消用户的访问权限，并撤消攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

API常用于访问 Kubernetes 集群中的凭据或机密的方法是从自定义威胁列表上的 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API操作是从您上传的威胁列表中包含的 IP 地址调用的。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。API观察到的情况通常与证书访问策略有关，在这种策略中，攻击者试图为您的 Kubernetes 集群收集密码、用户名和访问密钥。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和并在需要时撤销权限的原因。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

未经身份验证的用户调用了API常用于访问 Kubernetes 集群中的凭据或机密的。

默认严重级别：高

- 功能：EKS审核日志

此发现告知您system:anonymous用户已成功调用某项API操作。API由system:anonymous发出的呼叫未经身份验证。观察到的情况API通常与证书访问策略有关，在这种策略中，攻击者试图为您的 Kubernetes 集群收集密码、用户名和访问密钥。此活动表示允许对调查结果中报告的API操作进行匿名或未经身份验证的访问，也可能允许对其他操作进行匿名或未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

修复建议：

您应检查集群上已授予 system:anonymous 用户的权限，并确保所有权限都是必需的。如果权限是错误或恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。

有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

CredentialAccess:Kubernetes/TorIPCaller

API通常用于访问 Kubernetes 集群中的凭据或机密的方法是从 Tor 出口节点 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

这个发现告诉你，API是从 Tor 出口节点 IP 地址调用的。API观察到的情况通常与证书访问策略有关，在这种策略中，攻击者试图为您的 Kubernetes 集群收集密码、用户名和访问密钥。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这种情况可能表明有人未经授权访问您的 Kubernetes 集群资源，并意图隐藏攻击者的真实身份。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

DefenseEvasion:Kubernetes/MaliciousIPCaller

逃避防御措施的API常用方法是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API操作是从与已知恶意活动关联的 IP 地址调用的。API观察到的情况通常与逃避防御策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限

的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

逃避防御措施的API常用方法是从自定义威胁列表上的 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API操作是从您上传的威胁列表中包含的 IP 地址调用的。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。API观察到的情况通常与逃避防御策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

未经身份验证的用户调用了逃避防御措施的API常用方法。

默认严重级别：高

- 功能：EKS审核日志

此发现告知您system:anonymous用户已成功调用某项API操作。API由system:anonymous发出的呼叫未经身份验证。观察到的情况API通常与逃避防御策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。此活动表示允许对调查结果中报告的API操作进行匿名或未经身份验证的访问，也可能允许对其他操作进行匿名或未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

修复建议：

您应检查集群上已授予 `system:anonymous` 用户的权限，并确保所有权限都是必需的。如果权限是错误或恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。

有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

DefenseEvasion:Kubernetes/TorIPCaller

逃避防御措施的API常用方法是从 Tor 出口节点 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

这个发现告诉你，API是从 Tor 出口节点 IP 地址调用的。API观察到的情况通常与逃避防御策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这种情况可能表明有人未经授权访问您的 Kubernetes 集群，并意图隐藏攻击者的真实身份。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是`system:anonymous`，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Discovery:Kubernetes/MaliciousIPCaller

API通常用于在 Kubernetes 集群中发现资源的方法是从 IP 地址调用的。

默认严重级别：中

- 功能：EKS审核日志

此发现告诉您，API操作是从与已知恶意活动关联的 IP 地址调用的。观察到API的通常用于攻击的发现阶段，攻击者正在收集信息以确定您的 Kubernetes 集群是否容易受到更广泛的攻击。

用于未经身份验证的访问

MaliciousIPCaller对于未经身份验证的访问，不会生成调查结果。

SuccessfulAnonymousAccess结果是针对未经身份验证或匿名访问生成的。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Discovery:Kubernetes/MaliciousIPCaller.Custom

API通常用于发现 Kubernetes 集群中资源的方法是从自定义威胁列表上的 IP 地址调用的。

默认严重级别：中

- 功能：EKS审核日志

此发现告诉您，API是从您上传的威胁列表中包含的 IP 地址调用的。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。观察到API的通常用于攻击的发现阶段，攻击者正在收集信息以确定您的 Kubernetes 集群是否容易受到更广泛的攻击。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Discovery:Kubernetes/SuccessfulAnonymousAccess

API通常用于发现 Kubernetes 集群中资源的方法是由未经身份验证的用户调用的。

默认严重级别：中

- 功能：EKS审核日志

此发现告知您system:anonymous用户已成功调用某项API操作。API由system:anonymous发出的呼叫未经身份验证。观察到的情况API通常与攻击的发现阶段有关，即攻击者正在收集有关您的Kubernetes 集群的信息。此活动表示允许对调查结果中报告的API操作进行匿名或未经身份验证的访问，也可能允许对其他操作进行匿名或未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

此发现类型不包括运行状况检查API终端节点/healthz，例如/livez、/readyz、和/version。

修复建议：

您应检查集群上已授予 system:anonymous 用户的权限，并确保所有权限都是必需的。如果权限是错误或恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。

有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Discovery:Kubernetes/TorIPCaller

在 Kubernetes 集群中发现资源的API常用方法是从 Tor 出口节点 IP 地址调用的。

默认严重级别：中

- 功能：EKS审核日志

这个发现告诉你，API是从 Tor 出口节点 IP 地址调用的。观察到API的通常用于攻击的发现阶段，攻击者正在收集信息以确定您的 Kubernetes 集群是否容易受到更广泛的攻击。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这种情况可能表明有人未经授权访问您的 Kubernetes 集群，并意图隐藏攻击者的真实身份。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户在需要时调用APIand撤销权限的原因。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意

活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Execution:Kubernetes/ExecInKubeSystemPod

在 **kube-system** 命名空间内的容器组中执行了一条命令

默认严重级别：中

- 功能：EKS审核日志

这一发现告诉你，命令是使用 Kubernetes exec 在 kube-system 命名空间内的 pod 中执行的。API kube-system 命名空间是默认命名空间，主要用于系统级组件，例如 kube-dns 和 kube-proxy 在 kube-system 命名空间下的容器组或容器内执行命令的情况很少见，这种情况可能表明存在可疑活动。

修复建议：

如果意外执行此命令，则用于执行该命令的用户身份凭证可能已被盗用。撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Impact:Kubernetes/MaliciousIPCaller

API 通常用于篡改 Kubernetes 集群中资源的方法是从已知的恶意 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API 操作是从与已知恶意活动关联的 IP 地址调用的。观察到的情况 API 通常与冲击策略有关，在这种策略中，对手试图操纵、中断或销毁您的 AWS 环境中的数据。

修复建议：

如果该 KubernetesUserDetails 部分的调查结果中报告的用户是 system:anonymous，请按照《亚马逊用户指南》中 [亚马逊 EKS 安全最佳实践](#) 中的说明，调查允许匿名 EKS 用户调用 API 和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活

动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Impact:Kubernetes/MaliciousIPCaller.Custom

API通常用于篡改 Kubernetes 集群中资源的方法是从自定义威胁列表上的 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，API操作是从您上传的威胁列表中包含的 IP 地址调用的。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。观察到的情况API通常与冲击策略有关，在这种策略中，对手试图操纵、中断或销毁您的 AWS 环境中的数据。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Impact:Kubernetes/SuccessfulAnonymousAccess

未经身份API验证的用户调用了通常用于篡改 Kubernetes 集群中的资源的方法。

默认严重级别：高

- 功能：EKS审核日志

此发现告知您system:anonymous用户已成功调用某项API操作。API由system:anonymous发出的呼叫未经身份验证。API当攻击者篡改集群中的资源时，观察到的情况通常与攻击的影响阶段有关。此活动表示允许对调查结果中报告的API操作进行匿名或未经身份验证的访问，也可能允许对其他操作进行匿名或未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

修复建议：

您应检查集群上已授予 `system:anonymous` 用户的权限，并确保所有权限都是必需的。如果权限是错误或恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。

有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Impact:Kubernetes/TorIPCaller

API通常用于篡改 Kubernetes 集群中资源的方法是从 Tor 出口节点 IP 地址调用的。

默认严重级别：高

- 功能：EKS审核日志

这个发现告诉你，API是从 Tor 出口节点 IP 地址调用的。API观察到的情况通常与冲击策略有关，在这种策略中，对手试图操纵、中断或销毁您的 AWS 环境中的数据。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这种情况可能表明有人未经授权访问您的 Kubernetes 集群，并意图隐藏攻击者的真实身份。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是`system:anonymous`，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Persistence:Kubernetes/ContainerWithSensitiveMount

启动了挂载有敏感外部主机路径的容器。

默认严重级别：中

- 功能：EKS审核日志

此调查发现通知您，启动的容器配置了在 `volumeMounts` 部分具有写入权限的敏感主机路径。这使敏感主机路径可以从容器内部进行访问和写入。攻击者通常使用这种技术来访问主机的文件系统。

修复建议：

如果意外启动此容器，则用于启动容器的用户身份凭证可能已被盗用。撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果此容器的启动是正常的活动，则建议您使用由基于 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 字段的筛选条件组成的抑制规则。在筛选条件中，`imagePrefix` 字段应与调查发现中指定的 `imagePrefix` 字段相同。要了解有关创建抑制规则的更多信息，请参阅 [抑制规则](#)。

Persistence:Kubernetes/MaliciousIPCaller

从已知的恶意 IP 地址调用了用于获取 Kubernetes 集群持久访问权限的API常用方法。

默认严重级别：中

- 功能：EKS审核日志

此发现告诉您，API操作是从与已知恶意活动关联的 IP 地址调用的。API观察到的情况通常与持久性策略有关，在这种策略中，对手已获得对您的 Kubernetes 集群的访问权限并试图保持该访问权限。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是`system:anonymous`，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Persistence:Kubernetes/MaliciousIPCaller.Custom

从自定义威胁列表上的 IP 地址调用了获取 Kubernetes 集群持久访问权限的API常用方法。

默认严重级别：中

- 功能：EKS审核日志

此发现告诉您，API操作是从您上传的威胁列表中包含的 IP 地址调用的。调查发现详细信息的其他信息部分列有该调查发现所对应的威胁列表。API观察到的情况通常与持久性策略有关，在这种策略中，对手已获得对您的 Kubernetes 集群的访问权限并试图保持该访问权限。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Persistence:Kubernetes/SuccessfulAnonymousAccess

未经身份API验证的用户调用了获取 Kubernetes 集群高级权限的常用方法。

默认严重级别：高

- 功能：EKS审核日志

此发现告知您system:anonymous用户已成功调用某项API操作。API由system:anonymous发出的呼叫未经身份验证。观察到的情况API通常与持久性策略有关，在这种策略中，对手已获得对您的集群的访问权限并试图保持该访问权限。此活动表示允许对调查结果中报告的API操作进行匿名或未经身份验证的访问，也可能允许对其他操作进行匿名或未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

修复建议：

您应检查集群上已授予 system:anonymous 用户的权限，并确保所有权限都是必需的。如果权限是错误或恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。

有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Persistence:Kubernetes/TorIPCaller

API通常用于获取 Kubernetes 集群持久访问权限的方法是从 Tor 出口节点 IP 地址调用的。

默认严重级别：中

- 功能：EKS审核日志

这个发现告诉你，API是从 Tor 出口节点 IP 地址调用的。API观察到的情况通常与持久性策略有关，在这种策略中，对手已获得对您的 Kubernetes 集群的访问权限并试图保持该访问权限。Tor 是用于实现匿名通信的软件。通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这可能表示未经授权访问您的 AWS 资源，目的是隐藏攻击者的真实身份。

修复建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请按照《亚马逊用户指南》中[亚马逊EKS安全最佳实践](#)中的说明，调查允许匿名EKS用户调用API和撤销权限的原因（如有必要）。如果用户经过了身份验证，则应进行调查以确定该活动是合法活动还是恶意活动。如果活动是恶意活动，则撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

默认服务账户被授予了 Kubernetes 集群的管理员权限。

默认严重级别：高

- 功能：EKS审核日志

此调查发现通知您，Kubernetes 集群中命名空间的默认服务账户已被授予管理员权限。Kubernetes 会为集群中的所有命名空间创建一个默认服务账户。还会自动将默认服务帐号作为身份，分配给尚未明确关联到其他服务帐号的容器组。如果默认服务帐号具有管理员权限，则可能会导致容器组无意中以管理员权限启动。如果这类活动不是正常活动，则可能是配置错误或您的凭证已遭到盗用。

修复建议：

不应使用默认服务帐户向容器组授予权限。相反，您应为每个工作负载都分别创建一个专用服务帐户，并根据需要向相应的帐户授予权限。要解决此问题，您应为所有容器组和工作负载创建专用服务帐户，并更新容器组和工作负载以从默认服务帐户迁移到其专用帐户。然后删除默认服务账户的管理员权限。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

Policy:Kubernetes/AnonymousAccessGranted

该system:anonymous用户已获得访问 Kubernetes 集群的API权限。

默认严重级别：高

- 功能：EKS审核日志

此调查发现通知您，Kubernetes 集群上的用户成功创建了 ClusterRoleBinding 或 RoleBinding，以将用户 system:anonymous 绑定到某个角色。这允许对角色允许的API操作进行未经身份验证的访问。如果这类活动不是正常活动，则可能是配置错误或您的凭据遭到盗用。

修复建议：

您应检查已授予集群上的 system:anonymous 用户或 system:unauthenticated 群组的权限，并撤销不必要的匿名访问权限。有关更多信息，请参阅《亚马逊EKS用户指南》EKS中的亚马逊[安全最佳实践](#)。如果权限是恶意授予的，则应撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Policy:Kubernetes/ExposedDashboard

Kubernetes 集群的控制面板已在 Internet 上暴露

默认严重级别：中

- 功能：EKS审核日志

此调查发现通知您，集群的 Kubernetes 控制面板已通过负载均衡器服务在 Internet 上暴露。暴露的控制面板会使他人可从 Internet 访问到集群的管理界面，从而让攻击者利用可能存在的任何身份验证和访问控制漏洞进行攻击操作。

修复建议：

您应确保在 Kubernetes 控制面板上强制执行严格的身份验证和授权。还应实施网络访问控制，以限制特定 IP 地址对控制面板的访问。

有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Policy:Kubernetes/KubeflowDashboardExposed

Kubernetes 集群的 Kubeflow 控制面板已在 Internet 上暴露

默认严重级别：中

- 功能：EKS审核日志

此调查发现通知您，集群的 Kubeflow 控制面板已通过负载均衡器服务在 Internet 上暴露。暴露的 Kubeflow 控制面板会使他人可从 Internet 访问到 Kubeflow 环境的管理界面，从而让攻击者利用可能存在的任何身份验证和访问控制漏洞进行攻击操作。

修复建议：

您应确保在 Kubeflow 控制面板上强制执行严格的身份验证和授权。还应实施网络访问控制，以限制特定 IP 地址对控制面板的访问。

有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

PrivilegeEscalation:Kubernetes/PrivilegedContainer

您的 Kubernetes 集群上启动了一个具有根级访问权限的特权容器。

默认严重级别：中

- 功能：EKS审核日志

此调查发现通知您，您的 Kubernetes 集群上启动了一个特权容器，所使用的镜像以前从未用于启动集群中的特权容器。特权容器具有对主机的根级访问权限。攻击者可以启动特权容器作为权限升级策略，以获得对主机的访问权限，然后攻击主机。

修复建议：

如果意外启动此容器，则用于启动容器的用户身份凭证可能已被盗用。撤销用户的访问权限，并撤销攻击者对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

API通常用于访问机密的 Kubernetes 被异常调用。

默认严重级别：中

- 功能：EKS审核日志

这一发现告诉你，你的集群中的 Kubernetes 用户调用了检索敏感集群机密的异常API操作。观察到的情况API通常与证书访问策略有关，这些策略可能导致权限升级和集群内的进一步访问。如果预计不会出现这种行为，则可能表示配置错误或您的 AWS 凭据已被泄露。

异常检测机器学习 (ML) 模型将观API测结果确定为 GuardDuty 异常。机器学习模型评估EKS集群中的所有用户API活动，并识别与未经授权的用户使用的技术相关的异常事件。机器学习模型跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

检查授予集群中 Kubernetes 用户的权限，并确保所有这些权限都是必需的。如果权限是错误或恶意授予的，请撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

在 RoleBinding 您的 Kubernetes 集群中创建或修改了过于宽松的角色或敏感命名空间的或。 ClusterRoleBinding

默认严重级别：中*

Note

此调查发现的默认严重级别为“中”。但是，如果 RoleBinding或 ClusterRoleBinding 涉及 ClusterRoles admin或cluster-admin，则严重性为“高”。

- 功能：EKS审核日志

这一发现告诉你，你的 Kubernetes 集群中的用户创建了一个RoleBinding或将用户绑定ClusterRoleBinding到具有管理员权限或敏感命名空间的角色。如果预计不会出现这种行为，则可能表示配置错误或您的 AWS 凭据已被泄露。

异常检测机器学习 (ML) 模型将观API测结果确定为 GuardDuty 异常。机器学习模型会评估EKS集群中的所有用户API活动。此机器学习模型还可识别与未经授权的用户使用的技术相关的异常事件。机器学

习模型还跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

检查授予 Kubernetes 用户的权限。这些权限是在和中涉及的角色和主题中RoleBinding定义的ClusterRoleBinding。如果权限是错误或恶意授予的，请撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

Execution:Kubernetes/AnomalousBehavior.ExecInPod

命令是在吊舱内以异常方式执行的。

默认严重级别：中

- 功能：EKS审核日志

这个发现告诉你，命令是使用 Kubernetes exec 在 pod 中执行的。APIKubernetes exec API 允许在 Pod 中运行任意命令。如果预计用户、命名空间或 pod 不会出现这种行为，则可能表示配置错误或您的 AWS 凭据已被泄露。

异常检测机器学习 (ML) 模型将观API测结果确定为 GuardDuty 异常。机器学习模型会评估EKS集群中的所有用户API活动。此机器学习模型还可识别与未经授权的用户使用的技术相关的异常事件。机器学习模型还跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

如果此命令的执行意外发生，则用于执行该命令的用户身份凭证可能已被泄露。撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

工作负载以异常方式使用特权容器启动。

默认严重级别：高

- 功能：EKS审核日志

这一发现告诉您，工作负载是在您的 Amazon EKS 集群中使用特权容器启动的。特权容器具有对主机的根级访问权限。未经授权的用户可以启动特权容器作为一种权限升级策略，首先获得对主机的访问权限，然后对其进行入侵。

异常检测机器学习 (ML) 模型将观察到的容器创建或修改确定为 GuardDuty 异常。机器学习模型评估集 EKS群内的所有用户API和容器镜像活动。此机器学习模型还可识别与未经授权的用户使用的技术相关的异常事件。机器学习模型还会跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理、在您的账户中观察到的容器镜像以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

如果此容器启动是意外的，则用于启动容器的用户身份凭证可能已被泄露。撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

如果预计会启动此容器，则建议您使用带有基于

该resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix字段的筛选条件的抑制规则。在筛选条件中，该imagePrefix字段的值必须与查找结果中指定的imagePrefix字段相同。有关更多信息，请参阅 [抑制规则](#)。

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

工作负载的部署方式异常，在工作负载内安装了敏感的主机路径。

默认严重级别：高

- 功能：EKS审核日志

此发现告诉您，启动工作负载时使用的容器在该volumeMounts部分中包含敏感主机路径。这可能会使敏感的主机路径可以从容器内部访问和写入。未经授权的用户通常使用这种技术来访问主机的文件系统。

异常检测机器学习 (ML) 模型将观察到的容器创建或修改确定为 GuardDuty 异常。机器学习模型评估集 EKS 群内的所有用户 API 和容器镜像活动。此机器学习模型还可识别与未经授权的用户使用的技术相关的异常事件。机器学习模型还会跟踪 API 操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理、在您的账户中观察到的容器镜像以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常 API 请求的详细信息。

修复建议：

如果此容器启动是意外的，则用于启动容器的用户身份凭证可能已被泄露。撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅 [修复可能被泄露的凭证 AWS](#)。

如果预计会启动此容器，则建议您使用带有基于该 `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` 字段的筛选条件的抑制规则。在筛选条件中，该 `imagePrefix` 字段的值必须与查找结果中指定的 `imagePrefix` 字段相同。有关更多信息，请参阅 [抑制规则](#)。

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

工作负载以异常方式启动。

默认严重级别：低*

Note

默认严重性为“低”。但是，如果工作负载包含可能可疑的映像名称（例如已知的 pentest 工具），或者容器在启动时运行可能可疑的命令（例如反向 shell 命令），则此发现类型的严重性将被视为中等。

- 功能：EKS 审核日志

这一发现告诉您，Kubernetes 工作负载是在您的 Amazon 集群中以异常方式创建或修改的，例如 API 活动、新的容器映像或有风险的工作负载配置。EKS 未经授权的用户可以启动容器作为一种策略来执行任意代码，首先获得对主机的访问权限，然后对其进行入侵。

异常检测机器学习 (ML) 模型将观察到的容器创建或修改确定为 GuardDuty 异常。机器学习模型评估集 EKS 群内的所有用户 API 和容器镜像活动。此机器学习模型还可识别与未经授权的用户使用的技术相关

的异常事件。机器学习模型还会跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理、在您的账户中观察到的容器镜像以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

如果此容器启动是意外的，则用于启动容器的用户身份凭证可能已被泄露。撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

如果预计会启动此容器，则建议您使用带有基于该resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix字段的筛选条件的抑制规则。在筛选条件中，该imagePrefix字段的值必须与查找结果中指定的imagePrefix字段相同。有关更多信息，请参阅 [抑制规则](#)。

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

高度宽松的角色或 ClusterRole 是以异常方式创建或修改的。

默认严重级别：低

- 功能：EKS审核日志

这一发现告诉您，您的 Amazon 集群中的 Kubernetes 用户调ClusterRole用了创建Role或具有过多权限的异常API操作。EKSActors 可以使用具有强大权限的角色创建，以避免使用类似管理员的内置角色并避免被发现。过多的权限可能导致权限升级、远程代码执行，并可能导致对命名空间或集群的控制。如果预计不会出现这种行为，则可能表示配置错误或您的凭据已被泄露。

异常检测机器学习 (ML) 模型将观API测结果确定为 GuardDuty 异常。机器学习模型会评估您的 Amazon EKS 集群中的所有用户API活动，并识别与未经授权的用户使用的技术相关的异常事件。机器学习模型还会跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、使用的用户代理、在您的账户中观察到的容器镜像以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

检查Role或中定义的权限，确保ClusterRole需要所有权限并遵循最低权限原则。如果权限是错误或恶意授予的，请撤销用户访问权限并撤销未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

用户以异常方式检查了他们的访问权限。

默认严重级别：低

- 功能：EKS审核日志

这一发现告诉你，你的 Kubernetes 集群中的用户成功检查了是否允许可能导致权限升级和远程代码执行的已知强大权限。例如，用于检查用户权限的常用命令是 `kubectl auth can-i`。如果预计不会出现这种行为，则可能表示配置错误或您的凭据已被泄露。

异常检测机器学习 (ML) 模型将观API测结果确定为 GuardDuty 异常。机器学习模型会评估您的 Amazon EKS 集群中的所有用户API活动，并识别与未经授权的用户使用的技术相关的异常事件。机器学习模型还跟踪API操作的多个因素，例如发出请求的用户、发出请求的位置、正在检查的权限以及用户操作的命名空间。您可以在 GuardDuty 控制台的查找详细信息面板中找到异常API请求的详细信息。

修复建议：

检查授予 Kubernetes 用户的权限，确保所有权限都是必需的。如果权限是错误或恶意授予的，请撤消用户访问权限并撤消未经授权的用户对您的集群所做的任何更改。有关更多信息，请参阅[修复 EKS 审计日志监控调查发现](#)。

如果您的 AWS 凭证遭到泄露，请参阅[修复可能被泄露的凭证 AWS](#)。

运行时监控查找类型

亚马逊 GuardDuty 生成以下运行时监控结果，根据来自亚马逊EKS集群中亚马逊EC2主机和容器、Fargate 和 Amazon 工作负载以及ECS亚马逊EC2实例的操作系统级行为来指出潜在威胁。

Note

运行时系统监控调查发现类型基于从主机收集的运行时系统日志。日志中包含可能被恶意行为者控制的文件路径等字段。这些字段也包含在 GuardDuty 调查结果中，以提供运行时上下文。在 GuardDuty 控制台之外处理运行时监控结果时，必须对查找字段进行消毒。例如，当在网页上显示查找字段时，您可以对其进行HTML编码。

主题

- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)
- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [DefenseEvasion:Runtime/ProcessInjection.Proc](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [DefenseEvasion:Runtime/FilelessExecution](#)
- [Impact:Runtime/CryptoMinerExecuted](#)

- [Execution:Runtime/NewLibraryLoaded](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

CryptoCurrency:Runtime/BitcoinTool.B

Amazon EC2 实例或容器正在查询与加密货币相关活动关联的 IP 地址。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，您 AWS 环境中列出的 EC2 实例或容器正在查询与加密货币相关活动关联的 IP 地址。威胁行为者可能会试图控制计算资源，恶意将这些资源重新用于未经授权的加密货币挖掘。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果您使用此 EC2 实例或容器来挖掘或管理加密货币，或者其中任何一个都参与了区块链活动，则该 CryptoCurrency:Runtime/BitcoinTool.B 发现可能代表您的环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 CryptoCurrency:Runtime/BitcoinTool.B。第二个筛选条件应该是实例的实例 ID 或容器的容器镜像 ID，此类实例或容器涉及加密货币或区块链相关活动。有关更多信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅[修复运行时监控结果](#)。

Backdoor:Runtime/C&CActivity.B

Amazon EC2 实例或容器正在查询与已知命令和控制服务器关联的 IP。

默认严重级别：高

- 特征：运行时系统监控

此发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在查询与已知命令和控制 (C&C) 服务器关联的 IP。列出的实例或容器可能会被盗用。命令和控制服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是一组联网的设备，可能包括服务器 PCs、移动设备和物联网设备，这些设备受到一种常见的恶意软件的感染和控制。僵尸网络通常用于分发恶意软件和收集不当信息，例如信用卡号。根据僵尸网络的目的和结构，C&C 服务器还可能发出命令开始分布式拒绝服务 (DDoS) 攻击。

Note

如果查询的 IP 与 log4j 相关，则关联调查发现的字段将包含以下值：

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

UnauthorizedAccess:Runtime/TorRelay

您的 Amazon EC2 实例或容器正在作为 Tor 中继与 Tor 网络建立连接。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉你，你 AWS 环境中的 EC2 实例或容器正在与 Tor 网络建立连接，这表明它充当 Tor 中继。Tor 是用于实现匿名通信的软件。Tor 通过将客户端可能的非法流量从一个 Tor 中继转发到另一个 Tor 中继，来提高通信的匿名程度。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

UnauthorizedAccess:Runtime/TorClient

您的 Amazon EC2 实例或容器正在与 Tor Guard 或授权节点建立连接。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，您的 AWS 环境中的 EC2 实例或容器正在与 Tor Guard 或 Authority 节点建立连接。Tor 是用于实现匿名通信的软件。Tor Guard 和 Authority 节点充当 Tor 网络的初始网关。此流量可能表明此 EC2 实例或容器可能已遭到入侵，并且正在充当 Tor 网络上的客户端。这一发现可能表明有人未经授权访问您的 AWS 资源，目的是隐藏攻击者的真实身份。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/BlackholeTraffic

Amazon EC2 实例或容器正在尝试与已知黑洞的远程主机的 IP 地址进行通信。

默认严重级别：中

- 特征：运行时系统监控

这一发现告诉您，列出的EC2实例或 AWS 环境中的容器可能因为尝试与黑洞（或沉孔）的 IP 地址通信而受到威胁。黑洞是网络中的一些位置，在这些位置中会将传入或传出流量静默丢弃，而不向源通知数据未达到源目标接收方。黑洞 IP 地址指定没有运行的主机或者未分配主机的地址。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/DropPoint

Amazon EC2 实例或容器正试图与远程主机的 IP 地址进行通信，该主机已知该地址持有恶意软件捕获的凭证和其他被盗数据。

默认严重级别：中

- 特征：运行时系统监控

这一发现告诉您，您 AWS 环境中的EC2实例或容器正试图与远程主机的 IP 地址通信，该主机已知该地址持有恶意软件捕获的凭证和其他被盗数据。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Amazon EC2 实例或容器正在查询与加密货币活动关联的域名。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，您 AWS 环境中列出的 EC2 实例或容器正在查询与比特币或其他加密货币相关活动关联的域名。威胁行为者可能会试图控制计算资源，从而恶意将这些资源重新用于未经授权的加密货币挖掘。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果您使用此 EC2 实例或容器来挖掘或管理加密货币，或者其中任何一个都参与了区块链活动，则该 `CryptoCurrency:Runtime/BitcoinTool.B!DNS` 发现可能是您环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 `CryptoCurrency:Runtime/BitcoinTool.B!DNS`。第二个筛选条件应是实例的实例 ID 或容器的容器镜像 ID，该实例或容器涉及加密货币或区块链活动。有关更多信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅[修复运行时监控结果](#)。

Backdoor:Runtime/C&CActivity.B!DNS


Amazon EC2 实例或容器正在查询与已知命令和控制服务器关联的域名。

默认严重级别：高

- 特征：运行时系统监控

此发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在查询与已知命令和控制 (C&C) 服务器关联的域名。列出的 EC2 实例或容器可能遭到入侵。命令和控制服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是一组联网的设备，其中可能包括服务器 PCs、移动设备和物联网设备，这些设备被一种常见的恶意软件感染和控制。僵尸网络通常用于分发恶意软件和收集不当信息，例如信用卡号。根据僵尸网络的目的和结构，C&C 服务器还可能发出命令开始分布式拒绝服务 (DDoS) 攻击。

 Note

如果查询的域名与 `log4j` 相关，则相关调查发现的字段将包含以下值：

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

Note

要测试如何 GuardDuty 生成此查找类型，您可以从您的实例（用 dig 于 Linux 或 Windows nslookup s）向测试域 DNS 发出请求 `guardduty2activityb.com`。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/BlackholeTraffic!DNS

Amazon EC2 实例或容器正在查询被重定向到黑洞 IP 地址的域名。

默认严重级别：中

- 特征：运行时系统监控

此发现通知您列出的 EC2 实例或 AWS 环境中的容器可能由于查询的域名被重定向到黑洞 IP 地址而受到威胁。黑洞是网络中的一些位置，在这些位置中会将传入或传出流量静默丢弃，而不向源通知数据未到达源目标接收方。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/DropPoint!DNS

Amazon EC2 实例或容器正在查询远程主机的域名，该域名已知包含恶意软件捕获的凭证和其他被盗数据。

默认严重级别：中

- 特征：运行时系统监控

这一发现告诉您，您 AWS 环境中的 EC2 实例或容器正在查询远程主机的域名，该域名已知包含恶意软件捕获的凭据和其他被盗数据。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/DGADomainRequest.C!DNS

Amazon EC2 实例或容器正在查询通过算法生成的域。此类域名通常被恶意软件使用，可能表示 EC2 实例或容器遭到入侵。

默认严重级别：高

- 特征：运行时系统监控

此发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在尝试查询域生成算法 (DGA) 域。您的资源可能已被盗用。

DGAs 用于定期生成大量域名，这些域名可用作指挥和控制 (C&C) 服务器的集合点。命令和控制服务器是向僵尸网络的成员发布命令的计算机，僵尸网络是感染了相同类型恶意软件，并受其控制的一组连接到 Internet 的设备。大量潜在汇聚点的存在，使得有效关闭僵尸网络非常困难，因为受感染的计算机尝试每天与这样一些域名联系来接收更新或命令。

Note

这一发现基于 GuardDuty 威胁情报源中的已知 DGA 域。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/DriveBySourceTraffic!DNS

Amazon EC2 实例或容器正在查询远程主机的域名，该域名是已知的 Drive-By 下载攻击来源。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，列出的 EC2 实例或 AWS 环境中的容器可能受到威胁，因为它正在查询远程主机的域名，而该域名是已知的偷渡式下载攻击来源。这些是来自 Internet 的恶意计算机软件下载，可能会触发自动安装病毒、间谍软件或恶意软件。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Trojan:Runtime/PhishingDomainRequest!DNS

Amazon EC2 实例或容器正在查询网络钓鱼攻击中涉及的域名。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，您的 AWS 环境中有一个 EC2 实例或容器正在尝试查询涉及网络钓鱼攻击的域。网络钓鱼域由冒充合法机构的人设置，其目的是引诱个人提供敏感数据，如个人可识别信息、银行和信用卡信息、密码等。您的 EC2 实例或容器可能正在尝试检索存储在网络钓鱼网站上的敏感数据，或者可能正在尝试设置网络钓鱼网站。您的 EC2 实例或容器可能遭到入侵。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Impact:Runtime/AbusedDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与已知滥用域名关联的低信誉域名。

默认严重级别：中

- 特征：运行时系统监控

此发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在查询与已知的滥用域或 IP 地址关联的低信誉域名。滥用域名的例子包括提供免费子域名注册的顶级域名 (TLDs/LDs) 和二级域名 (2) 以及动态提供商。DNS 威胁行为者往往利用这些服务免费或低成本注册域名。这类低信誉域也可能是解析到注册商 Parking IP 地址的过期域，因此可能不再处于活跃状态。Parking IP 是注册商为未链接到任何服务的域引导流量的位置。由于威胁行为者通常使用这些注册商或服务进行 C&C 和恶意软件分发，因此列出的 Amazon EC2 实例或容器可能会遭到入侵。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Impact:Runtime/BitcoinDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与加密货币相关活动关联的低信誉域名。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在查询与比特币或其他加密货币相关活动相关的低信誉域名。威胁行为者可能会试图控制计算资源，恶意将这些资源重新用于未经授权的加密货币挖掘。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果您使用此 EC2 实例或容器来挖掘或管理加密货币，或者如果这些资源以其他方式参与区块链活动，则此发现可能代表您的环境的预期活动。如果您的 AWS 环境中出现这种情况，我们建议您为此发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 `Impact:Runtime/BitcoinDomainRequest.Reputation`。第二个筛选条件应是实例的实例 ID 或容器的容器镜像 ID，此类实例或容器涉及加密货币或区块链相关活动。有关更多信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅[修复运行时监控结果](#)。

Impact:Runtime/MaliciousDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与已知恶意域关联的低信誉域。

默认严重级别：高

- 特征：运行时系统监控

此发现告诉您，列出的 EC2 实例或 AWS 环境中的容器正在查询与已知恶意域或 IP 地址关联的低信誉域名。例如，域可能与已知的陷穴 IP 地址相关联。Sinkholed 域是以前由威胁行为者控制的域，如果向该域发出请求则可能表明该实例已被盗用。这些域也可能与已知的恶意活动或域生成算法相关。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Impact:Runtime/SuspiciousDomainRequest.Reputation

Amazon EC2 实例或容器正在查询信誉较低的域名，该域名由于过时或受欢迎程度低而具有可疑性。

默认严重级别：低

- 特征：运行时系统监控

这一发现告诉您，列出的EC2实例或您 AWS 环境中的容器正在查询一个被怀疑为恶意的低信誉域名。注意到该域的特征与先前观察到的恶意域一致，但是，我们的信誉模型无法将其与已知威胁明确关联起来。这些域通常是新近观察到的，或者接收到的流量较少。

低信誉域基于信誉评分模型进行评估。该模型对域的特征进行评估和排序，以确定其是否可能是恶意域。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

UnauthorizedAccess:Runtime/MetadataDNSRebind

Amazon EC2 实例或容器正在执行解析到实例元数据服务的DNS查询。

默认严重级别：高

- 特征：运行时系统监控

Note

目前，只有AMD64架构支持这种查找类型。

这一发现告诉您，您的 AWS 环境中的 EC2 实例或容器正在查询解析为 EC2 元数据 IP 地址 (169.254.169.254) 的域。此类 DNS 查询可能表明该实例是 DNS 重新绑定技术的目标。此技术可用于从 EC2 实例获取元数据，包括与该实例关联的 IAM 证书。

DNS 重新绑定涉及欺骗在 EC2 实例上运行的应用程序加载来自的返回数据 URL，其中中的域名 URL 解析为 EC2 元数据 IP 地址 (169.254.169.254)。这会导致应用程序访问 EC2 元数据，并可能将其提供给攻击者。

只有当实例运行允许注入的易受攻击的应用程序，或者有人在 EC2 实例上运行的 Web 浏览器 URL 中访问 EC2 元数据时 URLs，才可以使用 DNS 重新绑定来访问元数据。EC2

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

针对这一发现，您应该评估 EC2 实例或容器上是否有易受攻击的应用程序在运行，或者是否有人使用浏览器访问了调查结果中确定的域。如果根本原因在于有漏洞的应用程序，则修复漏洞。如果是由于某用户已浏览标识的域，则阻止该域或阻止用户进行访问。如果您确定此发现与上述任一案例有关，请[撤消与该 EC2 实例关联的会话](#)。

一些 AWS 客户故意将元数据 IP 地址映射到其权威 DNS 服务器上的域名。如果您的环境中出现这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 `UnauthorizedAccess:Runtime/MetaDataDNSRebind`。第二个筛选条件应该是 DNS 请求域或容器的容器镜像 ID。DNS 请求域值应与您映射到元数据 IP 地址 (169.254.169.254) 的域相匹配。有关创建抑制规则的信息，请参阅[抑制规则](#)。

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅[修复运行时监控结果](#)。

Execution:Runtime/NewBinaryExecuted

已执行容器中新创建或最近修改的二进制文件。

默认严重级别：中

- 特征：运行时系统监控

此调查发现通知您，容器中新创建或最近修改的二进制文件已执行。最佳做法是保持容器在运行时系统不可变，并且不应在容器的生命周期内创建或修改二进制文件、脚本或库。此行为表示获得容器访问权

限的恶意行为者下载并执行了恶意软件或其他软件，这是潜在入侵的一部分。尽管这种类型的活动可能表明存在漏洞，但它也是一种常见的使用模式。因此，GuardDuty 使用机制来识别此活动的可疑实例，并仅针对可疑实例生成此发现类型。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/DockerSocketAccessed

容器内的进程正在使用 Docker 套接字与 Docker 进程守护程序通信。

默认严重级别：中

- 特征：运行时系统监控

Docker 套接字是一个 Unix 域套接字，Docker 进程守护程序 (dockerd) 用以与其客户端进行通信。客户端可以执行各种操作，例如通过 Docker 套接字与 Docker 进程守护程序通信来创建容器。容器进程访问 Docker 套接字是可疑的。容器进程可以通过与 Docker 套接字通信并创建特权容器，来脱离容器并获得主机级访问权限。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/RuncContainerEscape

检测到有人企图通过 runC 逃出容器。

默认严重级别：高

- 特征：运行时系统监控

runC 是高级容器运行时（例如 Docker 和 Containerd）用来生成和运行容器的低级容器运行时。runC 始终以 root 权限执行，因为它需要执行创建容器的低级任务。威胁行为者可以通过修改或利用 runC 二进制文件中的漏洞来获得主机级别的访问权限。

此发现可检测到 runC 二进制文件的修改以及利用以下 runC 漏洞的潜在尝试：

- [CVE-2019-5736](#)— 利用漏洞 CVE-2019-5736 包括从容器内覆盖 runC 二进制文件。当容器内的进程修改 runC 二进制文件时，就会调用此发现。
- [CVE-2024-21626](#)— 利用漏洞 CVE-2024-21626 包括将当前工作目录 (CWD) 或容器设置为打开的文件描述符/proc/self/fd/*FileDescriptor*。例如，当检测到包含当前工作目录的容器进程/proc/self/fd/时，就会调用此发现/proc/self/fd/7。

这一发现可能表明恶意行为者试图在以下容器类型之一中进行漏洞：

- 带有攻击者控制图像的新容器。
- 拥有主机级 runC 二进制文件写入权限的操作者可以访问的现有容器。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

检测到有人企图通过CGroups释放剂逃出容器。

默认严重级别：高

- 特征：运行时系统监控

此调查发现通知您，已检测到有人试图修改控制组 (cgroup) 发布代理文件。Linux 使用控制组 (cgroup) 来限制、说明和隔离一组进程的资源使用情况。每个控制组都有一个发布代理文件 (release_agent)，该文件是一个脚本，当控制组内的任何进程终止时，Linux 会执行该脚本。发布代理文件始终在主机级别执行。通过向属于某个 cgroup 的发布代理文件写入任意命令，容器内的攻击者可以逃逸到主机。当该控制组内部的进程终止时，就会执行威胁行为者编写的命令。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

DefenseEvasion:Runtime/ProcessInjection.Proc

在容器或 Amazon EC2 实例中检测到使用 proc 文件系统的进程注入。

默认严重级别：高

- 特征：运行时系统监控

进程注入是威胁行为者使用的一种技术，用来向进程注入代码以逃避防御，并有可能提升权限。proc 文件系统 (procfs) 是 Linux 中的一种特殊文件系统，以文件的形式呈现进程的虚拟内存。该文件的路径是 /proc/PID/mem，其中 PID 是进程的唯一 ID。威胁行为者可以写入此文件，以向该进程注入代码。此调查发现可识别他人可能尝试向该文件的写入操作。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源类型可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

DefenseEvasion:Runtime/ProcessInjection.Ptrace

在容器或 Amazon EC2 实例中检测到使用 ptrace 系统调用的进程注入。

默认严重级别：中

- 特征：运行时系统监控

进程注入是威胁行为者使用的一种技术，用来向进程注入代码以逃避防御，并有可能提升权限。某个进程可以使用 ptrace 系统调用，将代码注入另一个进程。此调查发现可识别他人可能尝试使用 ptrace 系统调用向进程注入代码的操作。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源类型可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

在容器或 Amazon EC2 实例中检测到通过直接写入虚拟内存进行进程注入。

默认严重级别：高

- 特征：运行时系统监控

进程注入是威胁行为者使用的一种技术，用来向进程注入代码以逃避防御，并有可能提升权限。进程可以使用系统调用，例如 `process_vm_writew` 直接向另一个进程的虚拟内存注入代码。此调查发现可识别他人可能尝试使用系统调用向进程注入代码，从而向该进程的虚拟内存进行写入操作。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源类型可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Execution:Runtime/ReverseShell

容器或 Amazon EC2 实例中的进程创建了反向外壳。

默认严重级别：高

- 特征：运行时系统监控

反向 Shell 是一种在连接上创建的 Shell 会话，该连接从目标主机到威胁行为者主机。反向 Shell 与从攻击者主机向目标主机发起的普通 Shell 相反。威胁行为者在获得对目标的初始访问权限后，会创建一个反向 Shell 对目标执行命令。此调查发现可识别创建反向 Shell 的潜在尝试。

修复建议：

如果此活动是意外活动，则您的资源类型可能已被盗用。

DefenseEvasion:Runtime/FilelessExecution

容器或 Amazon EC2 实例中的进程正在执行内存中的代码。

默认严重级别：中

- 特征：运行时系统监控

当使用磁盘上的内存中可执行文件执行进程时，此调查发现会告知您这一情况。这是一种常见的防御逃避技术，可避免将恶意可执行文件写入磁盘，以逃避基于文件系统扫描的检测。尽管这种技术被恶意软件利用，但也有一些合法的用例。其中一个例子是 just-in-time (JIT) 编译器，它将编译后的代码写入内存并从内存中执行。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Impact:Runtime/CryptoMinerExecuted

容器或 Amazon EC2 实例正在执行与加密货币挖矿活动关联的二进制文件。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，您的 AWS 环境中的容器或 EC2 实例正在执行与加密货币挖矿活动关联的二进制文件。威胁行为者可能会试图控制计算资源，恶意将这些资源重新用于未经授权的加密货币挖掘。

运行时系统代理监控来自多种资源类型的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的查找结果面板中查看资源类型。

修复建议：

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型并查看[修复运行时监控结果](#)。

Execution:Runtime/NewLibraryLoaded

新创建或最近修改的库由容器内的进程加载。

默认严重级别：中

- 特征：运行时系统监控

此调查发现通知您，运行时系统期间在容器内创建或修改了库，并由在容器内运行的进程加载。最佳做法是保持容器在运行时系统不可变，不要在容器的生命周期内创建或修改二进制文件、脚本或库。在容器中加载新创建或修改的库，可能代表可疑活动。此行为表明，恶意行为者可能已获得对容器的访问权限，下载并执行了恶意软件或其他软件，属于潜在攻击行为的一部分。尽管这种类型的活动可能表明存在漏洞，但它也是一种常见的使用模式。因此，GuardDuty 使用机制来识别此活动的可疑实例，并仅针对可疑实例生成此发现类型。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅[修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

容器内的进程在运行时系统挂载了主机文件系统。

默认严重级别：中

- 特征：运行时系统监控

多种容器逃逸技术都包括在运行时将主机文件系统挂载到容器内。此调查发现通知您，容器内的进程可能尝试挂载主机文件系统，可能表明有人试图逃逸到主机。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/UserfaultfdUsage

进程使用 **userfaultfd** 系统调用来处理用户空间中的页面错误。

默认严重级别：中

- 特征：运行时系统监控

通常，页面错误由内核在内核空间中处理。但是，userfaultfd 系统调用允许进程在用户空间中处理文件系统上的页面错误。此功能十分实用，可以实施用户空间文件系统。而且，潜在的恶意进程也可以利用此功能从用户空间中断内核。使用 userfaultfd 系统调用中断内核是一种常见的利用技术，用于在利用内核竞争条件时延长竞争窗口有效期限。使用userfaultfd可能表示亚马逊弹性计算云 (AmazonEC2) 实例上存在可疑活动。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Execution:Runtime/SuspiciousTool

容器或 Amazon EC2 实例正在运行二进制文件或脚本，该文件或脚本经常用于攻击性安全场景，例如渗透测试活动。

默认严重级别：可变

这一发现的严重程度可以是高或低，这取决于检测到的可疑工具是双重用途还是仅用于攻击性用途。

- 特征：运行时系统监控

此发现告知您已在您的 AWS 环境中的 EC2 实例或容器上执行了可疑工具。这包括渗透测试活动中使用的工具，也称为后门工具、网络扫描仪和网络嗅探器。所有这些工具都可以在良性环境中使用，但也经常被具有恶意意图的威胁行为者使用。观察攻击性安全工具可能表明关联的 EC2 实例或容器已遭到入侵。

GuardDuty 检查相关的运行时活动和上下文，以便只有当关联的活动和上下文可能存在可疑时，它才会生成此结果。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Execution:Runtime/SuspiciousCommand

已在 Amazon EC2 实例或容器上执行了可疑命令，表明存在漏洞。

默认严重级别：可变

根据观察到的恶意模式的影响，这种发现类型的严重性可以是低、中或高。

- 特征：运行时系统监控

此发现告知您已执行可疑命令，并表明您 AWS 环境中的某个 Amazon EC2 实例或容器已遭到入侵。这可能意味着要么是从可疑来源下载文件然后执行的，要么正在运行的进程在其命令行中显示已知的恶意模式。这进一步表明系统上正在运行恶意软件。

GuardDuty 检查相关的运行时活动和上下文，以便只有当关联的活动和上下文可能存在可疑时，它才会生成此结果。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

DefenseEvasion:Runtime/SuspiciousCommand

命令已在列出的 Amazon EC2 实例或容器上执行，它试图修改或禁用 Linux 防御机制，例如防火墙或基本系统服务。

默认严重级别：可变

根据修改或禁用的防御机制，此发现类型的严重性可以是高、中或低。

- 特征：运行时系统监控

此发现告诉您，已执行了一个试图向本地系统的安全服务隐藏攻击的命令。这包括禁用 Unix 防火墙、修改本地 IP 表、删除 crontab 条目、禁用本地服务或接管 LDPreload 功能等操作。任何修改都是高度可疑的，并且是潜在的泄露迹象。因此，这些机制可以检测或防止系统的进一步损害。

GuardDuty 检查相关的运行时活动和上下文，以便只有当关联的活动和上下文可能存在可疑时，它才会生成此结果。

运行时系统代理监控来自多个资源的事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台的发现结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

DefenseEvasion:Runtime/PtraceAntiDebugging

容器或 Amazon EC2 实例中的进程已使用 ptrace 系统调用执行了反调试措施。

默认严重级别：低

- 特征：运行时系统监控

这一发现表明，在 Amazon EC2 实例或您 AWS 环境中的容器上运行的进程使用了带有 PTRACE_TRACEME 选项的 ptrace 系统调用。此活动会导致连接的调试器与正在运行的进程分离。如果未连接调试器，则无效。但是，这种活动本身就引起了人们的怀疑。这可能表明系统上正在运行恶意软件。恶意软件经常使用反调试技术来逃避分析，这些技术可以在运行时被检测到。

GuardDuty 检查相关的运行时活动和上下文，以便只有当关联的活动和上下文可能存在可疑时，它才会生成此结果。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Execution:Runtime/MaliciousFileExecuted

已在 Amazon EC2 实例或容器上执行了已知的恶意可执行文件。

默认严重级别：高

- 特征：运行时系统监控

这一发现告诉您，已在 Amazon EC2 实例或您 AWS 环境中的容器上执行了已知的恶意可执行文件。这有力地表明实例或容器可能遭到入侵，并且恶意软件已被执行。

恶意软件经常使用反调试技术来逃避分析，这些技术可以在运行时被检测到。

GuardDuty 检查相关的运行时活动和上下文，以便只有当关联的活动和上下文可能存在可疑时，它才会生成此结果。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

Execution:Runtime/SuspiciousShellCreated

Amazon EC2 实例或容器中的网络服务或可通过网络访问的进程已启动交互式 shell 进程。

默认严重级别：低

- 特征：运行时系统监控

这一发现告诉您，Amazon EC2 实例或您 AWS 环境中的容器中可通过网络访问的服务已启动交互式 shell。在某些情况下，这种情况可能表示漏洞利用后的行为。交互式外壳允许攻击者对受感染的实例或容器执行任意命令。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。您可以在父进程详细信息中查看可通过网络访问的进程信息。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

PrivilegeEscalation:Runtime/ElevationToRoot

在列出的 Amazon EC2 实例或容器上运行的进程已使用根权限。

默认严重级别：中

- 特征：运行时系统监控

这一发现告诉您，在列出的 Amazon EC2 或您的 AWS 环境中列出的容器中运行的进程通过异常或可疑的 setuid 二进制文件执行获得了根权限。这表明正在运行的进程可能受到威胁，EC2 例如通过漏洞利用或 setuid 利用漏洞。通过使用根权限，攻击者有可能在实例或容器上执行命令。

虽然旨在不 GuardDuty 为涉及经常使用该 sudo 命令的活动生成这种发现类型，但是当它识别出该活动为异常或可疑时，它就会生成此发现。

GuardDuty 检查相关的运行时活动和上下文，并仅在关联的活动和上下文异常或可疑时才生成此发现类型。

运行时系统代理监控来自多个资源的事件。要识别受影响的资源，请在 GuardDuty 控制台的调查结果详细信息中查看资源类型。

修复建议：

如果此活动是意外活动，则您的资源可能已被盗用。有关更多信息，请参阅 [修复运行时监控结果](#)。

适用于 EC2 查找类型的恶意软件防护

GuardDuty EC2 恶意软件防护为 EC2 提供了单一的恶意软件防护，可查找在扫描 EC2 实例或容器工作负载期间检测到的所有威胁。该调查发现包括扫描期间检测到的总数，并根据严重性提供检测到的

前 32 个威胁的详细信息。与其他 GuardDuty 发现不同，再次扫描相同的 EC2 实例或容器工作负载时，EC2 的恶意软件防护发现不会更新。

每次检测到恶意软件的扫描都会生成新的适用于 EC2 的恶意软件保护结果。EC2 恶意软件防护调查结果包括有关生成该发现的相应扫描以及启动该扫描的 GuardDuty 发现的信息。这样更容易将可疑行为与检测到的恶意软件关联起来。

Note

当 GuardDuty 检测到容器工作负载上的恶意活动时，EC2 恶意软件防护不会生成 EC2 级别的发现结果。

以下发现特定于 EC2 的 GuardDuty 恶意软件防护。

主题

- [Execution:EC2/MaliciousFile](#)
- [Execution:ECS/MaliciousFile](#)
- [Execution:Kubernetes/MaliciousFile](#)
- [Execution:Container/MaliciousFile](#)
- [Execution:EC2/SuspiciousFile](#)
- [Execution:ECS/SuspiciousFile](#)
- [Execution:Kubernetes/SuspiciousFile](#)
- [Execution:Container/SuspiciousFile](#)

Execution:EC2/MaliciousFile

在 EC2 实例上检测到恶意文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在您的 AWS 环境中列出的 EC2 实例上检测到一个或多个恶意文件。列出的实例可能被盗用。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Execution:ECS/MaliciousFile

在 ECS 集群上检测到恶意文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在属于 ECS 集群的容器工作负载上检测到一个或多个恶意文件。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

修复建议：

如果此活动是意外活动，则属于 ECS 集群的容器可能被盗用。有关更多信息，请参阅 [修复可能受损的集群 ECS](#)。

Execution:Kubernetes/MaliciousFile

在 Kubernetes 集群上检测到恶意文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在属于 Kubernetes 集群的容器工作负载上检测到一个或多个恶意文件。如果这是 EKS 托管集群，则调查发现详细信息将提供有关受影响的 EKS 资源的其他信息。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

修复建议：

如果此活动是意外活动，则您的容器工作负载可能被盗用。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Execution:Container/MaliciousFile

在独立容器上检测到恶意文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在容器工作负载上检测到一个或多个恶意文件，但未发现任何集群信息。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

修复建议：

如果此活动是意外活动，则您的容器工作负载可能被盗用。有关更多信息，请参阅 [修复可能受损的独立容器](#)。

Execution:EC2/SuspiciousFile

在 EC2 实例上检测到可疑文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

此发现表明 EC2 GuardDuty 恶意软件防护扫描已在 EC2 实例上检测到一个或多个可疑文件。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

SuspiciousFile 类型检测表明受影响的资源上存在可能不需要的程序，例如广告软件、间谍软件或两用工具。这些程序可能会对您的资源产生负面影响，或者被攻击者用于恶意目的。例如，攻击者可以将网络工具合法或恶意用作黑客工具，企图破坏资源。

检测到可疑文件后，请评估是否希望在您的 AWS 环境中看到检测到的文件。如果文件是意外文件，请按照下一部分提供的修复建议进行修复。

修复建议：

如果此活动是意外活动，则您的实例可能被盗用。有关更多信息，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

Execution:ECS/SuspiciousFile

在 ECS 集群上检测到可疑文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

此发现表明 EC2 GuardDuty 恶意软件防护扫描已在属于 ECS 集群的容器上检测到一个或多个可疑文件。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

SuspiciousFile 类型检测表明受影响的资源上存在可能不需要的程序，例如广告软件、间谍软件或两用工具。这些程序可能会对您的资源产生负面影响，或者被攻击者用于恶意目的。例如，攻击者可以将网络工具合法或恶意用作黑客工具，企图破坏资源。

检测到可疑文件后，请评估是否希望在您的 AWS 环境中看到检测到的文件。如果文件是意外文件，请按照下一部分提供的修复建议进行修复。

修复建议：

如果此活动是意外活动，则属于 ECS 集群的容器可能被盗用。有关更多信息，请参阅 [修复可能受损的集群 ECS](#)。

Execution:Kubernetes/SuspiciousFile

在 Kubernetes 集群上检测到可疑文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在属于 Kubernetes 集群的容器上检测到一个或多个可疑文件。如果这是 EKS 托管集群，则调查发现详细信息将提供有关受影响的 EKS 的其他信息。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

SuspiciousFile 类型检测表明受影响的资源上存在可能不需要的程序，例如广告软件、间谍软件或两用工具。这些程序可能会对您的资源产生负面影响，或者被攻击者用于恶意目的。例如，攻击者可以将网络工具合法或恶意用作黑客工具，企图破坏资源。

检测到可疑文件后，请评估是否希望在您的 AWS 环境中看到检测到的文件。如果文件是意外文件，请按照下一部分提供的修复建议进行修复。

修复建议：

如果此活动是意外活动，则您的容器工作负载可能被盗用。有关更多信息，请参阅 [修复 EKS 审计日志监控调查发现](#)。

Execution:Container/SuspiciousFile

在独立容器上检测到可疑文件。

默认严重级别：因检测到的威胁而异。

- 功能：EBS 恶意软件防护

这一发现表明，EC2 GuardDuty 恶意软件防护扫描已在没有集群信息的容器上检测到一个或多个可疑文件。有关更多信息，请参阅调查发现详细信息中的检测到的威胁部分。

SuspiciousFile 类型检测表明受影响的资源上存在可能不需要的程序，例如广告软件、间谍软件或两用工具。这些程序可能会对您的资源产生负面影响，或者被攻击者用于恶意目的。例如，攻击者可以将网络工具合法或恶意用作黑客工具，企图破坏资源。

检测到可疑文件后，请评估是否希望在您的 AWS 环境中看到检测到的文件。如果文件是意外文件，请按照下一部分提供的修复建议进行修复。

修复建议：

如果此活动是意外活动，则您的容器工作负载可能被盗用。有关更多信息，请参阅 [修复可能受损的独立容器](#)。

适用于 S3 查找类型的恶意软件防护

GuardDuty 仅当它检测到您的潜在安全威胁时才会生成调查结果 AWS 账户。S3 恶意软件防护的发现表明，启动恶意软件扫描的已上传对象包含潜在的恶意文件。

GuardDuty 要让 Amazon 在您的中生成调查结果 AWS 账户，请同时启用 S3 GuardDuty 和“恶意软件防护”。最佳做法是先启用 S3 的恶意软件防护，GuardDuty 然后再启用。如果此顺序与您不同，请确保在 S3 对象上传到您的受保护存储桶 GuardDuty 之前启用。

Note

GuardDuty 无法为启用之前扫描的 S3 对象生成查找结果 GuardDuty。要扫描现有 S3 对象，您可以重新上传该对象。

Object:S3/MaliciousFile

已在扫描的 S3 对象上检测到恶意文件。

默认严重级别：高

- 功能：S3 的恶意软件防护

此发现表明恶意软件扫描已检测到列出的 S3 对象为恶意对象。有关更多信息，请查看查找结果详细信息面板中的“检测到的威胁”部分。

建议补救措施：

如果这一发现出乎意料，那么 S3 对象可能是恶意的。有关建议的补救步骤的信息，请参见[修复可能有恶意的 S3 对象](#)。

GuardDuty RDS 保护查找类型

GuardDuty RDS Protection 可检测数据库实例上的异常登录行为。以下调查结果特定于 S3 存储桶资源，并且始终具有 Resource Type (资源类型)。调查结果的严重性和详细信息将因调查结果类型而异。

主题

- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.FailedLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce](#)
- [CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/MaliciousIPCaller.FailedLogin](#)
- [Discovery:RDS/MaliciousIPCaller](#)
- [CredentialAccess:RDS/TorIPCaller.SuccessfulLogin](#)

- [CredentialAccess:RDS/TorIPCaller.FailedLogin](#)
- [Discovery:RDS/TorIPCaller](#)

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

用户以异常方式成功登录到您账户中的 RDS 数据库。

默认严重性：可变

Note

根据与此发现相关的异常行为，默认严重性可以是“低”、“中”和“高”。

- 低 — 如果与此发现关联的用户名是从与私有网络关联的 IP 地址登录的。
- 中 — 如果与该发现关联的用户名是从公有 IP 地址登录的。
- 高-如果公有 IP 地址的登录尝试失败的模式持续存在，则表明访问策略过于宽松。

- 功能：RDS 登录活动监控

这一发现告诉您，在您的环境中，在 RDS 数据库上观察到异常成功登录。AWS 这可能表示之前的隐身用户首次登录到 RDS 数据库。常见的情况是内部用户登录数据库，该数据库由应用程序而不是单个用户以编程方式访问。

GuardDuty Machine Learning (ML) 模型将这种成功登录识别为异常。机器学习模型会评估您的所有数据库登录事件，[支持的亚马逊 Aurora 和亚马逊 RDS 数据库](#) 并识别与对手使用的技术相关的异常事件。机器学习模型跟踪 RDS 登录活动的各种因素，例如发出请求的用户、发出请求的位置以及使用的特定数据库连接详细信息。有关可能异常的登录事件的信息，请参阅[RDS 基于登录活动的异常](#)。

修复建议：

如果关联的数据库意外出现此活动，建议更改关联数据库用户的密码，并查看可用的审计日志，了解异常用户执行的活动。中等和高严重性的发现可能表明对数据库的访问策略过于宽松，并且用户凭据可能已被暴露或泄露。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过成功登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

在您账户的 RDS 数据库上观察到一次或多次异常的登录尝试失败。

默认严重级别：低

- 功能：RDS 登录活动监控

此发现告诉您，在您的环境中的 RDS 数据库上发现了一个或多个异常登录失败。AWS 来自公有 IP 地址的登录尝试失败可能表明您账户中的 RDS 数据库遭到潜在恶意行为者的暴力攻击。

GuardDuty 异常检测机器学习 (ML) 模型将这些失败的登录识别为异常。机器学习模型会评估您的所有数据库登录事件，[支持的亚马逊 Aurora 和亚马逊 RDS 数据库](#) 并识别与对手使用的技术相关的异常事件。机器学习模型跟踪 RDS 登录活动的各种因素，例如发出请求的用户、发出请求的位置以及使用的特定数据库连接详细信息。有关可能异常的 RDS 登录活动的信息，请参阅[RDS 基于登录活动的异常](#)。

修复建议：

如果关联的数据库出现意外情况，则可能表明该数据库已公开或对数据库的访问策略过于宽松。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过失败登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

在经历了一系列异常的登录尝试失败之后，用户以异常方式成功地从公有 IP 地址登录到您账户中的 RDS 数据库。

默认严重级别：高

- 功能：RDS 登录活动监控

此发现告诉您，在您环境中的 RDS 数据库上观察到异常登录表明成功使用了暴力破解。AWS 在异常成功登录之前，观察到持续存在异常登录尝试失败的模式。这表明您账户中与 RDS 数据库关联的用户和密码可能已被泄露，并且 RDS 数据库可能已被潜在的恶意行为者访问。

GuardDuty 异常检测机器学习 (ML) 模型将这种成功的暴力登录识别为异常。机器学习模型会评估您的所有数据库登录事件，[支持的亚马逊 Aurora 和亚马逊 RDS 数据库](#) 并识别与对手使用的技术相关的异常

事件。机器学习模型跟踪 RDS 登录活动的各种因素，例如发出请求的用户、发出请求的位置以及使用的特定数据库连接详细信息。有关可能异常的 RDS 登录活动的信息，请参阅[RDS 基于登录活动的异常](#)。

修复建议：

此活动表明数据库凭据可能已被泄露或泄露。建议更改关联数据库用户的密码，并查看可用的审计日志，了解可能受到威胁的用户所执行的活动。持续存在的异常登录尝试失败模式表明对数据库或数据库的访问策略过于宽松，也可能已向公众公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过成功登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

用户成功地从已知的恶意 IP 地址登录到您账户中的 RDS 数据库。

默认严重级别：高

- 功能：RDS 登录活动监控

此发现告诉您，成功的 RDS 登录活动来自与 AWS 环境中已知恶意活动关联的 IP 地址。这表明您账户中与 RDS 数据库关联的用户和密码可能已被泄露，并且 RDS 数据库可能已被潜在的恶意行为者访问。

修复建议：

如果关联的数据库出现意外情况，则可能表明用户凭据可能已被泄露或泄露。建议更改关联数据库用户的密码，并查看可用的审计日志，了解受感染用户执行的活动。此活动还可能表明对数据库的访问策略过于宽松，或者数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过成功登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

与已知恶意活动关联的 IP 地址尝试登录您账户中的 RDS 数据库，但未成功。

默认严重级别：中

- 功能：RDS 登录活动监控

此发现告诉您，与已知恶意活动关联的 IP 地址试图登录您AWS环境中的 RDS 数据库，但未能提供正确的用户名或密码。这表明潜在的恶意行为者可能正试图破坏您账户中的 RDS 数据库。

修复建议：

如果关联的数据库出现意外情况，则可能表明该数据库的访问策略过于宽松，或者该数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过失败登录事件修复可能受攻击的数据库](#)。

Discovery:RDS/MaliciousIPCaller

与已知恶意活动关联的 IP 地址探测了您账户中的 RDS 数据库；未尝试进行身份验证。

默认严重级别：中

- 功能：RDS 登录活动监控

此发现告诉您，尽管没有尝试登录，但与已知恶意活动关联的 IP 地址探测了您AWS环境中的 RDS 数据库。这可能表明潜在的恶意行为者正试图扫描可公开访问的基础架构。

修复建议：

如果关联的数据库出现意外情况，则可能表明该数据库的访问策略过于宽松，或者该数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过失败登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

用户从 Tor 出口节点 IP 地址成功登录到您账户中的 RDS 数据库。

默认严重级别：高

- 功能：RDS 登录活动监控

这一发现告诉您，用户从 Tor 出口节点 IP 地址成功登录到您AWS环境中的 RDS 数据库。Tor 是用于实现匿名通信的软件。它通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。此可能表示有人未经授权访问您的 AWS 资源并意图隐藏攻击者的真实身份。

修复建议：

如果关联的数据库出现意外情况，则可能表明用户凭据可能已被泄露或泄露。建议更改关联数据库用户的密码，并查看可用的审计日志，了解受感染用户执行的活动。此活动还可能表明对数据库的访问策略过于宽松，或者数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过成功登录事件修复可能受攻击的数据库](#)。

CredentialAccess:RDS/TorIPCaller.FailedLogin

一个 Tor IP 地址试图登录您账户中的 RDS 数据库，但未成功。

默认严重级别：中

- 功能：RDS 登录活动监控

这一发现告诉您，Tor 退出节点 IP 地址试图登录您 AWS 环境中的 RDS 数据库，但未能提供正确的用户名或密码。Tor 是用于实现匿名通信的软件。它通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。此可能表示有人未经授权访问您的 AWS 资源并意图隐藏攻击者的真实身份。

修复建议：

如果关联的数据库出现意外情况，则可能表明该数据库的访问策略过于宽松，或者该数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过失败登录事件修复可能受攻击的数据库](#)。

Discovery:RDS/TorIPCaller

Tor 退出节点 IP 地址探测了您账户中的 RDS 数据库，但未尝试进行身份验证。

默认严重级别：中

- 功能：RDS 登录活动监控

这一发现告诉你，尽管没有尝试登录，但 Tor 退出节点 IP 地址探测了你 AWS 环境中的 RDS 数据库。这可能表明潜在的恶意行为者正试图扫描可公开访问的基础架构。Tor 是用于实现匿名通信的软件。它通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。这可能表示未经授权访问了您账户中的 RDS 资源，目的是隐藏潜在恶意攻击者的真实身份。

修复建议：

如果关联的数据库出现意外情况，则可能表明该数据库的访问策略过于宽松，或者该数据库已公开。建议将数据库放在私有 VPC 中，并将安全组规则限制为仅允许来自必要来源的流量。有关更多信息，请参阅[通过失败登录事件修复可能受攻击的数据库](#)。

Lambda Protection 查找类型

本节介绍特定于您的AWS Lambda资源并resourceType列为的查找类型Lambda。对于所有 Lambda 发现，我们建议您检查相关资源并确定其行为是否符合预期。如果活动获得授权，则可以使用[抑制规则](#)或[可信 IP 和威胁列表](#)来防止针对该资源的误报通知。

如果活动意外，最佳安全做法是假设 Lambda 可能遭到入侵，并遵循补救建议。

主题

- [Backdoor:Lambda/C&CActivity.B](#)
- [CryptoCurrency:Lambda/BitcoinTool.B](#)
- [Trojan:Lambda/BlackholeTraffic](#)
- [Trojan:Lambda/DropPoint](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:Lambda/TorClient](#)
- [UnauthorizedAccess:Lambda/TorRelay](#)

Backdoor:Lambda/C&CActivity.B

Lambda 函数正在查询与已知命令和控制服务器关联的 IP 地址。

默认严重级别：高

- 功能：Lambda 网络活动监控

这一发现告诉您，AWS您的环境中列出的 Lambda 函数正在查询与已知命令和控制 (C&C) 服务器关联的 IP 地址。与生成的调查结果关联的 Lambda 函数可能遭到破坏。C&C 服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是感染了相同类型恶意软件并受其控制的一组连接到 Internet 的设备 (其中可能包括 PC、服务器、移动设备和物联网设备)。僵尸网络通常用于分发恶意软件和收集不当信息，例如信用卡号。根据僵尸网络的用途和结构，C&C 服务器也可以发布命令来启动分布式拒绝服务 (DDoS) 攻击。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

CryptoCurrency:Lambda/BitcoinTool.B

EC2 实例正在查询与加密货币相关活动关联的 IP 地址。

默认严重级别：高

- 功能：Lambda 网络活动监控

此调查结果通知您，您 AWS 环境中的 EC2 实例正在查询与比特币或其他加密货币相关活动关联的 IP 地址。威胁行为者可能会试图控制 Lambda 函数，以便恶意地将其重新用于未经授权的加密货币挖矿。

修复建议：

如果您使用此 Lambda 函数来挖掘或管理加密货币，或者该函数以其他方式参与区块链活动，则它可能是您环境的预期活动。如果您的环境中出现这种情况，我们建议您为此调查结果设置隐藏规则。禁止规则应由两个筛选条件组成。第一个条件应使用 Finding type (调查结果类型) 属性，其值为 。第二个筛选条件应该是区块链活动中涉及的函数的 Lambda 函数名称。有关创建禁止规则的信息，请参阅[禁止规则](#)。

如果此活动出乎意料，则您的 Lambda 函数可能会受到损害。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

Trojan:Lambda/BlackholeTraffic

EC2 实例正在尝试与作为已知黑洞的远程主机的 IP 地址进行通信。

默认严重级别：中

- 功能：Lambda 网络活动监控

这一发现告诉您，AWS 您的环境中列出的 Lambda 函数正在尝试与黑洞（或漏洞）的 IP 地址进行通信。黑洞是指网络中这样的位置：传入或传出流量将会无提示放弃，不向源通知其数据未达到其目标接收方。黑洞 IP 地址指定没有运行的主机或者未分配主机的地址。列出的 Lambda 函数可能遭到入侵。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

Trojan:Lambda/DropPoint

EC2 实例正在尝试与已知持有凭证和恶意软件捕获的其他被盗数据的远程主机的 IP 地址进行通信。

默认严重级别：中

- 功能：Lambda 网络活动监控

此调查结果通知您，您 AWS 环境中的 EC2 实例正在尝试与已知持有凭证和恶意软件捕获的其他被盗数据的远程主机的 IP 地址进行通信。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Lambda 函数正在与自定义威胁列表上的 IP 地址建立连接。

默认严重级别：中

- 功能：Lambda 网络活动监控

此调查结果通知您，您 AWS 环境中的 EC2 实例出站通信所指向的 IP 地址，包括在您上传的威胁列表中。在中，威胁列表包含已知的恶意 IP 地址。将根据已上传威胁列表生成结果。您可以在 GuardDuty 控制台的发现详情中查看威胁列表的详细信息。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

UnauthorizedAccess:Lambda/TorClient

EC2 实例正在连接到一个 Tor Guard 或 Authority 节点。

默认严重级别：高

- 功能：Lambda 网络活动监控

此调查结果告知您，您 AWS 环境中的 EC2 实例正在连接到一个 Tor Guard 或 Authority 节点。Tor 是用于实现匿名通信的软件。Tor Guard 和 Authority 节点充当 Tor 网络的初始网关。此流量可能表示此 Lambda 函数可能已遭到入侵。它现在充当 Tor 网络上的客户端。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

UnauthorizedAccess:Lambda/TorRelay

EC2 实例正在以 Tor 中继身份连接到 Tor 网络。

默认严重级别：高

- 功能：Lambda 网络活动监控

此调查结果告知您，您 AWS 环境中的 EC2 实例正在以一种暗示其充当 Tor 中继的方式与 Tor 网络建立连接。Tor 是用于实现匿名通信的软件。Tor 中继通过将客户端可能的非法流量从一个 Tor 中继转发到另一个 Tor 中继，来提高通信的匿名程度。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能受损的 Lambda 函数](#)。

停用调查结果类型

调查结果是一个通知，包含有关发现的潜在安全问题的详细信息。有关对 GuardDuty 调查结果类型的重要更改（包括新添加和停用的调查结果类型）的信息，请参阅[Amazon 的文档历史记录 GuardDuty](#)。

以下查找类型已停用，不再由 GuardDuty 生成。

⚠ Important

您无法重新激活已停用的 调查结果类型。

主题

- [Exfiltration:S3/ObjectRead.Unusual](#)
- [Impact:S3/PermissionsModification.Unusual](#)
- [Impact:S3/ObjectDelete.Unusual](#)
- [Discovery:S3/BucketEnumeration.Unusual](#)
- [Persistence:IAMUser/NetworkPermissions](#)
- [Persistence:IAMUser/ResourcePermissions](#)
- [Persistence:IAMUser/UserPermissions](#)
- [PrivilegeEscalation:IAMUser/AdministrativePermissions](#)
- [Recon:IAMUser/NetworkPermissions](#)
- [Recon:IAMUser/ResourcePermissions](#)
- [Recon:IAMUser/UserPermissions](#)
- [ResourceConsumption:IAMUser/ComputeResources](#)
- [Stealth:IAMUser/LoggingConfigurationModified](#)
- [UnauthorizedAccess:IAMUser/ConsoleLogin](#)
- [UnauthorizedAccess:EC2/TorIPCaller](#)
- [Backdoor:EC2/XORDDOS](#)
- [Behavior:IAMUser/InstanceLaunchUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.A](#)
- [UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

Exfiltration:S3/ObjectRead.Unusual

一个 IAM 实体以可疑的方式调用了 S3 API。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

- 数据源：S3 的 CloudTrail 数据事件

这一发现告诉您，您AWS环境中的一个 IAM 实体正在进行 API 调用，这些调用涉及 S3 存储桶，并且与该实体的既定基准不同。本活动中使用的 API 调用与攻击的渗透阶段相关联，在该阶段中，攻击者正试图收集数据。此活动是可疑的，因为 IAM 实体调用 API 的方式不寻常。例如，此 IAM 实体以前没有调用此类 API 的历史记录，或者该 API 是在异常位置调用的。

修复建议：

如果关联的委托人意想不到此活动，则可能表明证书已暴露或您的 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Impact:S3/PermissionsModification.Unusual

一个 IAM 实体调用了 API 来修改一个或多个 S3 资源的权限。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

这一发现告诉您，一个 IAM 实体正在进行旨在修改环境中一个或多个存储桶或对象权限的 AWS API 调用。攻击者可能执行此操作以允许在账户之外共享信息。此活动是可疑的，因为 IAM 实体调用 API 的方式不寻常。例如，此 IAM 实体以前没有调用此类 API 的历史记录，或者该 API 是在异常位置调用的。

修复建议：

如果关联的委托人意想不到此活动，则可能表明证书已暴露或您的 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Impact:S3/ObjectDelete.Unusual

IAM 实体调用了用于删除 S3 桶中数据的 API。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

这一发现告诉您，您的 AWS 环境中的一个特定 IAM 实体正在进行 API 调用，旨在通过删除列出的 S3 存储桶本身来删除该存储桶中的数据。此活动是可疑的，因为 IAM 实体调用 API 的方式不寻常。例如，此 IAM 实体以前没有调用此类 API 的历史记录，或者该 API 是在异常位置调用的。

修复建议：

如果关联的委托人意想不到此活动，则可能表明证书已暴露或您的 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Discovery:S3/BucketEnumeration.Unusual

一个 IAM 实体调用了 S3 API，用于在您的网络中发现 S3 存储桶。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

这一发现告诉您，一个 IAM 实体已调用 S3 API 来发现您的环境中的 S3 存储桶，例如。ListBuckets 此类活动与攻击的发现阶段有关，攻击者正在收集信息以确定您的 AWS 环境是否容

易受到更广泛的攻击。此活动是可疑的，因为 IAM 实体调用 API 的方式不寻常。例如，此 IAM 实体以前没有调用此类 API 的历史记录，或者该 API 是在异常位置调用的。

修复建议：

如果关联的委托人意想不到此活动，则可能表明证书已暴露或您的 S3 权限不够严格。有关更多信息，请参阅[修复可能遭到入侵的 S3 存储桶](#)。

Persistence:IAMUser/NetworkPermissions

IAM 用户调用了 API，该 API 通常用于更改您的 AWS 账户中的安全组、路由和 ACL 的网络访问权限。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

此调查结果表明，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有调用此 API 的历史记录。

此发现是在可疑情况下更改网络配置设置时触发的，例如委托人调用 CreateSecurityGroup API 时没有此操作的历史记录。攻击者通常会尝试更改安全组，从而允许各个端口上的特定入站流量，以提高其访问可能已在您的 EC2 实例上植入的自动程序的能力。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Persistence:IAMUser/ResourcePermissions

委托人调用了 API，该 API 通常用于更改您的 AWS 账户中各种资源的安全访问策略。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

此调查结果表明，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有调用此 API 的历史记录。

当检测到附加到 AWS 资源的策略或权限发生了变化时，例如您的 AWS 环境中的委托人调用了 PutBucketPolicy API，但之前没有这样做的历史记录时，就会触发此发现。某些服务，如 Amazon S3，支持授予一个或多个委托人对资源的访问权限的资源附加型权限。使用被盗的凭证，攻击者可以更改附加到某资源的策略，从而授予他们对该资源的未来访问权限。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Persistence:IAMUser/UserPermissions

委托人调用了一个 API，该 API 通常用于在您的 AWS 账户中添加、修改或删除 IAM 用户、组或策略。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

此调查结果表明，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有调用此 API 的历史记录。

此发现是由环境中用户相关权限的可疑更改触发的，例如，当您的 AWS 环境中的委托人调用了 API 时，之前没有调用过 AttachUserPolicy API。AWS 攻击者可能会使用被盗的凭证来创建新用户，为现有用户添加访问策略，或者创建访问密钥以最大限度地提高他们对账户的访问权限，即使他们的原

始接入点已关闭。例如，账户的所有者可能会注意到特定的 IAM 用户或密码被盗，并将其从账户中删除。但是，他们可能不会删除由欺诈创建的管理员主体创建的其他用户，从而使攻击者可以访问他们的 AWS 帐户。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

PrivilegeEscalation:IAMUser/AdministrativePermissions

委托人尝试给自己分配高度宽松的策略。

默认严重级别：低

Note

如果权限提升尝试不成功，此调查结果的严重级别为“低”；如果权限提升尝试成功，则为“中”。

此调查结果通知您，您的 AWS 环境中的特定委托人展现出的行为可能被视为权限提升攻击。此调查结果在用户或角色尝试给自己分配高度宽松的策略时触发。如果相关用户或角色不应具有管理权限，则表示该用户的凭证已被盗用或者该角色的权限可能未正确配置。

攻击者将使用被盗的凭证来创建新用户，为现有用户添加访问策略，或者创建访问密钥以最大限度地提高他们对账户的访问权限，即使他们的原始接入点已关闭。该账户的拥有者可能会注意到，某个特定 IAM 用户或密码已被盗并且将其从账户中删除，但可能不会删除由通过欺骗手段创建的管理委托人创建的其他用户，从而让攻击者仍可访问其 AWS 账户。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Recon:IAMUser/NetworkPermissions

委托人调用了一个 API，该 API 通常用于更改您的 AWS 账户中的安全组、路由和 ACL 的网络访问权限。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

此调查结果表明，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有调用此 API 的历史记录。

当在可疑的情况下探测到您的 AWS 账户中的资源访问权限时，会触发此调查结果。例如，如果以前没有执行此操作的历史记录的委托人调用了 StopLogging API。攻击者可能使用被盗凭证执行您的 AWS 应用程序的测试来查找漏洞，以找出有价值的信息或确定他们已拥有的凭证的功能。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Recon:IAMUser/ResourcePermissions

委托人调用了 API，该 API 通常用于更改您的 AWS 账户中各种资源的安全访问策略。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

此调查结果表明，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有调用此 API 的历史记录。

当在可疑的情况下探测到您的 AWS 账户中的资源访问权限时，会触发此调查结果。例如，如果以前没有执行此操作的历史记录的委托人调用了 StopLogging API。攻击者可能使用被盗凭证执行您的 AWS 应用程序的测试来查找漏洞，以找出有价值的信息或确定他们已拥有的凭证的功能。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Recon:IAMUser/UserPermissions

委托人调用了 API，该 API 通常用于在您的 AWS 账户中添加、修改或删除 IAM 用户、组或策略。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

当在可疑的情况下探测到您的 AWS 环境中的用户权限时，会触发此调查结果。例如，如果以前没有执行此操作的历史记录的委托人调用了 StopLogging API。攻击者可能使用被盗凭证执行您的 AWS 应用程序的测试来查找漏洞，以找出有价值的信息或确定他们已拥有的凭证的功能。

此调查结果表示，您的 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有通过此方法调用该 API 的历史记录。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

ResourceConsumption:IAMUser/ComputeResources

委托人调用了 API，该 API 通常用于启动计算资源，如 EC2 实例。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

当在可疑的情况下启动您的 AWS 环境中的 EC2 实例时，会触发此调查结果。这一发现表明，您的 AWS 环境中的特定委托人表现出的行为与既定基准不同；例如，如果委托人（AWS 账户根用户 IAM 角色或 IAM 用户）在以前没有调用过 RunInstances API 的情况下调用了 API。这可能指示攻击者正在使用被盗凭证窃取计算时间（可能用于加密货币挖矿或密码破解）。它还可能指示攻击者正在使用您的 AWS 环境中的 EC2 实例及其凭证来维护对您的账户的访问。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

Stealth:IAMUser/LoggingConfigurationModified

委托人调用了 API，该 API 通常用于停止 CloudTrail 日志记录、删除现有日志以及消除您的 AWS 账户中活动的跟踪。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

当在可疑的情况下修改您的 AWS 账户中的日志记录配置时，会触发此调查结果。这一发现告诉您，您的 AWS 环境中的特定委托人表现出的行为与既定基准不同；例如，如果委托人（AWS 账户根用户 IAM 角色或 IAM 用户）调用了 StopLogging API，但之前没有这样做的记录。这可能指示攻击者正在尝试通过消息任何其活动的跟踪来覆盖其跟踪。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:IAMUser/ConsoleLogin

发现了您的 AWS 账户中委托人的异常控制台登录。

默认严重级别：中

Note

此调查结果的默认严重性为“中”。但是，如果使用在 AWS 实例上创建的临时 AWS 凭证调用 API，则调查结果的严重性为“高”。

当在可疑的情况下检测到控制台登录时，会触发此调查结果。例如，如果以前没有执行此操作的历史记录的委托人从以前从未用过的客户端或异常位置调用了 ConsoleLogin API。这可能指示被盗凭证正在用来获取对您的 AWS 账户的访问权限，或者有效的用户正在以无效或不安全的方式（例如，不是通过经批准的 VPN）访问该账户。

此调查结果通知您，您 AWS 环境中的特定委托人表现出的行为与所建立的基准有差异。此委托人以前没有从此特定位置使用此客户端应用程序的登录活动的历史记录。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

UnauthorizedAccess:EC2/TorIPCaller

EC2 实例正在接收来自 Tor 退出节点的入站连接。

默认严重级别：中

此调查结果告知您 AWS 环境中的 EC2 实例正在接收来自 Tor 退出节点的入站连接。Tor 是用于实现匿名通信的软件。它通过一系列网络节点之间的中继来加密和随机反弹通信。最后一个 Tor 节点被称为出口节点。此可能表示有人未经授权访问您的 AWS 资源并意图隐藏攻击者的真实身份。

修复建议：

如果此活动是意外的，则表示您的 EC2 实例可能已受到攻击。有关更多信息，请参阅[修复可能遭到入侵的 Amazon 实例 EC2](#)。

Backdoor:EC2/XORDDOS

EC2 实例尝试与关联到 XorDDos 恶意软件的 IP 地址通信。

默认严重级别：高

此调查结果通知您，您的 AWS 环境中存在 EC2 实例尝试与关联到 XorDDoS 恶意软件的 IP 地址通信。此 EC2 实例可能遭盗用。XOR DDoS 是木马恶意软件，可劫持 Linux 系统。为了获取对系统的访问，它启动暴力攻击，用于发现 Linux 上安全外壳 (SSH) 服务的密码。获取 SSH 凭证并成功登录之后，它使用根特权运行脚本，下载并安装 XOR DDoS。然后，此恶意软件将成为僵尸网络的一部分，用于对其他目标启动分布式拒绝服务 (DDoS) 攻击。

修复建议：

如果此活动是意外的，则表示您的 EC2 实例可能已受到攻击。有关更多信息，请参阅[修复可能遭到入侵的 Amazon 实例 EC2](#)。

Behavior:IAMUser/InstanceLaunchUnusual

IAM 用户启动了异常类型的 EC2 实例。

默认严重级别：高

此调查结果通知您，您 AWS 环境中的特定 IAM 用户表现出的行为与所建立的基准有差异。此 IAM 用户以前没有启动此类型 EC2 实例的历史记录。您的凭证可能遭盗用。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

CryptoCurrency:EC2/BitcoinTool.A

EC2 实例与比特币矿池通信。

默认严重级别：高

此调查结果通知您，您 AWS 环境中的 EC2 实例与比特币矿池通信。在数字加密货币挖矿领域中，矿池是通过网络共享其处理能力的矿工的资源池，以根据在解析数据块中所贡献的工作量来拆分回报。除非您使用此 EC2 实例进行比特币挖矿，否则您的 EC2 实例可能遭盗用。

修复建议：

如果此活动是意外的，则表示您的 EC2 实例可能已受到攻击。有关更多信息，请参阅[修复可能遭到入侵的 Amazon 实例 EC2](#)。

UnauthorizedAccess:IAMUser/UnusualASNCaller

从异常网络的 IP 地址调用了 API。

默认严重级别：高

此调查结果告知您已从异常网络的 IP 地址调用特定活动。在所述用户的整个 AWS 使用历史记录中从未观察到此网络。此活动可以包含登录控制台、尝试启动 EC2 实例、创建新的 IAM 用户、修改您的 AWS 权限等。这可能表示有人未经授权访问您的 AWS 资源。

修复建议：

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅。有关更多信息，请参阅[修复可能被泄露的凭证 AWS](#)。

按资源类型列出的调查发现

以下页面按与 GuardDuty 调查结果相关的资源类型分类：

- [EC2 调查发现类型](#)
- [IAM查找类型](#)
- [S3 调查发现类型](#)
- [EKS审核日志查找类型](#)
- [运行时监控查找类型](#)
- [适用于 EC2 查找类型的恶意软件防护](#)
- [适用于 S3 查找类型的恶意软件防护](#)
- [RDS 保护查找类型](#)
- [Lambda Protection 查找类型](#)

调查发现表

下表显示按基础数据来源或功能排序的所有处于活动状态的调查发现类型（如果适用）。以下某些调查发现类型的严重性可能会变化，用星号（*）表示。有关调查发现类型严重性变化的信息，请查看该查找类型的详细描述。

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 的数据事件	低
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 的数据事件	高
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 的数据事件	高
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail S3 的数据事件	中
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail S3 的数据事件	高
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail S3 的数据事件	高
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail S3 的数据事件	高
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail S3 的数据事件	高
Impact:S3/Anomalous	Amazon S3	CloudTrail S3 的数据事件	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
sBehavior .Write			
Impact:S3 /MaliciousIPCaller	Amazon S3	CloudTrail S3 的数据事件	高
PenTest:S3/KaliLinux	Amazon S3	CloudTrail S3 的数据事件	中
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail S3 的数据事件	中
PenTest:S3/PentooLinux	Amazon S3	CloudTrail S3 的数据事件	中
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail S3 的数据事件	高
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail S3 的数据事件	高
CredentialAccess:IAMUser/AnonymousBehavior	IAM	CloudTrail 管理事件	中
DefenseEvasion:IAMUser/AnonymousBehavior	IAM	CloudTrail 管理事件	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	低
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	高
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	高
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/KaliLinux	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/ParrrotLinux	IAM	CloudTrail 管理事件	中
PenTest:IAMUser/PentooLinux	IAM	CloudTrail 管理事件	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail 管理事件	低*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail 管理事件	高*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理事件	低
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail 管理事件	高
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail 管理事件	低

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail 管理事件	高
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail 管理事件	中
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理事件	中
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理事件	中
Recon:IAMUser/TorIPCaller	IAM	CloudTrail 管理事件	中
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail 管理事件	低
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail 管理事件	低

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail 管理事件	中
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail 管理事件	中
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail S3 的管理事件或 CloudTrail 数据事件	低

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail S3 的管理事件或 CloudTrail 数据事件	高
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNS 日志	高
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNS 日志	高
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNS 日志	中
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNS 日志	高
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNS 日志	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNS 日志	低
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNS 日志	中
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNS 日志	高
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNS 日志	高
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNS 日志	高
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNS 日志	高
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNS 日志	中
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNS 日志	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNS日志	高
Execution:Container/MaliciousFile	容器	EBS恶意软件防护	因检测到的威胁而异
Execution:Container/SuspiciousFile	容器	EBS恶意软件防护	因检测到的威胁而异
Execution:EC2/MaliciousFile	EC2	EBS恶意软件防护	因检测到的威胁而异
Execution:EC2/SuspiciousFile	EC2	EBS恶意软件防护	因检测到的威胁而异
Execution:ECS/MaliciousFile	ECS	EBS恶意软件防护	因检测到的威胁而异
Execution:ECS/SuspiciousFile	ECS	EBS恶意软件防护	因检测到的威胁而异
Execution:Kubernetes/MaliciousFile	Kubernetes	EBS恶意软件防护	因检测到的威胁而异
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBS恶意软件防护	因检测到的威胁而异

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
CredentialAccess:Kubernetes/AnomalousBehaviors.SecretsAccessed	Kubernetes	EKS审核日志	中
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKS审核日志	高
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS审核日志	高
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS审核日志	高
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKS审核日志	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
DefenseEv asion:Kub ernetes/M aliciousIPCaller	Kubernetes	EKS审核日志	高
DefenseEv asion:Kub ernetes/M aliciousI PCaller.C ustom	Kubernetes	EKS审核日志	高
DefenseEv asion:Kub ernetes/S uccessful Anonymous Access	Kubernetes	EKS审核日志	高
DefenseEv asion:Kub ernetes/T orIPCaller	Kubernetes	EKS审核日志	高
Discovery :Kubernet es/Anomal ousBehavi or.Permis sionChecked	Kubernetes	EKS审核日志	低
Discovery :Kubernetes/ MaliciousIPCall er	Kubernetes	EKS审核日志	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Discovery :Kubernetes/ MaliciousIPCall er.Custom	Kubernetes	EKS审核日志	中
Discovery :Kubernet es/Succes sfulAnony mousAccess	Kubernetes	EKS审核日志	中
Discovery :Kubernetes/ TorIPCaller	Kubernetes	EKS审核日志	中
Execution :Kubernet es/ExecIn KubeSyste mPod	Kubernetes	EKS审核日志	中
Execution :Kubernet es/Anomal ousBehavi or.ExecInPod	Kubernetes	EKS审核日志	中
Execution :Kubernet es/Anomal ousBehavi or.Worklo adDeployed	Kubernetes	EKS审核日志	低

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKS审核日志	高
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS审核日志	高
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKS审核日志	高
Impact:Kubernetes/TorIPCaller	Kubernetes	EKS审核日志	高
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKS审核日志	中
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKS审核日志	中
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKS审核日志	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Persisten ce:Kubernetes/ SuccessfulAno nymousAccess	Kubernetes	EKS审核日志	高
Persisten ce:Kubernetes/ TorIPCaller	Kubernetes	EKS审核日志	中
Policy:Ku bernetes/ AdminAcce ssToDefau ltService Account	Kubernetes	EKS审核日志	高
Policy:Ku bernetes/ Anonymous AccessGranted	Kubernetes	EKS审核日志	高
Policy:Ku bernetes/ KubeflowD ashboardE xposed	Kubernetes	EKS审核日志	中
Policy:Ku bernetes/ ExposedDa shboard	Kubernetes	EKS审核日志	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Privilege Escalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKS审核日志	中*
Privilege Escalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKS审核日志	低
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKS审核日志	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Privilege Escalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKS审核日志	高
Privilege Escalation:Kubernetes/PrivilegedContainer	Kubernetes	EKS审核日志	中
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda 网络活动监控	高
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda 网络活动监控	高
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda 网络活动监控	中
Trojan:Lambda/DropPoint	Lambda	Lambda 网络活动监控	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda 网络活动监控	中
UnauthorizedAccess:Lambda/TrustedClient	Lambda	Lambda 网络活动监控	高
UnauthorizedAccess:Lambda/TrustedRelay	Lambda	Lambda 网络活动监控	高
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	支持的亚马逊 Aurora 和亚马逊 RDS 数据库	RDS 登录活动监控	低
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	支持的亚马逊 Aurora 和亚马逊 RDS 数据库	RDS 登录活动监控	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	变量*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	中
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	高
CredentialAccess:RDS/TorIPCaller.FailedLogin	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	中
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	高
Discovery:RDS/MaliciousIPCaller	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Discovery:RDS/TorIPCaller	支持的亚马逊 Aurora 和亚马逊 RDS数据库	RDS登录活动监控	中
Backdoor:Runtime/C&CActivity.B	实例、EKS集群、ECS集群或容器	运行时监控	高
Backdoor:Runtime/C&CActivity.B!DNS	实例、EKS集群、ECS集群或容器	运行时监控	高
Cryptocurrency:Runtime/BitcoinTool.B	实例、EKS集群、ECS集群或容器	运行时监控	高
Cryptocurrency:Runtime/BitcoinTool.B!DNS	实例、EKS集群、ECS集群或容器	运行时监控	高
DefenseEvasion:Runtime/FilelessExecution	实例、EKS集群、ECS集群或容器	运行时监控	中
DefenseEvasion:Runtime/ProcessInjection.Proc	实例、EKS集群、ECS集群或容器	运行时监控	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
DefenseEv asion:Runtime/ ProcessInject ion.Ptrace	实例、EKS集 群、ECS集群或 容器	运行时监控	中
DefenseEv asion:Runtime/ ProcessInject ion.Virtu alMemoryWrite	实例、EKS集 群、ECS集群或 容器	运行时监控	高
DefenseEv asion:Runtime/ PtraceAntiDeb ugging	实例、EKS集 群、ECS集群或 容器	运行时监控	低
DefenseEv asion:Runtime/ SuspiciousCom mand	实例、EKS集 群、ECS集群或 容器	运行时监控	高
Execution :Runtime/ Malicious FileExecuted	实例、EKS集 群、ECS集群或 容器	运行时监控	高
Execution :Runtime/ NewBinary Executed	实例、EKS集 群、ECS集群或 容器	运行时监控	中
Execution :Runtime/ NewLibrar yLoaded	实例、EKS集 群、ECS集群或 容器	运行时监控	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Execution:Runtime/SuspiciousCommand	实例、EKS集群、ECS集群或容器	运行时监控	Variable
Execution:Runtime/SuspiciousShellCreated	实例、EKS集群、ECS集群或容器	运行时监控	低
Execution:Runtime/SuspiciousTool	实例、EKS集群、ECS集群或容器	运行时监控	Variable
Execution:Runtime/ReverseShell	实例、EKS集群、ECS集群或容器	运行时监控	高
Impact:Runtime/AbusedDomainRequest.Reputation	实例、EKS集群、ECS集群或容器	运行时监控	中
Impact:Runtime/BitcoinDomainRequest.Reputation	实例、EKS集群、ECS集群或容器	运行时监控	高
Impact:Runtime/CryptoMinerExecuted	实例、EKS集群、ECS集群或容器	运行时监控	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Impact:Runtime/MaliciousDomainRequest.Reputation	实例、EKS集群、ECS集群或容器	运行时监控	中
Impact:Runtime/SuspiciousDomainRequest.Reputation	实例、EKS集群、ECS集群或容器	运行时监控	低
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	实例、EKS集群、ECS集群或容器	运行时监控	高
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	实例、EKS集群、ECS集群或容器	运行时监控	中
PrivilegeEscalation:Runtime/DockerSocketAccessed	实例、EKS集群、ECS集群或容器	运行时监控	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Privilege Escalation:Runtime/ElevationToRoot	实例、EKS集群、ECS集群或容器	运行时监控	中
Privilege Escalation:Runtime/RuncContainerEscape	实例、EKS集群、ECS集群或容器	运行时监控	高
Privilege Escalation:Runtime/UserfulfdUsage	实例、EKS集群、ECS集群或容器	运行时监控	中
Object:S3/MaliciousFile	S3Object	S3 的恶意软件防护	高
Trojan:Runtime/BlackholeTraffic	实例、EKS集群、ECS集群或容器	运行时监控	中
Trojan:Runtime/BlackholeTraffic!DNS	实例、EKS集群、ECS集群或容器	运行时监控	中
Trojan:Runtime/DropPoint	实例、EKS集群、ECS集群或容器	运行时监控	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Trojan:Runtime/DGADomainRequest.C!DNS	实例、EKS集群、ECS集群或容器	运行时监控	高
Trojan:Runtime/DriveBySourceTraffic!DNS	实例、EKS集群、ECS集群或容器	运行时监控	高
Trojan:Runtime/DropPoint!DNS	实例、EKS集群、ECS集群或容器	运行时监控	中
Trojan:Runtime/PhishingDomainRequest!DNS	实例、EKS集群、ECS集群或容器	运行时监控	高
UnauthorizedAccess:Runtime/MetadataDNSRebind	实例、EKS集群、ECS集群或容器	运行时监控	高
UnauthorizedAccess:Runtime/TorClient	实例、EKS集群、ECS集群或容器	运行时监控	高
UnauthorizedAccess:Runtime/TorRelay	实例、EKS集群、ECS集群或容器	运行时监控	高

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Backdoor:EC2/C&CActivity.B	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Dns	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Udp	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC 流日志	高
Backdoor:EC2/SpamBot	EC2	VPC 流日志	中
Behavior:EC2/NetworkPortUnusual	EC2	VPC 流日志	中
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC 流日志	中

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC 流日志	高
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC 流日志	中
DefenseEvasion:EC2/UnusualDohActivity	EC2	VPC 流日志	中
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC 流日志	中
Impact:EC2/PortSweep	EC2	VPC 流日志	高
Impact:EC2/WinRMBruteForce	EC2	VPC 流日志	低*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC 流日志	高
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC 流日志	低*

调查发现类型	资源类型	基础数据来源/功能	调查发现的严重性
Recon:EC2/Portscan	EC2	VPC 流日志	中
Trojan:EC2/BlackholeTraffic	EC2	VPC 流日志	中
Trojan:EC2/DropPoint	EC2	VPC 流日志	中
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC 流日志	中
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC 流日志	低*
UnauthorizedAccess:EC2/SSHBBruteForce	EC2	VPC 流日志	低*
UnauthorizedAccess:EC2/TorClient	EC2	VPC 流日志	高
UnauthorizedAccess:EC2/TorRelay	EC2	VPC 流日志	高

管理 Amazon GuardDuty 调查结果

GuardDuty 提供了几项重要功能，可帮助您对发现结果进行排序、存储和管理。这些功能将帮助您根据特定环境定制调查发现，减少低价值调查发现带来的干扰，让您专注于独特的 AWS 环境面临的威胁。查看本页的主题，了解如何使用这些功能来提高调查结果 GuardDuty 的价值。

主题：

[摘要控制面板](#)

了解 GuardDuty 控制台中提供的摘要仪表板的组件。

[筛选调查发现](#)

了解如何根据您指定的条件筛选 GuardDuty 结果。

[抑制规则](#)

了解如何通过抑制规则自动筛选 GuardDuty 提醒您发现的结果。抑制规则会根据筛选条件自动存档调查发现。

[使用可信 IP 列表和威胁列表](#)

使用基于可公开路由的 IP 地址的 IP 列表和威胁列表自定义 GuardDuty 监控范围。可信 IP 列表可防止从您认为可信的 IP 生成非 DNS 调查结果，而 Intel 威胁列表会 GuardDuty 提醒您注意用户定义的活动 IPs。

[导出调查发现](#)

将生成的调查结果导出到 Amazon S3 存储桶，这样您就可以保留超过 90 天调查结果保留期的记录。GuardDuty 使用这些历史数据来跟踪您账户中潜在的可疑活动，并评估建议的补救措施是否成功。

[使用 Amazon CloudWatch Events 创建对 GuardDuty 调查结果的自定义响应](#)

通过 Amazon CloudWatch 事件为 GuardDuty 发现的结果设置自动通知。您还可以通过“CloudWatch 事件”自动执行其他任务，以帮助您对发现的结果做出回应。

[了解 EC2 恶意软件防护扫描期间跳过资源的 CloudWatch 日志和原因](#)

了解如何审核 GuardDuty 恶意软件防护 CloudWatch 日志，EC2 以及扫描过程中可能跳过受影响的 Amazon EC2 实例或 Amazon EBS 卷的原因是什么。

[在 EC2 GuardDuty 恶意软件防护中报告误报](#)

了解如何在 S3 恶意软件防护中报告潜在的误报威胁检测。

摘要控制面板

摘要控制面板提供您在当前地区生成的 GuardDuty 调查结果 AWS 账户 的汇总视图。目前，该控制面板支持多达 5000 个调查发现。但是，您可以使用 GuardDuty 控制台上的“调查结果”页面或[GetFindings](#)或来查看所有调查结果的详细信息[ListFindings](#)。

Note

调查结果摘要只能通过 GuardDuty 控制台获得，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。

以下部分将帮助您访问控制面板并了解其组件。

内容

- [访问摘要控制面板](#)
- [了解摘要控制面板](#)
- [提供有关摘要控制面板的反馈](#)

访问摘要控制面板

在 GuardDuty 控制台上，“摘要”仪表盘显示了当前地区最近生成的 5,000 个 GuardDuty 调查结果的合并视图。

要访问摘要控制面板

1. 打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择摘要。当您打开控制台时，会 GuardDuty 显示摘要仪表盘。
3. 默认情况下，显示当天的摘要：今天。GuardDuty 控制台提供了查看过去 2 天、过去 7 天和过去 30 天摘要的选项。要更改默认时间范围，请从概览窗格上方的下拉列表中选择一项。

4. 筛选数据

- 调查发现最多的账户、调查发现最多的资源和最少发生的调查发现小部件，可帮助您根据调查发现的严重性级别筛选数据。
- 调查发现最多的资源小部件还允许根据可能受影响的资源类型筛选数据。

成员账户可以查看属于自己账户的可能受影响资源的详细信息。如果您是 GuardDuty 管理员账户，想要查看可能受影响的资源的详细信息，请使用关联成员账户的凭据打开 GuardDuty 控制台。

5. 保护计划的覆盖范围

保护计划覆盖范围提供贵组织 GuardDuty 中已启用的成员账户的数量。只有被授权的 GuardDuty 管理员才能看到统计信息。

了解摘要控制面板

摘要控制面板在以下部分显示聚合数据。在继续查看和了解摘要之前，请确保从控制台顶部的区域选择器中选择所需的 AWS 区域。另外，请务必从概览窗格上方的下拉菜单中选择所需的时间范围。如果没有为所选参数生成任何调查发现，则任何小部件中都不会有可用的数据。

在最近 5,000 个 GuardDuty 调查结果中，汇总仪表板显示了基于前 5 个结果的数据，其中包含发现次数最多的帐户、包含最多发现结果的资源以及出现次数最少的结果。要进行更深入的分析，请参阅 GuardDuty 控制台中的调查结果页面。

概述

该部分提供以下数据：

- 调查发现总数：表示当前区域中您的账户中生成的调查发现总数。
- 高严重性调查结果：表示当前区域中严重性级别较高的 GuardDuty 发现数量。
- 含调查发现的资源：表示与调查发现相关联且可能被盗用的资源数量。
- 含调查发现的账户：表示至少生成一个调查发现的账户数量。如果您是独立账户，则此字段中的值为 1。

对于过去 7 天和过去 30 天的时间范围，概览窗格可能分别显示每周 (WoW) 或每月 (MoM) 生成的调查发现的百分比差异。如果前一周或前一月没有调查发现，那么在无数据可比较的情况下，可能无法得出百分比差异。

如果您是 GuardDuty 管理员帐户，则所有这些字段都会提供组织中所有成员账户的汇总数据。

按严重性分类的调查发现

该部分显示一个条形图，其中包含选定时间范围内的调查发现总数。您可以查看在选定时间范围内特定日期生成的低、中或高严重性调查发现数量。

最常见的调查发现类型

本节以饼图说明了从当前地区最近生成的多达5,000份发现中观察到的前五种常见 GuardDuty 发现类型。将鼠标悬停在每个扇区上时，饼图会显示以下数据：

- 调查发现计数：表示在选定时间范围内生成该调查发现的次数。
- 严重性：表示调查发现的严重性级别，例如“中”和“高”。
- 百分比：表示该调查发现类型在饼图中所占的比例。
- 上次生成：表示自上次生成此调查发现类型以来过去多长时间。

调查发现最多的账户

该部分提供以下数据：

- 账户：表示生成调查结果的 AWS 账户 ID。
- 调查发现计数：表示为此账户 ID 生成调查发现的次数。
- 上次生成：表示自上次为此账户 ID 生成调查发现类型以来过去多长时间。
- 高严重性：默认情况下，显示高严重性调查发现类型的数据。该字段的可能选项包括高严重性、中严重性和所有严重性。

含调查发现的资源

该部分提供以下数据：

- 资源：表示可能受影响的资源类型，如果此资源属于您的账户，则可以访问快速链接以查看资源详细信息。如果您是 GuardDuty 管理员账户，则可以使用该资源所属的成员账户的凭据访问 GuardDuty 控制台，查看可能受影响的资源的详细信息。
- 帐户：表示此资源所属的 AWS 账户 ID。
- 调查发现计数：表示此资源与查找结果关联的次数。

- 上次生成：表示自上次生成与此资源关联的调查发现类型以来过去多长时间。
- 所有资源类型：默认情况下，显示所有资源类型的数据。通过使用下拉列表，您可以查看特定资源类型的数据，例如实例AccessKey、Lambda 等。
- 高严重性：默认情况下，显示高严重性调查发现类型的数据。通过下拉列表，您可以查看其他严重性级别的数据。可能的选项包括高严重性、中严重性和所有严重性。

最少发生的调查发现

本节详细介绍了在您的 AWS 环境中不经常生成的查找类型。此见解可帮助您调查环境中出现的威胁模式并采取行动。该表显示以下数据：

- 调查发现类型：表示调查发现类型名称。
- 调查发现计数：表示在选定时间范围内生成此调查发现类型的次数。
- 上次生成：表示自上次生成此调查发现类型以来过去多长时间。
- 高严重性：默认情况下，显示高严重性调查发现类型的数据。该字段的可能选项包括高严重性、中严重性和所有严重性。

保护计划的覆盖范围

本节提供了属于您的组织并在当前版本中启用了一项或多项功能以及其他功能（如果适用）配置的活跃成员账户的数量 AWS 区域。

只有授权的 GuardDuty 管理员才能查看其组织内成员账户的统计信息。如果未配置某项功能，请在“操作”列下选择“配置”。

创建新 AWS 组织时，生成整个组织的统计数据最多可能需要 24 小时。

提供有关摘要控制面板的反馈

GuardDuty 鼓励您就摘要控制面板的可用性、功能和性能提供反馈。反馈有助于我们改善控制面板。

要提供有关摘要控制面板的反馈

1. 打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择摘要。当您打开 GuardDuty 控制台时，它会显示摘要仪表板。
3. 在控制面板的右上角选择反馈。此操作将打开一个表单。提供反馈后，选择提交。

筛选调查发现

调查发现筛选条件允许您查看匹配指定条件的调查发现，筛选出任何不匹配的调查发现。您可以使用 Amazon GuardDuty 控制台轻松创建查找筛选条件，也可以 [CreateFilter API](#) 使用创建筛选条件 JSON。查看以下部分，了解如何在控制台中创建筛选条件。要使用这些筛选条件自动存档传入的调查发现，请参阅 [抑制规则](#)。

在 GuardDuty 控制台中创建过滤器

可以通过 GuardDuty 控制台创建和测试查找过滤器。您可以保存通过控制台创建的筛选条件，以便在抑制规则或在将来的筛选操作中使用。筛选条件由至少一个筛选标准组成，包含一个与至少一个值配对的筛选条件属性。

创建筛选条件时，请注意以下几点：

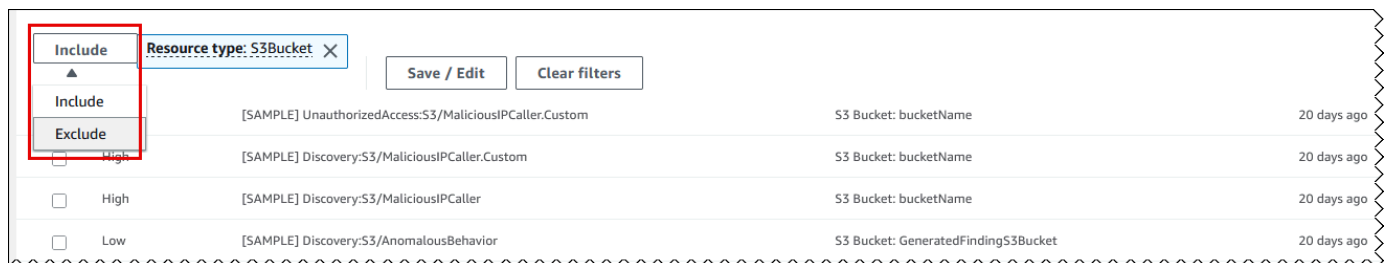
- 筛选条件不接受通配符。
- 您可以指定最少 1 个属性，最多 50 个属性作为特定筛选条件。
- 当您使用等于或不等于条件来筛选账户 ID 等属性值时，最多可以指定 50 个值。
- 每个筛选条件属性都作为 AND 运算符进行计算。同一属性的多个值计算为 AND/OR。

筛选调查结果 (控制台)

1. 在“按属性筛选”下，选择添加筛选条件。这将显示过滤器属性的扩展列表。
2. 从展开的属性列表中，选择要指定为筛选条件的属性，例如账户 ID 或操作类型。

有关属性的完整列表，请参见 [筛选条件属性](#)。

3. 在显示的文本字段中，为所选属性指定一个值，然后选择“应用”。
4. 要添加多个筛选条件，请重复步骤 1-3。
5. 默认情况下，该列表显示与应用的筛选条件相匹配的结果。如果要查看与筛选器属性不匹配的结果，请选择筛选器旁边的“排除”。



6. 将指定的属性和值保存为筛选器

- a. 要将指定的属性及其值（筛选条件）保存为筛选器，请选择“保存/编辑”。
- b. 输入过滤规则名称和描述。
- c. 选择保存。

筛选条件属性

使用API操作创建筛选器或对结果进行排序时，必须在中指定筛选条件JSON。这些筛选条件与调查结果的相关信息JSON相关。下表包含筛选器属性的控制台显示名称及其等效JSON字段名称的列表。

控制台字段名称	JSON 字段名称
帐户 ID	accountId
调查发现 ID	id
区域	region
严重性	severity 您可以根据查找结果类型的严重性级别筛选查找结果类型。有关严重性值的更多信息，请参阅 GuardDuty 调查结果的严重性级别 。如果severity与API、或一起使用 AWS CLI AWS CloudFormation，则会为其分配一个数值。有关更多信息，请参阅 Amazon GuardDuty API 参考 findingCriteria 中的。
调查发现类型	type
更新时间	updatedAt
访问密钥 ID	资源。 accessKeyDetails。 accessKeyId
委托人 ID	资源。 accessKeyDetails。 principalId
用户名	资源。 accessKeyDetails。 userName

控制台字段名称	JSON 字段名称
用户类型	资源。accessKeyDetails。userType
IAM实例配置文件 ID	资源。instanceDetails。iamInstanceProfile.id
实例 ID	资源。instanceDetails。instanceId
实例映像 ID	资源。instanceDetails。imageId
实例标签键	资源。instanceDetails.tags.key
实例标签值	资源。instanceDetails.tags.value
IPv6地址	资源。instanceDetails。networkInterfaces。 ipv6 地址
私有IPv4地址	资源。instanceDetails。networkInterfaces。 privateIpAddresses。privateIpAddress
公共DNS名称	资源。instanceDetails。networkInterfaces。 publicDnsName
公有 IP	资源。instanceDetails。networkInterfaces。 publicIp
安全组 ID	资源。instanceDetails。networkInterfaces。 securityGroups。groupId
安全组名称	资源。instanceDetails。networkInterfaces。 securityGroups。groupName
子网 ID	资源。instanceDetails。networkInterfaces。 subnetId
VPC身份证	资源。instanceDetails。networkInterfaces。 vpcId
前哨基地 ARN	资源。instanceDetails.outpost ARN
资源类型	资源。resourceType

控制台字段名称	JSON 字段名称
存储桶权限	资源.3. BucketDetails publicAccess. effective Permission
Bucket name (存储桶名称)	资源. BucketDetails s3 .name
Bucket tag key	resource.s3 .tags.key BucketDetails
Bucket tag value	资源. BucketDetails s3 .tags.value
存储桶类型	资源. BucketDetails s3 .type
操作类型	服务行动。 actionType
API被称为	服务行动。 awsApiCallaction.api
API来电者类型	服务行动。 awsApiCall行动。 callerType
API错误码	服务行动。 awsApiCall行动。 errorCode
API来电者城市	服务行动。 awsApiCall行动。 remotepD etails.city。 cityName
API来电者国家	服务行动。 awsApiCall行动。 remotepD etails.国家。 countryName
API来电者IPv4地址	服务行动。 awsApiCall行动。 remotepD etails。 ipAddressV4
API来电者IPv6地址	服务行动。 awsApiCall行动。 remotepD etails。 ipAddressV6
API来电者 ASN ID	服务行动。 awsApiCall行动。 remotepD etails.organization.asn
API来电者ASN姓名	服务行动。 awsApiCall行动。 remotepD etails.组织。 asnOrg
API来电者服务名称	服务行动。 awsApiCall行动。 serviceName

控制台字段名称	JSON 字段名称
DNS请求域名	服务行动。 dnsRequestAction.domain
DNS请求域名后缀	服务行动。 dnsRequestAction。 domainWithSuffix
网络连接受阻	服务行动。 networkConnectionAction. 已屏蔽
网络连接方向	服务行动。 networkConnectionAction。 connectionDirection
网络连接本地端口	服务行动。 networkConnectionAction。 localPortDetails.port
网络连接协议	服务行动。 networkConnectionAction. 协议
网络连接城市	服务行动。 networkConnectionAction。 remoteIpDetails.city。 cityName
网络连接国家/地区	服务行动。 networkConnectionAction。 remoteIpDetails. 国家。 countryName
网络连接远程IPv4地址	服务行动。 networkConnectionAction。 remoteIpDetails。 ipAddressV4
网络连接远程IPv6地址	服务行动。 networkConnectionAction。 remoteIpDetails。 ipAddressV6
网络连接远程 IP ASN ID	服务行动。 networkConnectionAction。 remoteIpDetails.organization.asn
网络连接远程 IP ASN 名称	服务行动。 networkConnectionAction。 remoteIpDetails. 组织。 asnOrg
网络连接远程端口	服务行动。 networkConnectionAction。 remotePortDetails.port
附属的远程账户	服务行动。 awsApiCall行动。 remoteAccountDetails. 关联的

控制台字段名称	JSON 字段名称
Kubernetes API 来电者地址 IPv4	服务行动。kubernetesApiCall行动。remoteIpDetails。ipAddressV4
Kubernetes API 来电者地址 IPv6	服务行动。kubernetesApiCall行动。remoteIpDetails。ipAddressV6
Kubernetes 命名空间	服务行动。kubernetesApiCall动作。命名空间
Kubernetes API 来电者 ID ASN	服务行动。kubernetesApiCall行动。remoteIpDetails.organization.asn
Kubernetes 调API用请求 URI	服务行动。kubernetesApiCall行动。requestUri
Kubernetes 状态码 API	服务行动。kubernetesApiCall行动。statusCode
网络连接本地IPv4地址	服务行动。networkConnectionAction。localIpDetails。ipAddressV4
网络连接本地IPv6地址	服务行动。networkConnectionAction。localIpDetails。ipAddressV6
协议	服务行动。networkConnectionAction。协议
API呼叫服务名称	服务行动。awsApiCall行动。serviceName
API来电者账号	服务行动。awsApiCall行动。remoteAccountDetails。accountId
威胁列表名称	服务。additionalInfo。threatListName
资源角色	服务。resourceRole
EKS集群名称	资源。eksClusterDetails.name
Kubernetes 工作负载名称	资源。kubernetesDetails。kubernetesWorkloadDetails.name

控制台字段名称	JSON 字段名称
Kubernetes 工作负载命名空间	资源。kubernetesDetails。kubernetesWorkloadDetails. 命名空间
Kubernetes 用户名	资源。kubernetesDetails。kubernetesUserDetails。用户名
Kubernetes 容器映像	资源。kubernetesDetails。kubernetesWorkloadDetails.containers.image
Kubernetes 容器映像前缀	资源。kubernetesDetails。kubernetesWorkloadDetails. 容器。imagePrefix
扫描 ID	服务。ebsVolumeScan详情。scanId
EBS批量扫描威胁名称	服务。ebsVolumeScan详情。scanDetections。threatDetectedBy姓名。threatNames.name
S3 对象扫描威胁名称	服务。malwareScanDetails.treats.name
威胁严重性	服务。ebsVolumeScan详情。scanDetections。threatDetectedBy姓名。threatNames。严重性
文件 SHA	服务。ebsVolumeScan详情。scanDetections。threatDetectedBy姓名。threatNames。filePaths.hash
ECS集群名称	资源。ecsClusterDetails.name
ECS容器镜像	资源。ecsClusterDetails。taskDetails.containers.image
ECS任务定义 ARN	资源。ecsClusterDetails。taskDetails。definitionArn
独立容器映像	资源。containerDetails.image

控制台字段名称	JSON 字段名称
数据库实例 Id	资源。 rdsDbInstance详情。 dbInstanceIdentifier
数据库集群 Id	资源。 rdsDbInstance详情。 dbClusterIdentifier
数据库引擎	资源。 rdsDbInstance细节。 引擎
数据库用户	资源。 rdsDbUserDetails. 用户
数据库实例标签键	资源。 rdsDbInstance详细信息.tags.key
数据库实例标签值	资源。 rdsDbInstance详情标签值
可执行文件 SHA -256	服务。 runtimeDetails. 进程。 executableSha256
进程名称	服务。 runtimeDetails.process.name
可执行文件路径	服务。 runtimeDetails. 进程。 executablePath
Lambda 函数名称	资源。 lambdaDetails。 functionName
Lambda 函数 ARN	资源。 lambdaDetails。 functionArn
Lambda 函数标签键	资源。 lambdaDetails.tags.key
Lambda 函数标签值	资源。 lambdaDetails.tags.value
DNS请求域名	服务行动。 dnsRequestAction。 domainWithSuffix

抑制规则

抑制规则是一组标准，由与值配对的筛选器属性组成，用于通过自动归档与指定标准匹配的新调查发现来筛选调查发现。抑制规则可用于筛选低价值调查发现、误报调查发现或您不打算应对的威胁，以便更轻松地区别对环境影响最大的安全威胁。

创建抑制规则后，只要使用该规则，就会自动存档与规则中定义的标准匹配的新调查发现。您可以使用现有筛选条件创建抑制规则，也可以根据您定义的新筛选条件来创建抑制规则。您可以配置抑制规则以抑制整个调查发现类型，或者定义更精细的筛选条件，仅禁止特定调查发现类型的特定实例。您可以随时编辑抑制规则。

禁止显示的发现不会发送到亚马逊简单存储服务 AWS Security Hub、Amazon Detective 或亚马逊 EventBridge，如果您通过 Security Hub、第三方或其他警报和票务应用程序使用 GuardDuty 发现 SIEM，则会降低查找噪音水平。如果您已启用[恶意软件防护 EC2](#)，则隐藏的 GuardDuty 发现将不会启动恶意软件扫描。

GuardDuty 即使搜索结果符合您的禁止规则，也会继续生成结果，但是，这些发现会自动标记为已存档。存档的查找结果将在 GuardDuty 其中存储 90 天，在此期间可以随时查看。您可以在 GuardDuty 控制台中查看隐藏的查找结果，方法是从查找结果表中选择“已存档”，或者 GuardDuty API 使用 `findingCriteria.service.archived` 等于 `true` 的 [ListFindings API](#)

Note

在多账户环境中，只有 GuardDuty 管理员才能创建禁止规则。

抑制规则的常见用例和示例

以下查找类型具有应用抑制规则的常见用例。选择查找结果名称以了解有关该查找结果的更多信息。查看用例描述，决定是否要为该发现类型制定抑制规则。

Important

GuardDuty 建议您以被动方式构建抑制规则，并且仅针对您在环境中反复发现误报的发现建立抑制规则。

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)— 使用抑制规则自动存档在将 VPC 网络配置为路由 Internet 流量，使其从本地网关而不是从 Internet Gateway 流出时生成的结果。VPC

当网络配置为路由 Internet 流量，使其从本地网关而不是从 Internet Gateway (IGW) 流出时，VPC 就会生成此结果。常用配置（例如使用[AWS Outposts](#)或 VPC VPN 连接）可能会导致流量以这种方式路由。如果这是预期行为，建议您使用抑制规则并创建一个包含两个筛选条件的规则。第一个标准是 `finding type`（调查发现类型），它应是 `UnauthorizedAccess:IAMUser/`

InstanceCredentialExfiltration.OutsideAWS。第二个筛选条件是API呼叫者IPv4地址以及您的本地 Internet 网关的 IP 地址或CIDR范围。以下示例显示了用于根据API呼叫者 IP 地址抑制此查找类型的过滤器。

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS  
API caller IPv4 address: 198.51.100.6
```

Note

要包含多个API来电者，IPs您可以为每个来电者添加一个新的API来电者IPv4地址过滤器。

- [Recon:EC2/Portscan](#)：使用脆弱性评测应用程序时，使用抑制规则来自动存档调查发现。

抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 Recon:EC2/Portscan。第二个筛选条件应与托管这些漏洞评估工具的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工具的实例可识别哪些条件。以下示例显示了您将使用的过滤器，用于根据具有特定值的实例来抑制此查找类型AMI。

```
Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
```

- [UnauthorizedAccess:EC2/SSHBruteForce](#)：当针对堡垒机实例时，使用抑制规则来自动存档调查发现。

如果暴力攻击的目标是堡垒主机，则这可能代表您的 AWS 环境的预期行为。如果是这种情况，我们建议您为此调查发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 UnauthorizedAccess:EC2/SSHBruteForce。第二个筛选条件应与用作堡垒主机的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工具的实例可识别哪些条件。以下示例代表了根据具有特定实例标签值的实例来抑制此调查发现类型的筛选条件。

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- [Recon:EC2/PortProbeUnprotectedPort](#)：当针对有意公开的实例时，使用抑制规则来自动存档调查发现。

这可能是有意暴露实例的情况，例如，在它们托管 Web 服务器时。如果您的 AWS 环境中出现这种情况，我们建议您为此发现设置抑制规则。抑制规则应由两个筛选条件组成。第一个条件应使用调查发现类型属性，其值为 Recon:EC2/PortProbeUnprotectedPort。第二个筛选条件应与用作堡垒主机的一个或多个实例匹配。您可以使用实例映像 ID 属性或标签值属性，具体取决于托管这些工

具的实例可识别哪些条件。以下示例代表了根据控制台中具有特定实例标签键的实例来抑制此调查发现类型的筛选条件。

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

运行时监控结果的推荐抑制规则

- 当容器内的进程与 Docker 套接字通信时会生成 [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)。您的环境中可能有一些容器出于合法原因需要访问 Docker 套接字。从此类容器访问将生成 PrivilegeEscalation:Runtime/DockerSocketAccessed 调查发现。如果您的 AWS 环境中出现这种情况，我们建议您为此发现类型设置抑制规则。第一个条件应使用值等于 PrivilegeEscalation:Runtime/DockerSocketAccessed 的调查发现类型字段。第二个筛选条件是可执行路径字段，其值等于生成的调查发现中进程的 executablePath。或者，第二个筛选条件可以使用 Exec utive SHA -256 字段，其值等于生成的结果executableSha256中流程的值。
- Kubernetes 集群将自己的DNS服务器作为 pod 运行，例如。coredns因此，每次从 pod 中DNS查找，都会 GuardDuty 捕获两个DNS事件 — 一个来自 pod，另一个来自服务器 pod。这可能会为以下DNS发现生成重复项：
 - [Backdoor:Runtime/C&CActivity.B!DNS](#)
 - [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
 - [Impact:Runtime/AbusedDomainRequest.Reputation](#)
 - [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
 - [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
 - [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
 - [Trojan:Runtime/BlackholeTraffic!DNS](#)
 - [Trojan:Runtime/DGADomainRequest.C!DNS](#)
 - [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
 - [Trojan:Runtime/DropPoint!DNS](#)
 - [Trojan:Runtime/PhishingDomainRequest!DNS](#)

重复的发现将包括与您的DNS服务器 pod 对应的 pod、容器和进程详细信息。您可以使用这些字段设置抑制规则，以抑制重复的调查发现。第一个筛选条件应使用查找结果类型字段，其值等于本节前面提供的DNS查找结果列表中的查找结果类型。第二个筛选条件可以是值等于DNS服务器的可执行路径，也可以是executablePath可执行文件路径，其值等于生成的查找结

果 `executableSHA256` 中的 DNS 服务器值的可执行文件 SHA -256。作为可选的第三个筛选条件，您可以使用 Kubernetes 容器镜像字段，其值等于生成的结果中 DNS 服务器 Pod 的容器镜像。

创建抑制规则

选择您的首选访问方法来创建用于 GuardDuty 查找类型的抑制规则。

Console

您可以使用 GuardDuty 控制台可视化、创建和管理抑制规则。抑制规则的生成方式与筛选条件相同，现有保存的筛选条件可用作抑制规则。有关创建筛选条件的更多信息，请参阅 [筛选调查发现](#)。

要使用控制台创建抑制规则：

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在调查发现页面上，选择抑制调查发现以打开抑制规则面板。
3. 要打开筛选条件菜单，请在添加筛选条件中输入 **filter criteria**。您可以从列表中选择一个条件。为所选条件输入一个有效值。

Note

要确定有效值，请查看调查发现表，并选择要抑制的调查发现。在调查结果面板中查看其详细信息。

您可以添加多个筛选条件，确保只有那些要抑制的调查发现显示在表中。

4. 输入抑制规则的名称和描述。有效字符包括字母数字字符、句点 (.)、破折号 (-)、下划线 (_) 和空格。
5. 选择保存。


您也可以从现有保存的筛选条件创建抑制规则。有关创建筛选条件的更多信息，请参阅 [筛选调查发现](#)。

要使用保存的筛选条件创建抑制规则：

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在调查发现页面上，选择抑制调查发现以打开抑制规则面板。

3. 从保存的规则下拉列表中，选择保存的筛选条件。
4. 您还可以添加新的筛选条件。如果您不需要其他筛选条件，请跳过此步骤。

要打开筛选条件菜单，请在添加筛选条件中输入 **filter criteria**。您可以从列表中选择一个条件。为所选条件输入一个有效值。

 Note

要确定有效值，请查看调查发现表，并选择要抑制的调查发现。在调查结果面板中查看其详细信息。

5. 输入抑制规则的名称和描述。有效字符包括字母数字字符、句点 (.)、破折号 (-)、下划线 (_) 和空格。
6. 选择保存。

API/CLI

要使用API以下方法创建禁止规则，请执行以下操作：

1. 您可以通过创建禁止规则 [CreateFilter](#) API。为此，请按照下面详述的示例格式在JSON文件中指定筛选条件。以下示例将抑制任何DNS请求到 test.example.com 域的未存档的低严重性搜索结果。对于中严重性调查发现，输入列表是 ["4", "5", "7"]。对于高严重性调查发现，输入列表是 ["6", "7", "8"]。您还可以根据列表中的任意一个值进行筛选。

```
{
  "Criterion": {
    "service.archived": {
      "Eq": [
        "false"
      ]
    },
    "service.action.dnsRequestAction.domain": {
      "Eq": [
        "test.example.com"
      ]
    },
    "severity": {
      "Eq": [
        "1",
        "2",

```

```
    "3"  
  ]  
}  
}
```

有关JSON字段名称及其控制台等效项的列表，请参阅[筛选条件属性](#)。

要测试您的筛选条件，请使用中的相同JSON标准 [ListFindings](#)API，并确认选择的结果是否正确。要使用您自己的.json 文件来测试您的筛选条件detectorId，AWS CLI 请按照示例进行操作。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
finding-criteria file://criteria.json
```

2. 上传要用作抑制规则的过滤器，[CreateFilter](#)API或者使用 AWS CLI以下示例，使用您自己的检测器 ID、抑制规则的名称和.json 文件。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的“设置”页面，或者运行[ListDetectors](#)API。

```
aws guardduty create-filter --action ARCHIVE --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria  
file://criteria.json
```

您可以使用以编程方式查看过滤器列表。[ListFilter](#)API您可以通过向提供筛选器名称来查看单个筛选器的详细信息[GetFilter](#)API。使用更新过滤器[UpdateFilter](#)或使用将其删除[DeleteFilter](#)API。

删除抑制规则

选择您的首选访问方法以删除用于 GuardDuty 查找类型的禁止规则。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。

2. 在调查发现页面上，选择抑制调查发现以打开抑制规则面板。
3. 从保存的规则下拉列表中，选择保存的筛选条件。
4. 选择 Delete rule (删除规则)。

API/CLI

运行 [DeleteFilter](#) API。为特定区域指定过滤器名称和关联的检测器 ID。

或者，您可以使用以下 AWS CLI 示例，替换格式为中的值 *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

要查找与您的账户和当前地区 `detectorId` 对应的，请参阅 <https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行 [ListDetectors](#) API。

使用可信 IP 列表和威胁列表

Amazon 通过分析和处理 VPC 流日志、AWS CloudTrail 事件日志和日志来 GuardDuty 监控您的 AWS 环境安全。DNS 您可以自定义此监控范围，配置 GuardDuty 为停止 IPs 来自您自己的可信 IP 列表的可信警报，并对自己的威胁列表 IPs 中的已知恶意软件发出警报。

可信 IP 列表和威胁列表仅适用于发往公开可路由 IP 地址的流量。列表的效果适用于所有 VPC 流日志和 CloudTrail 调查结果，但不适用于 DNS 调查结果。

GuardDuty 可以配置为使用以下类型的列表。

可信 IP 列表

可信 IP 列表由您信任的 IP 地址组成，这些地址用于与您的 AWS 基础架构和应用程序进行安全通信。GuardDuty 不会为可信 IP 列表上的 IP 地址生成 VPC 流日志或 CloudTrail 查找结果。单个可信 IP 列表中最多可以包含 2000 个 IP 地址和 CIDR 范围。在任何给定时间，每个区域的每个 AWS 账户只能上传一个可信 IP 列表。

威胁 IP 列表

威胁列表由已知的恶意 IP 地址组成。此列表可以由第三方威胁情报提供，也可以专门为您的组织创建。除了由于可能存在可疑活动而生成发现结果外，GuardDuty 还会根据这些威胁列表生成调查结果。单个威胁列表中最多可以包含 250,000 个 IP 地址和 CIDR 范围。GuardDuty 仅根据涉及威胁列

表中 IP 地址和CIDR范围的活动生成调查结果；这些发现结果不是根据域名生成的。在任何给定时间点，AWS 账户 每个区域最多可以上传六个威胁列表。

Note

如果在可信 IP 列表和威胁列表中包含相同的 IP，则可信 IP 列表将首先处理该 IP，并且不会生成调查发现。

在多账户环境中，只有 GuardDuty 管理员账户中的用户才能添加和管理可信 IP 列表和威胁列表。管理员账户上传的可信 IP 列表和威胁列表会被强加到其成员账户的 GuardDuty 功能上。换句话说，在成员账户 GuardDuty 中，根据涉及管理员账户威胁列表中已知恶意 IP 地址的活动生成调查结果，而不会根据涉及管理员账户可信 IP 列表中 IP 地址的活动生成调查结果。有关更多信息，请参阅 [在 Amazon 中管理多个账户 GuardDuty](#)。

列表格式

GuardDuty 接受以下格式的列表。

托管可信 IP 列表或威胁 IP 列表的每个文件的最大大小为 35MB。在您的可信 IP 列表和威胁 IP 列表中，IP 地址和CIDR范围必须每行显示一个。只接受IPv4地址。

- 纯文本 () TXT

此格式支持CIDR区块和单个 IP 地址。以下示例列表使用纯文本 (TXT) 格式。

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- 结构化威胁信息表达 (STIX)

此格式支持CIDR区块和单个 IP 地址。以下示例列表使用了该STIX格式。

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:ttp="http://stix.mitre.org/TTP-1"
```

```

xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:example="http://example.com/"
xsi:schemaLocation="
http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
version="1.2">
<stix:Observables cybox_major_version="1" cybox_minor_version="1">
  <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
    <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
      <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
        <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
          </cybox:Properties>
        </cybox:Object>
      </cybox:Observable>
    <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
      <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
          <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
            </cybox:Properties>
          </cybox:Object>
        </cybox:Observable>
      <cybox:Observable
id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
        <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">

```


⚠ Important

这些操作未包含在 AmazonGuardDutyFullAccess 托管策略中。

对可信 IP 列表和威胁列表使用服务器端加密

GuardDuty 支持列表的以下加密类型：SSE-AES256 和 SSE-KMS。SSE不支持-C。有关 S3 加密类型的更多信息，请参阅[使用服务器端加密保护数据](#)。

如果您的列表使用服务器端加密进行SSE加密，KMS则必须向 GuardDuty 服务相关角色授予解密文件的AWSServiceRoleForAmazonGuardDuty权限才能激活列表。在KMS密钥策略中添加以下声明，并将账户 ID 替换为您自己的账户 ID：

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

添加和激活可信 IP 列表或威胁 IP 列表

选择以下访问方法之一添加和激活可信 IP 列表或威胁 IP 列表。

Console

(可选) 步骤 1：获取URL列表的位置

1. 打开 Amazon S3 控制台，网址为<https://console.aws.amazon.com/s3/>。
2. 在导航窗格中，选择桶。
3. 选择包含要添加的特定列表的 Amazon S3 存储桶名称。
4. 选择对象（列表）名称以查看其详细信息。
5. 在“属性”选项卡下，复制此对象URI的 S3。

步骤 2：添加可信 IP 列表或威胁列表

Important

默认情况下，在任何给定时间点，您只能拥有一个可信 IP 列表。同样，您最多可以拥有 6 个威胁列表。

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择列表。
3. 在 List management 页面上，选择 Add a trusted IP list 或 Add a threat list。
4. 根据您的选择，将出现一个对话框。使用以下步骤：
 - a. 对于列表名称，输入列表的名称。

列表命名限制-列表名称可以包括小写字母、大写字母、数字、短划线 (-) 和下划线 (_)。
 - b. 对于位置，请提供您上传列表的位置。如果您还没有，请参阅 [Step 1: Fetching location URL of your list](#)。

位置格式 URL

 - <https://s3.amazonaws.com/bucket.name/file.txt>
 - <https://s3-aws-region.amazonaws.com/bucket.name/file.txt>
 - <http://bucket.s3.amazonaws.com/file.txt>
 - <http://bucket.s3-aws-region.amazonaws.com/file.txt>
 - <s3://bucket.name/file.txt>
 - c. 选中 I agree 复选框。
 - d. 选择 Add list。默认情况下，已添加列表的状态为非活动。要使列表生效，必须激活列表。

步骤 3：激活可信 IP 列表或威胁列表

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择列表。
3. 在列表管理页面上，选择要激活的列表。
4. 选择操作，然后选择激活。此列表最多可能需要 15 分钟才能生效。

API/CLI

对于可信 IP 列表

- 运行 [CreateIPSet](#)。务必提供要为其创建此可信 IP 列表的成员账户的 detectorId。

列表命名限制-列表名称可以包括小写字母、大写字母、数字、短划线 (-) 和下划线 (_)。

- 或者，您可以通过运行以下 AWS Command Line Interface 命令来执行此操作，并确保将 detector-id 替换为要为其更新可信 IP 列表的成员账户的检测器 ID。

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

对于威胁列表

- 运行 [CreateThreatIntelSet](#)。务必提供要为其创建此威胁列表的成员账户的 detectorId。
- 或者，您可以通过运行以下 AWS Command Line Interface 命令来执行此操作。务必提供要为其创建威胁列表的成员账户的 detectorId。

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/amzn-s3-demo-bucket2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

Note

激活或更新任何 IP 列表后，最多 GuardDuty 可能需要 15 分钟才能同步该列表。

更新可信 IP 列表和威胁列表

您可以更新列表名称，或更新添加到已添加并激活的列表中的 IP 地址。如果您更新了列表，则必须重新激活该列表 GuardDuty 才能使用最新版本的列表。

选择一种访问方法更新可信 IP 或威胁列表。

Console

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择列表。
3. 在列表管理页面上，选择要更新的可信 IP 集或威胁列表。
4. 选择操作，然后选择编辑。
5. 在更新列表对话框中，根据需要更新信息。

列表命名限制-列表名称可以包括小写字母、大写字母、数字、短划线 (-) 和下划线 (_)。

6. 选中我同意复选框，然后选择更新列表。状态列中的值将变为非活动。
7. 重新激活更新的列表
 - a. 在列表管理页面上，选择要再次激活的列表。
 - b. 选择操作，然后选择激活。

API/CLI

1. 运行 [UpdateIPSet](#) 以更新可信 IP 列表。
 - 或者，您可以运行以下 AWS CLI 命令来更新可信 IP 列表，并确保将 `detector-id` 替换为要为其更新可信 IP 列表的成员账户的检测器 ID。

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. 运行 [UpdateThreatIntelSet](#) 以更新威胁列表
 - 或者，您可以运行以下 AWS CLI 命令来更新威胁列表，并确保将 `detector-id` 替换为要为其更新威胁列表的成员账户的检测器 ID。

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

停用或删除可信 IP 列表或威胁列表

选择一种访问方法来删除（使用控制台）或停用（使用API/CLI）可信 IP 列表或威胁列表。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择列表。
3. 在列表管理页面上，选择要删除的列表。
4. 选择操作，然后选择删除。
5. 确认操作并选择删除。表中将不再提供特定列表。

API/CLI

1. 对于可信 IP 列表

运行 [UpdateIPSet](#) 以更新可信 IP 列表。

- 或者，您可以运行以下 AWS CLI 命令来更新可信 IP 列表，并确保将 `detector-id` 替换为要为其更新可信 IP 列表的成员账户的检测器 ID。

要查找与您的账户和当前地区 `detectorId` 对应的，请参阅<https://console.aws.amazon.com/guardduty/> 控制台中的设置页面，或运行 [ListDetectors](#) API。

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. 对于威胁列表

运行 [UpdateThreatIntelSet](#) 以更新威胁列表

- 或者，您可以运行以下 AWS CLI 命令来更新可信 IP 列表，并确保将 `detector-id` 替换为要为其更新威胁列表的成员账户的检测器 ID。

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

导出调查发现

GuardDuty 将生成的调查结果保留 90 天。GuardDuty 将活跃的调查结果导出到 Amazon EventBridge (EventBridge)。您可以选择将生成的调查结果导出到亚马逊简单存储服务 (Amazon S3) 存储桶。这将帮助您跟踪账户中潜在可疑活动的历史数据，并评估建议的补救措施是否成功。

生成的任何新的活跃发现将在 GuardDuty 生成结果后大约 5 分钟内自动导出。您可以设置将活动发现的更新导出到的频率 EventBridge。您选择的频率适用于将新出现的现有发现导出到 S3 存储桶 (配置后) 和 Detective (集成后)。EventBridge 有关如何 GuardDuty 汇总多个出现的现有发现的信息，请参阅 [GuardDuty 查找聚合](#)

在配置设置以将调查结果导出到 Amazon S3 存储桶时，GuardDuty 使用 AWS Key Management Service (AWS KMS) 对 S3 存储桶中的调查结果数据进行加密。这要求您为 S3 存储桶和 AWS KMS 密钥添加权限，以便 GuardDuty 可以使用它们导出账户中的调查结果。

内容

- [注意事项](#)
- [步骤 1-导出调查结果所需的权限](#)
- [第 2 步 — 将策略附加到您的密钥 KMS](#)
- [第 3 步 — 将策略附加到 Amazon S3 存储桶](#)
- [步骤 4-将调查结果导出到 S3 存储桶 \(控制台\)](#)
- [步骤 5-设置导出更新的活动发现的频率](#)

注意事项

在继续执行导出结果的先决条件和步骤之前，请考虑以下关键概念：

- 导出设置是区域性的 — 您需要在使用的每个区域中配置导出选项 GuardDuty。
- 将调查结果导出到不同 AWS 区域 (跨区域) 的 Amazon S3 存储桶 — GuardDuty 支持以下导出设置：
 - 您的 Amazon S3 存储桶或对象以及 AWS KMS 密钥必须属于同一存储桶或对象 AWS 区域。
 - 对于在商业区域生成的调查结果，您可以选择将这些发现导出到任何商业区域的 S3 存储桶中。但是，您无法将这些发现导出到可选区域的 S3 存储桶中。
 - 对于在选择加入区域生成的调查结果，您可以选择将这些发现导出到生成这些结果的同一个选择加入区域或任何商业区域。但是，您无法将调查结果从一个选择加入区域导出到另一个选择加入区域。

- 导出调查结果的权限-要配置导出活动发现的设置，您的 S3 存储桶必须具有 GuardDuty 允许上传对象的权限。您还必须拥有 GuardDuty 可用于加密发现结果的密 AWS KMS 钥。
- 不导出存档的查找结果-默认行为是不导出存档的查找结果，包括隐藏的查找结果的新实例。

当 GuardDuty 查找结果生成为“已存档”时，您需要将其取消存档。这会将筛选器查找状态更改为“活动”。GuardDuty 根据您的配置[步骤 5-导出调查结果的频率](#)将更新导出到现有未存档的查找结果。

- GuardDuty 管理员帐户可以导出关联成员帐户中生成的调查结果-当您在管理员帐户中配置导出结果时，在同一区域中生成的关联成员帐户的所有结果也将导出到您为管理员帐户配置的相同位置。有关更多信息，请参阅[了解 GuardDuty 管理员账户和成员账户之间的关系](#)。

步骤 1-导出调查结果所需的权限

在配置导出调查结果的设置时，您可以选择一个用于存储调查结果的 Amazon S3 存储桶和用于数据加密的 AWS KMS 密钥。除了 GuardDuty 操作权限外，您还必须拥有以下操作的权限，才能成功配置用于导出结果的设置：

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`

第 2 步 — 将策略附加到您的密钥 KMS

GuardDuty 使用对存储桶中的调查结果数据进行 AWS Key Management Service 加密。要成功配置设置，必须先 GuardDuty 授予使用 KMS 密钥的权限。您可以通过将[策略附加](#)到 KMS 密钥来授予权限。

当您使用其他帐户的 KMS 密钥时，您需要通过登录拥有 AWS 帐户 该密钥的帐户来应用密钥策略。将设置配置为导出结果时，还需要拥有密钥 ARN 的帐户的密钥。

修改的 KMS 密钥策略 GuardDuty 以加密导出的结果

1. 在 <https://console.aws.amazon.com/kms> s 处打开控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 选择现有 KMS 密钥或执行《AWS Key Management Service 开发人员指南》中[创建新密钥](#)的步骤，您将使用该密钥对导出的结果进行加密。

Note

您的KMS密钥和 Amazon S3 存储桶的密钥必须相同。AWS 区域

您可以使用相同的 S3 存储桶和 KMS key pair 从任何适用区域导出调查结果。有关更多信息，[注意事项](#) 请参阅，了解如何跨区域导出调查结果。

4. 在 Key policy (密钥策略) 部分，选择 Edit (编辑)。

如果显示“切换到策略视图”，请选择它以显示密钥策略，然后选择“编辑”。

5. 将以下策略块复制到您的KMS密钥策略中，以授予使用您的密钥的 GuardDuty 权限。

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

6. 通过替换以下格式化值来编辑策略 *red* 在策略示例中：

1. Replace (替换) *KMS key ARN* 使用KMS密钥的 Amazon 资源名称 (ARN)。要找到密钥 ARN，请参阅[查找密钥 ID 和ARN](#) 《AWS Key Management Service 开发人员指南》。
2. Replace (替换) *123456789012* 使用拥有导出调查结果的 GuardDuty 账户的 AWS 账户 ID。
3. Replace (替换) *Region2* 以及 AWS 区域 GuardDuty 发现的产生地。
4. Replace (替换) *SourceDetectorID* 加detectorID上调查结果产生的特定地区的 GuardDuty 账户。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectors](#)API。

Note

如果您在选择加入的区域 GuardDuty 中使用，请将“服务”的值替换为该地区的区域终端节点。例如，如果您 GuardDuty 在中东（巴林）(me-south-1) 地区使用，请替换为。"Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com"有关每个选择加入区域的终端节点的信息，请参阅[GuardDuty 终端节点和配额](#)。

7. 如果您在最后一语句之前添加了策略声明，请在添加此语句之前添加逗号。确保KMS密钥策略的JSON语法有效。

选择保存。

8. （可选）将密钥复制ARN到记事本中，以便在后续步骤中使用。

第 3 步 — 将策略附加到 Amazon S3 存储桶

向要将结果导出到的 Amazon S3 存储桶添加权限，以便 GuardDuty 可以将对象上传到此 S3 存储桶。无论使用属于您的账户还是其他账户的 Amazon S3 存储桶 AWS 账户，您都必须添加这些权限。

如果您在任何时候决定将调查结果导出到其他 S3 存储桶，则要继续导出调查结果，则必须向该 S3 存储桶添加权限并重新配置导出查找结果设置。

如果您还没有要将这些发现导出的 Amazon S3 存储桶，请参阅 Amazon S3 用户指南中的[创建存储桶](#)。

为您的 S3 存储桶策略附加权限

1. 执行 Amazon S3 用户指南中[创建或编辑存储桶策略](#)下的步骤，直到出现编辑存储桶策略页面。
2. 示例策略显示了如何授予将调查结果导出到 Amazon S3 存储桶的 GuardDuty 权限。如果在配置导出查找结果后更改路径，则必须修改策略以授予对新位置的权限。

复制以下示例策略并将其粘贴到存储桶策略编辑器中。

如果您在最后一语句之前添加了策略声明，请在添加此语句之前添加逗号。确保KMS密钥策略的JSON语法有效。

S3 存储桶示例策略

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGuardDutygetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": "Amazon S3 bucket ARN",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "AllowGuardDutyPutObject",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    }
  ]
}

```

```

    "Sid": "DenyUnencryptedUploadsThis is optional",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "aws:kms"
      }
    }
  },
  {
    "Sid": "DenyIncorrectHeaderThis is optional",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
      }
    }
  },
  {
    "Sid": "DenyNon-HTTPS",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    }
  }
]
}

```

3. 通过替换以下格式化值来编辑策略 *red* 在策略示例中：

1. Replace (替换) *Amazon S3 bucket ARN* 使用亚马逊 S3 存储桶的亚马逊资源名称 (ARN)。您可以在<https://console.aws.amazon.com/s3/>控制台的编辑存储桶策略页面ARN上找到该存储桶。
2. Replace (替换) *123456789012* 使用拥有导出调查结果的 GuardDuty 账户的 AWS 账户 ID。
3. Replace (替换) *Region2* 以及 AWS 区域 GuardDuty 发现的产生地。
4. Replace (替换) *SourceDetectorID* 加detectorID上调查结果产生的特定地区的 GuardDuty 账户。

要查找与您的账户和当前地区detectorId对应的，请参阅<https://console.aws.amazon.com/guardduty/>控制台中的设置页面，或运行[ListDetectorsAPI](#)。

5. Replace (替换) *[optional prefix]* 的一部分 *S3 bucket ARN/[optional prefix]* 占位符值，其中包含要将结果导出到的可选文件夹位置。有关使用前缀的更多信息，请参阅 Amazon S3 用户指南中的[使用前缀组织对象](#)。

当您提供尚不存在的可选文件夹位置时，仅当与 S3 存储桶关联的账户与导出结果的账户相同时，才 GuardDuty会创建该位置。将调查结果导出到属于其他账户的 S3 存储桶时，该文件夹的位置必须已经存在。

6. Replace (替换) *KMS key ARN* 使用与导出到 S3 存储桶的调查结果的加密相关的KMS密钥的 Amazon 资源名称 (ARN)。要找到密钥ARN，请参阅[查找密钥 ID 和ARN](#)《AWS Key Management Service 开发人员指南》。

Note

如果您在选择加入的区域 GuardDuty 中使用，请将“服务”的值替换为该地区的区域终端节点。例如，如果您 GuardDuty 在中东 (巴林) (me-south-1) 地区使用，请替换为。"Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com"有关每个选择加入区域的终端节点的信息，请参阅[GuardDuty 终端节点和配额](#)。

4. 选择保存。

步骤 4-将调查结果导出到 S3 存储桶 (控制台)

GuardDuty 允许您将调查结果导出到另一个存储桶中的现有存储桶 AWS 账户。

在创建新的 S3 存储桶或选择账户中的现有存储桶时，您可以添加可选前缀。配置导出调查结果时，请在 S3 存储桶中为查找结果 GuardDuty 创建一个新文件夹。前缀将附加到 GuardDuty 创建的默认文件夹结构中。例如，可选前缀的格式为 `/AWSLogs/123456789012/GuardDuty/Region`。

S3 对象的整个路径将是 `amzn-s3-demo-bucket/prefix-name/UUID.json.gz`。UUID 是随机生成的，不代表探测器 ID 或发现 ID。

Important

KMS 密钥和 S3 存储桶必须位于同一区域。

在完成这些步骤之前，请确保已将相应的策略附加到 KMS 密钥和现有 S3 存储桶。

配置导出结果

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 在导航窗格中，选择 Settings (设置)。
3. 在“设置”页面的“查找结果导出选项”下，对于 S3 存储桶，选择立即配置 (或根据需要编辑)。
4. 对于 S3 存储桶 ARN，请输入 **bucket ARN**。要查找存储桶 ARN，请参阅 Amazon S3 用户指南中的 [查看 S3 存储桶的属性](#)。在 <https://console.aws.amazon.com/guardduty/> 控制台中关联存储桶的“属性”页面的“权限”选项卡中。
5. 对于 KMS 密钥 ARN，请输入 **key ARN**。要找到密钥 ARN，请参阅 [查找密钥 ID 和 ARN](#) 《AWS Key Management Service 开发人员指南》。
6. 附加策略
 - 执行相关步骤以附加 S3 存储桶策略。有关更多信息，请参阅 [第 3 步 — 将策略附加到 Amazon S3 存储桶](#)。
 - 执行附加 KMS 密钥策略的步骤。有关更多信息，请参阅 [第 2 步 — 将策略附加到您的密钥 KMS](#)。
7. 选择保存。

步骤 5-设置导出更新的活动发现的频率

根据您的环境配置导出更新的活动发现的频率。默认情况下，每 6 小时导出一次更新的调查发现。这意味着，在最近一次导出之后更新的任何调查发现都包含在下一次导出的内容中。如果每 6 小时导出一次更新的调查发现，且导出发生在 12:00，则在 12:00 后更新的任何调查发现都会在 18:00 导出。

要设置频率

1. 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。
2. 选择设置。
3. 在调查发现导出选项部分，选择更新调查发现的频率。这设置了将更新的活跃调查结果导出到 Amazon S3 EventBridge 和 Amazon S3 的频率。可从以下选项中进行选择：
 - 每 15 分钟更新 EventBridge 一次 S3
 - 每 1 小时更新 EventBridge 一次 S3
 - 每 6 小时更新CWE一次 S3 (默认)
4. 选择 Save changes (保存更改)。

使用 Amazon CloudWatch Events 创建对 GuardDuty 调查结果的自定义响应

GuardDuty 当调查结果发生任何变化时，会为 [Amazon Events 创建 CloudWatch 事件](#)。将创建 CloudWatch 事件的查找更改包括新生成的调查结果或新汇总的调查结果。尽最大努力发出事件。

每个 GuardDuty 发现都被分配了一个查找 ID。GuardDuty 使用唯一的查找 ID 为每个发现创建一个 CloudWatch 事件。现有调查发现的所有后续实例都会聚合到原始调查发现中。有关更多信息，请参阅 [GuardDuty 查找聚合](#)。

Note

如果您的账户是 GuardDuty 委托管理员，则 CloudWatch 事件将发布到您的账户以及生成调查结果的成员账户。

通过将 CloudWatch 事件与配合使用 GuardDuty，您可以自动执行任务，以帮助您应对 GuardDuty 调查结果所揭示的安全问题。

要接收有关基于 CloudWatch 事件的 GuardDuty 发现的通知，您必须为创建 CloudWatch 事件规则和 GuardDuty 目标。通过此规则 CloudWatch，可以将 GuardDuty 生成的结果通知发送到规则中指定的目标。有关更多信息，请参阅 [为 GuardDuty \(CLI\) 创建 CloudWatch 事件规则和目标](#)。

主题

- [CloudWatch 的事件通知频率 GuardDuty](#)
- [CloudWatch 的事件格式 GuardDuty](#)
- [创建 CloudWatch 事件规则以通知您 GuardDuty 发现的结果 \(控制台\)](#)
- [为 GuardDuty \(CLI\) 创建 CloudWatch 事件规则和目标](#)
- [CloudWatch GuardDuty 多账户环境的事件](#)

CloudWatch 的事件通知频率 GuardDuty

具有唯一调查发现 ID 的新生成调查发现的通知

GuardDuty 在发现后的 5 分钟内根据其 CloudWatch 事件发送通知。此事件（和此通知）还包括此调查发现的所有后续事件，这些事件在具有唯一 ID 的调查发现生成后 5 分钟内发生。

Note

默认情况下，有关新生成的调查发现的通知频率为 5 分钟。此频率无法更新。

后续调查发现事件的通知

默认情况下，对于每个具有唯一查找结果 ID 的查找结果，GuardDuty 会将在 6 小时时间间隔内发生的特定查找类型的所有后续事件聚合到一个事件中。GuardDuty 然后根据此事件发送有关这些后续事件的通知。默认情况下，对于后续出现的现有调查结果，GuardDuty 会每 6 小时根据 CloudWatch 事件发送一次通知。

只有管理员帐户可以自定义发送有关事件后续发现事件的通知的默认频率。CloudWatch 成员帐户中的用户无法自定义此频率。管理员帐户在其自己的帐户中设置的频率值适用于其所有成员帐户的 GuardDuty 功能。如果管理员帐户中的用户将此频率值设置为 1 小时，则所有成员帐户也将有 1 小时的频率接收有关后续发现事件的通知。有关更多信息，请参阅 [在 Amazon 中管理多个帐户 GuardDuty](#)。

Note

作为管理员帐户，您可以自定义有关后续查找事件的默认通知频率。可能的值为 15 分钟、1 小时或 6 小时（默认值）。有关设置通知频率的信息，请参阅 [步骤 5-设置导出更新的活动发现的频率](#)。

使用“CloudWatch 事件”监控存档的 GuardDuty调查结果

对于手动存档的调查结果，这些发现的初次和所有后续出现的结果（存档完成后生成）将按上述频率发送到“CloudWatch 事件”。

对于自动存档的查找结果，这些发现的初次和所有后续出现的结果（存档完成后生成）不会发送到 Events。CloudWatch

CloudWatch 的事件格式 GuardDuty

CloudWatch [的事件](#) GuardDuty 采用以下格式。

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
  "detail-type": "GuardDuty Finding",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

Note

“detail”值将单个调查发现的 JSON 详细信息作为对象返回，而不是返回“findings”值，后者可以支持数组中的多个调查发现。

有关在 GUARDDUTY_FINDING_JSON_OBJECT 中包括的所有参数的完整列表，请参阅 [GetFindings](#)。在 GUARDDUTY_FINDING_JSON_OBJECT 中显示的 id 参数是之前介绍的调查发现 ID。

创建 CloudWatch 事件规则以通知您 GuardDuty 发现的结果（控制台）

您可以 GuardDuty 将 CloudWatch 事件与一起使用，通过将查找事件发送到消息中心来设置自动 GuardDuty 查找警报，以帮助提高 GuardDuty 发现结果的可见性。本主题向您展示如何通过设置 SNS 主题然后将该主题与事件规则关联来向电子邮件、Slack 或 Amazon Chime 发送调查结果提醒。CloudWatch

设置 Amazon SNS 主题和端点

首先，您必须在 Amazon Simple Notification Service 中设置一个主题并添加一个端点。有关更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的[入门](#)。

此过程用于确定要将 GuardDuty 查找数据发送到何处。在创建 CloudWatch 事件规则期间或之后，可以将 SNS 主题添加到事件规则中。

Email setup

创建 SNS 主题

1. 登录 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 从导航窗格中选择 Topics (主题)，然后选择 Create Topic (创建主题)。
3. 在创建主题部分，选择标准。接下来，输入主题名称，例如 **GuardDuty_to_Email**。其他详细信息是可选的。
4. 选择创建主题。此时系统会打开新主题的主题详细信息。
5. 在“Subscriptions (订阅)”部分中，选择 Create Subscription (创建订阅)。
6.
 - a. 从协议菜单中选择电子邮件。
 - b. 在 Endpoint (终端节点) 字段中，添加您想要用于接收通知的电子邮件地址。

Note

创建后，您需要通过电子邮件客户端确认订阅。

c. 选择创建订阅

7. 在收件箱中查收订阅消息，然后选择 Confirm Subscription (确认订阅)

Slack setup

创建 SNS 主题

1. 登录 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 从导航窗格中选择 Topics (主题)，然后选择 Create Topic (创建主题)。
3. 在创建主题部分，选择标准。接下来，输入主题名称，例如 **GuardDuty_to_Slack**。其他详细信息是可选的。选择创建主题以完成。

配置 AWS Chatbot 客户端

1. 导航到 AWS Chatbot 控制台
2. 从配置的客户端面板中，选择配置新客户端。
3. 选择 Slack 并单击“配置”进行确认。

Note

选择 Slack 时，您必须选择“允许”以确认 AWS Chatbot 访问通道的权限。

4. 选择配置新通道以打开配置详细信息窗格。
 - a. 输入通道的名称。
 - b. 对于 Slack 通道，选择您要使用的通道。要将私有 Slack 通道与 AWS Chatbot 结合使用，请选择私有通道。
 - c. 在 Slack 中，右键单击通道名称并选择“复制链接”来复制私有通道的通道 ID。
 - d. 在 AWS 管理控制台的 AWS Chatbot 窗口中，将从 slack 复制的 ID 粘贴到私有通道 ID 字段。
 - e. 在权限中，如果您还没有角色，请选择使用模板创建 IAM 角色。
 - f. 对于策略模板，选择“通知”权限。这是 AWS Chatbot 的 IAM policy 模板。它为 CloudWatch 警报、事件和日志以及 Amazon SNS 主题提供了必要的读取和列出权限。
 - g. 选择您之前在其中创建 SNS 主题的区域，然后选择您创建的用于向 Slack 通道发送通知的 Amazon SNS 主题。
5. 选择配置。

Chime setup

创建 SNS 主题

1. 登录 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v3/home>。
2. 从导航窗格中选择 Topics (主题)，然后选择 Create Topic (创建主题)。
3. 在创建主题部分，选择标准。接下来，输入主题名称，例如 **GuardDuty_to_Chime**。其他详细信息是可选的。选择创建主题以完成。

配置 AWS Chatbot 客户端

1. 导航到 AWS Chatbot 控制台
2. 从配置的客户端面板中，选择配置新客户端。
3. 选择 Chime 并单击“配置”进行确认。
4. 在配置详细信息窗格中，输入通道的名称。
5. 在 Chime 中打开所需的聊天室
 - a. 选择右上角的齿轮图标，然后选择管理 Webhook 和自动程序。
 - b. 选择复制 URL 以将 Webhook URL 复制到剪贴板。
6. 在 AWS 管理控制台的 AWS Chatbot 窗口中，将复制的 URL 粘贴到 Webhook URL 字段。
7. 在权限中，如果您还没有角色，请选择使用模板创建 IAM 角色。
8. 对于策略模板，选择“通知”权限。这是 AWS Chatbot 的 IAM policy 模板。它为 CloudWatch 警报、事件和日志以及 Amazon SNS 主题提供了必要的读取和列出权限。
9. 选择您之前在其中创建 SNS 主题的区域，然后选择您创建的用于向 Chime 聊天室发送通知的 Amazon SNS 主题。
10. 选择配置。

为 GuardDuty调查结果设置一个 CloudWatch 事件

1. 打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 从导航窗格中选择 Rules (规则)，然后选择 Create Rule (创建规则)。
3. 从“服务名称”菜单中选择 GuardDuty。
4. 从“事件类型”菜单中选择“GuardDuty查找”。
5. 在 Event Pattern Preview (事件模式预览) 中，选择 Edit (编辑)。

6. 将下面的 JSON 代码粘贴到 Event Pattern Preview (事件模式预览) 中，然后选择 Save (保存)

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
```

```
        6.9,  
        7,  
        7.0,  
        7.1,  
        7.2,  
        7.3,  
        7.4,  
        7.5,  
        7.6,  
        7.7,  
        7.8,  
        7.9,  
        8,  
        8.0,  
        8.1,  
        8.2,  
        8.3,  
        8.4,  
        8.5,  
        8.6,  
        8.7,  
        8.8,  
        8.9  
    ]  
}  
}
```

Note

上面的代码将对任何中到高严重性调查发现发出提醒。

7. 在 Targets (目标) 部分，单击 Add Target (添加目标)。
8. 从 Select Targets (选择目标) 菜单中，选择 SNS Topic (SNS 主题)。
9. 对于 Select Topic (选择主题)，请选择您在步骤 1 中创建的 SNS 主题的名称。
10. 配置事件的输入。
 - 如果您要为 Chime 或 Slack 设置通知，请跳到步骤 11，则输入类型默认为匹配事件。
 - 如果您要通过 SNS 设置电子邮件通知，请按照以下步骤自定义发送到收件箱的消息：
 - a. 展开 Configure input (配置输入)，然后选择 Input Transformer (输入转换器)。

- b. 复制以下代码并将其粘贴到 Input Path (输入路径) 字段中。

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

- c. 复制以下代码并将其粘贴到 Input Template (输入模板) 字段中，以便格式化电子邮件。

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
<Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. 单击 Configure Details (配置详细信息)。
12. 在 Configure rule details (配置规则详细信息) 页面中，输入规则的名称 (Name) 和 Description (描述)，然后选择 Create Rule (创建规则)。

为 GuardDuty (CLI) 创建 CloudWatch 事件规则和目标

以下过程说明如何使用 AWS CLI 命令为其创建 CloudWatch 事件规则和目标 GuardDuty。具体而言，该过程向您展示了如何创建一个规则，该规则 CloudWatch 允许为 GuardDuty 生成的所有发现发送事件，并添加一个 AWS Lambda 函数作为规则的目标。

Note

除了 Lambda 函数外，还 CloudWatch 支持以下目标类型：亚马逊 EC2 实例、Amazon Kinesis 直播、亚马逊 ECS 任务 AWS Step Functions、状态机、run 命令 GuardDuty 和内置目标。

您也可以 GuardDuty 通过 CloudWatch 事件控制台为其创建 CloudWatch 事件规则和目标。有关更多信息和详细步骤，请参阅[创建在 CloudWatch 事件上触发的事件规则](#)。在事件源部分，对于服务名称，选择 **GuardDuty**；对于事件类型，选择 **GuardDuty Finding**。

创建规则和目标

1. 要创建允许为 GuardDuty 生成的所有发现发送事件的规则，请运行 CloudWatch 以下 CloudWatch CLI 命令。

```
AWS events put-rule --name Test --event-pattern "{\"source\":  
[\"aws.guardduty\"]}"
```

Important

您可以进一步自定义规则，CloudWatch 使其指示仅针对 GuardDuty 生成的结果的子集发送事件。该子集基于规则中指定的一个或多个调查发现属性。例如，使用以下 CLI 命令创建一条规则，CloudWatch 允许仅针对严重性为 5 或 8 的 GuardDuty 发现发送事件：

```
AWS events put-rule --name Test --event-pattern "{\"source\":  
[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],  
\"detail\":{\"severity\":[5,8]}}"
```

为此，您可以使用 JSON 中可用的任何属性值来查找 GuardDuty 结果。

2. 要附加 Lambda 函数作为您在步骤 1 中创建的规则的目标，请运行以下 CL CloudWatch I 命令。

```
AWS events put-targets --rule Test --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

Note

请务必将<your_function>上述命令中的事件替换为实际的 Lambda 函数。GuardDuty

3. 要添加调用目标所需的权限，请运行以下 Lambda CLI 命令。

```
AWS lambda add-permission --function-name <your_function> --statement-  
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Note

请务必将<your_function>上述命令中的事件替换为实际的 Lambda 函数。GuardDuty

Note

在上面的步骤中，我们使用 Lambda 函数作为触发 CloudWatch 事件的规则的目标。您也可以将其他 AWS 资源配置为触发 CloudWatch 事件的目标。有关更多信息，请参阅 [PutTargets](#)。

CloudWatch GuardDuty 多账户环境的事件

作为 GuardDuty 管理员，您的账户中的 CloudWatch 事件规则将根据您的成员账户的适用发现触发。这意味着，如果您通过管理员账户中的“CloudWatch 事件”设置查找通知（如上一节所述），则除了您自己的调查结果外，您还会收到由您的成员账户生成的高严重性和中等严重性调查结果的通知。

您可以使用 GuardDuty 查找结果的 JSON 详细信息 `accountId` 字段来标识搜索结果的来源成员账户。

要开始在控制台中为环境中的特定成员账户编写自定义事件规则，请创建新规则，并将以下模板粘贴到“事件模式预览”中，同时添加要触发事件的成员账户的账户 ID。

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

Note

此示例将在列出的账户 ID 的任何调查发现上触发。可添加多个 ID，按照 JSON 语法用逗号分隔。

了解 EC2 恶意软件防护扫描期间跳过资源的 CloudWatch 日志和原因

GuardDuty EC2 恶意软件防护将事件发布到您的亚马逊 CloudWatch 日志组 `/aws/guardduty/malware-scan-events`。对于与恶意软件扫描相关的每个事件，您可以监控受影响资源的状态和扫描结果。在 EC2 恶意软件防护扫描期间，某些 Amazon EC2 资源和 Amazon EBS 卷可能已被跳过。

审计 EC2 GuardDuty 恶意软件防护中的 CloudWatch 日志

`/aws/guardduty/malware-scan-events` CloudWatch 日志组中支持三种类型的扫描事件。

EC2 恶意软件防护扫描事件名称	说明
EC2_SCAN_STARTED	在 EC2 GuardDuty 恶意软件防护启动恶意软件扫描过程（例如准备拍摄 EBS 卷快照）时创建。
EC2_SCAN_COMPLETED	在针对受影响资源的至少一个 EBS 卷的 EC2 GuardDuty 恶意软件防护扫描完成时创建。此事件还包括属于扫描的 EBS 卷的 <code>snapshotId</code> 。扫描完成后，扫描结果将是 <code>CLEAN</code> 、 <code>THREATS_FOUND</code> 或 <code>NOT_SCANNED</code> 。
EC2_SCAN_SKIPPED	在 EC2 GuardDuty 恶意软件防护扫描跳过受影响资源的所有 EBS 卷时创建。要确定跳过的原因，请选择相应的事件并查看详细信息。有关跳过原因的更多信息，请参见下文的 恶意软件扫描期间跳过资源的原因 。

Note

如果您使用的是 AWS Organizations，Organizations 中成员账户中的 CloudWatch 日志事件会同时发布到管理员帐户和成员账户的日志组。

选择您首选的访问方式来查看和查询 CloudWatch 事件。

Console

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 在导航窗格中，在日志下选择日志组。选择 /aws/guardduty/ malware-scan-events 日志组以查看 EC2 恶意软件防护的扫描事件。GuardDuty

要运行查询，选择 Log Insights。

有关运行查询的信息，请参阅 Amazon CloudWatch 用户指南中的[使用 Log Insights 分析日志数据](#)。

3. 选择扫描 ID 以监控受影响资源和恶意软件调查发现的详细信息。例如，您可以使用运行以下查询来筛选 CloudWatch 日志事件 scanId。务必使用您自己的有效 **## ID**。

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- 要使用日志组，请参阅[使用 Amazon CloudWatch 用户指南 AWS CLI 中的搜索日志条目](#)。

选择 /aws/guardduty/ malware-scan-events 日志组以查看 EC2 恶意软件防护的扫描事件。GuardDuty

- 要查看和筛选日志事件，请分别参阅 [GetLogEvents](#) Amazon CloudWatch API 参考中的和 [FilterLogEvents](#)

GuardDuty EC2 日志保留的恶意软件防护

/aws/guardduty/ malware-scan-events 日志组的默认日志保留期为 90 天，之后日志事件将自动删除。要更改日志组的日志保留策略，请参阅《亚马逊 CloudWatch 用户指南》中的“CloudWatch 日志”或《亚马逊 CloudWatch [API 参考](#)》PutRetentionPolicy 中的“[更改日志数据保留期](#)”。CloudWatch

恶意软件扫描期间跳过资源的原因

在与恶意软件扫描相关的事件中，可能在扫描过程中跳过某些 EC2 资源和 EBS 卷。下表列出了 EC2 GuardDuty 恶意软件防护可能无法扫描资源的原因。如果适用，请使用建议的步骤来解决这些问题，

并在下次 EC2 GuardDuty 恶意软件防护启动恶意软件扫描时扫描这些资源。其他问题用于告知您事件的过程，且不可采取行动。

跳过的原因	说明	建议的步骤
RESOURCE_NOT_FOUND	在resourceArn 您的 AWS 环境中找不到用于启动按需恶意软件扫描的。	验证您的 Amazon EC2 实例或容器工作负载的 resourceArn ，然后重试。
ACCOUNT_INELIGIBLE	您尝试启动按需恶意软件扫描的 AWS 账户 ID 尚未启用 GuardDuty。	确认 GuardDuty 该 AWS 账户已启用。 在新版本 GuardDuty 中启用后 AWS 区域，最多可能需要 20 分钟才能同步。
UNSUPPORTED_KEY_ENCRYPTION	GuardDuty EC2 恶意软件防护支持未加密和使用客户托管密钥加密的卷。不支持扫描使用 Amazon EBS 加密 进行加密的 EBS 卷。 目前，在不适用此跳过理由的情况下，存在地区差异。有关这些内容的更多信息 AWS 区域，请参阅特定于区域的功能可用性 。	将您的加密密钥替换为客户托管式密钥。有关 GuardDuty 支持的加密类型的更多信息，请参阅 支持用于恶意软件扫描的 Amazon EBS 卷 。
EXCLUDED_BY_SCAN_SETTINGS	在恶意软件扫描期间，EC2 实例或 EBS 卷被排除在外。有两种可能性：要么将	更新您的扫描选项或与您的 Amazon EC2 资源关联的标签。有关更多信息，请参阅

跳过的原因	说明	建议的步骤
	标签添加到包含列表中但资源未与此标签关联，要么将标签添加到排除列表并且资源与此标签相关联，要么此资源的 GuardDuty Excluded 标签设置为了 true。	使用用户定义的标签扫描选项 。
UNSUPPORTED_VOLUME_SIZE	容量大于 2048 GB。	不可操作。
NO_VOLUME_S_ATTACHED	GuardDuty EC2 恶意软件防护在您的账户中找到了该实例，但没有将 EBS 卷附加到该实例以继续扫描。	不可操作。
UNABLE_TO_SCAN	这是内部服务错误。	不可操作。
SNAPSHOT_NOT_FOUND	找不到从 EBS 卷创建并与服务账户共享的快照，且 EC2 GuardDuty 恶意软件防护无法继续扫描。	检查 CloudTrail 以确保快照不是故意删除的。
SNAPSHOT_QUOTA_REACHED	您已达到每个区域允许的最大快照容量。这不仅可以防止保留快照，还可以防止创建新快照。	您可以移除旧快照或请求增加配额。您可以在《AWS 一般参考指南》的 服务限额 下查看每个区域快照的默认限制以及如何申请增加配额。

跳过的原因	说明	建议的步骤
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	已将超过 11 个 EBS 卷附加到一个 EC2 实例。GuardDuty EC2 恶意软件防护扫描了前 11 个 EBS 卷，这些卷是通过 deviceName 按字母顺序排序获得的。	不可操作。
UNSUPPORTED_PRODUCT_CODE_TYPE	GuardDuty 不支持使用 as 扫描实例 productCode 例 marketplace。有关更多信息，请参阅 Amazon EC2 用户指南中的 付费 AMI 。 有关 productCode 的更多信息，请参阅《Amazon EC2 API 参考》中的 ProductCode 。	不可操作。


在 EC2 GuardDuty 恶意软件防护中报告误报

GuardDuty EC2 的恶意软件保护扫描可能会将您的 Amazon EC2 实例或容器工作负载中的无害文件识别为恶意文件或有害文件。为了改善您使用适用于 EC2 和该 GuardDuty 服务的恶意软件防护的体验，如果您认为在扫描期间被识别为恶意或有害的文件实际上不包含恶意软件，则可以报告误报结果。

误报文件提交

1. 登录 <https://console.aws.amazon.com/guardduty> 控制台。
2. 当您发现看似误报的结果时，请联系 AWS Support 以启动误报文件提交流程。

3. 选择恶意软件扫描。
4. 选择扫描以查看其调查发现 ID。
5. 提供调查发现 ID。您还必须提供文件的 SHA-256 哈希。这是确保适用于 EC2 的 GuardDuty 恶意软件防护收到正确文件所必需的。
6. 该 AWS Support 团队将为您提供一个亚马逊简单存储服务 (S3) URL，您可以用它来上传文件和 SHA-256 哈希。成功上传文件后通知 AWS Support 团队。

 Warning

请勿直接向 AWS Support 提供文件或 SHA-256 哈希。您只能通过提供的 URL 将文件和哈希上传到 Amazon S3。如果您在收到 URL 后 7 天内未上传文件和哈希，该 URL 将失效。如果 URL 失效，您必须联系 AWS Support 以接收新的 URL。

GuardDuty 将您的文件保留不超过 30 天。GuardDuty 团队成员将分析您提交的内容，并采取适当措施来改善您使用适用于 EC2 的恶意软件防护和 GuardDuty 服务的体验。

修复发现的安全问题 GuardDuty

Amazon GuardDuty 生成的[调查结果](#)表明存在潜在的安全问题。在此版本中 GuardDuty，潜在的安全问题表明您的环境中的 EC2 实例或容器工作负载受损，或者您的 AWS 环境中存在一组凭据泄露。以下各节介绍了针对这些场景的建议修复步骤。如果有其他修复方案，将在具体调查发现类型的条目中加以说明。您可以从[活动调查发现类型表](#)中选择某一调查发现类型，即可获取该类型的完整信息。

内容

- [修复可能遭到入侵的 Amazon 实例 EC2](#)
- [修复可能遭到入侵的 S3 存储桶](#)
- [修复可能有恶意的 S3 对象](#)
- [修复可能受损的集群 ECS](#)
- [修复可能被泄露的凭证 AWS](#)
- [修复可能受损的独立容器](#)
- [修复 EKS 审计日志监控调查发现](#)
- [修复运行时监控结果](#)
- [修复可能受损的数据库](#)
- [修复可能受损的 Lambda 函数](#)

修复可能遭到入侵的 Amazon 实例 EC2

请按照以下建议步骤修复 AWS 环境中可能受到威胁的 EC2 实例：

1. 识别可能遭到入侵的 Amazon EC2 实例

调查可能遭盗用实例中的恶意软件，并清除任何发现的恶意软件。您可以使用[按需恶意软件扫描](#)来识别可能受感染的 EC2 实例中的恶意软件，或者查看是否[AWS Marketplace](#)有有用的合作伙伴产品可以识别和删除恶意软件。

2. 隔离可能遭到入侵的 Amazon EC2 实例

如果可能，请使用以下步骤隔离可能受到威胁的实例：

1. 创建专用的隔离安全组。隔离安全组应仅具有来自特定 IP 地址的入站和出站访问权限。确保没有允许流量的入站或出站规则 `0.0.0.0/0 (0-65535)`。

2. 将隔离安全组与该实例关联。
3. 从可能受到威胁的实例中移除新创建的隔离安全组以外的所有安全组关联。

Note

现有跟踪的连接不会因为更改安全组而终止，只有未来的流量才会被新的安全组有效阻止。

有关已跟踪和未跟踪连接的信息，请参阅《[亚马逊EC2用户指南](#)》中的[亚马逊EC2安全组连接跟踪](#)。

有关阻止来自可疑现有连接的更多流量的信息，请参阅《[事件应手册](#)》中的“[NACLs 基于网络强制 IoCs 以防止更多流量](#)”。

3. 确定可疑活动源

如果检测到恶意软件，则根据您账户中的发现类型，识别并停止您的EC2实例上可能存在的未经授权的活动。这可能需要执行一些操作，例如，关闭任何打开的端口、更改访问策略以及升级应用程序以修复漏洞。

如果您无法识别并阻止可能遭到入侵的EC2实例上的未经授权的活动，我们建议您终止受感染的EC2实例，并根据需要将其替换为新实例。以下是用于保护您的EC2实例的其他资源：

- [Amazon 最佳实践中的“安全和联网”部分 EC2](#)
- [适用于 Linux 实例的亚马逊EC2安全组和适用于 Windows 实例的亚马逊安全组 EC2](#)
- [Amazon 的安全 EC2](#)
- [保护您的EC2实例的提示 \(Linux\)](#)。
- [AWS 安全最佳实践](#)
- [基础设施域事件已开启 AWS](#)

4. 浏览 AWS re:Post

浏览[AWS re:Post](#)以获得更多帮助。

5. 提交技术支持请求

如果您是 Premium Support 服务包的订阅用户，您可以提交[技术支持](#)请求。

修复可能遭到入侵的 S3 存储桶

请按照以下建议步骤修复 AWS 环境中可能遭到入侵的 Amazon S3 存储桶：

1. 确定可能受到威胁的 S3 资源。

S3 的 GuardDuty 调查结果将在查找结果详细信息中列出关联的 S3 存储桶、其 Amazon 资源名称 (ARN) 及其所有者。

2. 确定可疑活动的来源和使用的API呼叫。

使用的API呼叫将按查找结果详细信息API中列出。来源将是IAM委托人 (IAM角色、用户或账户)，识别详细信息将在调查结果中列出。根据源类型，提供远程 IP 地址或源域信息，以便您评估源是否已获得授权。如果发现涉及来自 Amazon EC2 实例的证书，则还将包括该资源的详细信息。

3. 确定调用源是否有权访问已识别的资源。

例如，考虑以下情况：

- 如果涉及IAM用户，他们的凭证是否可能遭到泄露？有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。
- 如果从一个API以前没有调用过这种类型的委托人调用的API，那么这个源是否需要访问权限才能执行此操作？能否进一步限制存储桶权限？
- 如果可以从用户名 ANONYMOUS_PRINCIPAL 和用户类型 AWSAccount 看到访问，则表明存储桶是公有的，并已被访问。这个存储桶应该是公有的吗？如果不是，请查看下面的安全建议，了解共享 S3 资源的替代解决方案。
- 如果访问是成功PreflightRequest调用的，则从用户名ANONYMOUS_PRINCIPAL中看到用户类型为，AWSAccount则表示存储桶设置了跨域资源共享 (CORS) 策略。这个存储桶应该有 CORS政策吗？如果不是，请确保存储桶不会无意中公开，并查看下面的安全建议，了解共享 S3 资源的替代解决方案。有关更多信息，CORS请参阅 S3 用户指南中的[使用跨源资源共享 \(CORS\)](#)。

4. 确定 S3 存储桶是否包含敏感数据。

使用 [Amazon Macie](#) 确定 S3 存储桶是否包含敏感数据，例如个人身份信息 (PII)、财务数据或证书。如果您的 Macie 账户启用了自动敏感数据发现，请查看 S3 存储桶的详细信息，以便更好地了解 S3 存储桶的内容。如果您的 Macie 账户禁用了此功能，我们建议您将其开启以加快评估速度。或者，您可以创建并运行敏感数据发现作业，以检查 S3 存储桶对象中的敏感数据。有关更多信息，请参阅[使用 Macie 发现敏感数据](#)。

如果访问已获授权，则可以忽略调查发现。<https://console.aws.amazon.com/guardduty/>控制台允许您设置规则来完全禁止单个发现，这样它们就不会再出现。有关更多信息，请参阅 [抑制规则](#)。

如果您确定自己的 S3 数据已被未授权方泄露或访问，请查看以下 S3 安全建议，以收紧权限并限制访问权限。适当的修复解决方案取决于特定环境的需求。

基于特定 S3 存储桶访问需求的建议

以下列表根据特定的 Amazon S3 存储桶访问需求提供了建议：

- 为了集中限制公众访问您的 S3 数据的使用，S3 会阻止公共访问。可以通过四种不同的设置为接入点、存储桶和 AWS 账户启用阻止公共访问设置，以控制访问的粒度。有关更多信息，请参阅 [S3 屏蔽公共访问权限设置](#)。
- AWS 访问策略可用于控制 IAM 用户如何访问您的资源或如何访问您的存储桶。有关更多信息，请参阅 [使用存储桶策略和用户策略](#)。

此外，您可以使用具有 S3 存储桶策略的虚拟私有云 (VPC) 终端节点来限制对特定 VPC 端点的访问。有关更多信息，请参阅 [Amazon S3 VPC 终端节点存储桶策略示例](#)

- 要暂时允许账户以外的受信任实体访问您的 S3 对象，您可以创建 URL 通过 S3 进行预签名。此访问权限是使用您的账户凭证创建的，根据使用的凭证，可持续 6 小时到 7 天。有关更多信息，请参阅 [URLs 使用 S3 生成预签名](#)。
- 对于需要在不同源之间共享 S3 对象的用例，您可以使用 S3 接入点创建权限集，这些权限集仅限于私有网络中的对象。有关更多信息，请参阅 [使用 Amazon S3 接入点管理数据访问](#)。
- 要安全地向其他 AWS 账户授予对您的 S3 资源的访问权限，您可以使用访问控制列表 (ACL)，有关更多信息，请参阅 [使用管理 S3 访问权限 ACLs](#)。

有关 S3 安全选项的更多信息，请参阅 [S3 安全最佳实践](#)。

修复可能有恶意的 S3 对象

在中生成 [适用于 S3 查找类型的恶意软件防护](#) 时 AWS 账户，潜在的恶意资源类型是 S3 Object。

使用以下推荐步骤来修复生成的调查结果：

1. 通过检查与发现结果 ObjectDetails 关联的 S3 来识别潜在的恶意的 S3 对象。
2. 隔离受影响的 S3 对象。如果您在为关联的 Amazon S3 存储桶启用 S3 恶意软件防护时启用了标记，GuardDuty 则必须为此对象分配了恶意标签。使用基于标签的访问控制 (TBAC) 来限制对此 S3 对象的访问。有关更多信息，请参阅 [使用基于标签的访问控制 \(\) TBAC](#)。

或者，如果您不再需要此对象，也可以选择将其删除或移至隔离的 S3 存储桶。有关删除 S3 对象的注意事项的信息，请参阅 Amazon S3 用户指南中的 [删除对象](#)。

修复可能受损的集群 ECS

请按照以下建议步骤修复 AWS 环境中可能遭到入侵的 Amazon ECS 集群：

1. 确定可能受到威胁的ECS集群。

用于EC2查找的 GuardDuty 恶意软件防护在查找结果的详细信息面板中ECS提供了ECS集群的详细信息。

2. 评估恶意软件源

评估检测到的恶意软件是否在容器的映像中。如果映像中包含有恶意软件，请识别使用该映像运行的所有其他任务。有关正在运行的任务的信息，请参见[ListTasks](#)。

3. 隔离可能受影响的任務

通过拒绝任务的所有入口和出口流量来隔离受影响的任務。拒绝所有流量规则可以切断与任务的所有连接，从而帮助您阻止已经在进行的攻击。

如果访问已获授权，则可以忽略调查发现。<https://console.aws.amazon.com/guardduty/>控制台允许您设置规则来完全禁止单个发现，这样它们就不会再出现。有关更多信息，请参阅[抑制规则](#)。

修复可能被泄露的凭证 AWS

请按照以下建议步骤修复您的 AWS 环境中可能被泄露的凭证：

1. 识别可能受到威胁的IAM实体和使用的API呼叫。

使用的API呼叫将按查找结果详细信息API中列出。IAM实体（IAM角色或用户）及其标识信息将列在调查结果详细信息的“资源”部分中。所涉及的IAM实体的类型可以通过“用户类型”字段确定，该IAM实体的名称将在“用户名”字段中。调查结果中涉及的IAM实体类型也可以通过使用的访问密钥ID来确定。

对于以 AKIA 开头的密钥：

这种类型的密钥是与IAM用户或关联的长期客户管理的凭证。AWS 账户根用户有关管理IAM用户访问密钥的信息，请参阅[管理IAM用户的访问密钥](#)。

对于以 ASIA 开头的密钥：

此类型的密钥是由 AWS Security Token Service 生成的短期临时凭证。这些密钥仅存在很短的时间，无法在 AWS 管理控制台中查看或管理。IAM 角色将始终使用 AWS STS 证书，但也可以为 IAM 用户生成证书，有关更多信息，AWS STS 请参阅 [IAM：临时安全证书](#)。

如果使用了角色，用户名称字段将指示所用角色的名称。您可以 AWS CloudTrail 通过检查 CloudTrail 日志条目的 sessionIssuer 元素来确定如何请求密钥，有关更多信息，请参阅 [IAM 和中的 AWS STS 信息 CloudTrail](#)。

2. 查看 IAM 实体的权限。

打开控制 IAM 台。根据所用实体的类型，选择“用户”或“角色”选项卡，然后通过搜索字段中键入已识别的名称来找到受影响的实体。使用 Permission (权限) 和 Access Advisor (访问顾问) 选项卡可查看该实体的有效权限。

3. 确定 IAM 实体凭证的使用是否合法。

请与凭证用户联系以确定活动是否是有意进行的。

例如，确定此用户是否执行了以下操作：

- 调用了 GuardDuty 调查结果中列出的 API 操作
- 在 GuardDuty 调查结果中列出的时间调用了该 API 操作
- 从 GuardDuty 调查结果中列出的 IP 地址调用了该 API 操作

如果此活动是对 AWS 凭证的合法使用，则可以忽略该 GuardDuty 发现。<https://console.aws.amazon.com/guardduty/> 控制台允许您设置规则来完全禁止单个发现，这样它们就不会再出现。有关更多信息，请参阅 [抑制规则](#)。

如果您无法确认此活动是否为合法用途，则可能是由于特定访问密钥 (IAM 用户的登录凭证，或者可能是整个 AWS 账户访问密钥) 遭到泄露所致。如果您怀疑自己的凭证已被泄露，请查看 [“我的 AWS 账户可能已被泄露”](#) 文章中的信息以解决此问题。

修复可能受损的独立容器

1. 隔离可能受损的容器

以下步骤将帮助您识别潜在的恶意容器工作负载：

- 打开 GuardDuty 控制台，网址为 <https://console.aws.amazon.com/guardduty/>。

- 在“调查结果”页面上，选择相应的调查结果以查看调查结果面板。
- 在调查发现面板的受影响的资源部分，您可以查看容器的 ID 和名称。

将此容器与其他容器工作负载隔离。

2. 暂停容器

暂停容器中的所有进程。

有关冻结容器的信息，请参阅[暂停容器](#)。

停止容器

如果上述步骤失败，并且容器没有暂停，请停止容器运行。如果您启用了该[快照保留](#)功能，则 GuardDuty 将保留包含恶意软件的 EBS 卷的快照。

有关停止容器的信息，请参阅[停止容器](#)。

3. 评估是否存在恶意软件

评估恶意软件是否在容器的映像中。

如果访问已获授权，则可以忽略调查发现。<https://console.aws.amazon.com/guardduty/>控制台允许您设置规则来完全禁止单个发现，这样它们就不会再出现。GuardDuty 控制台允许您设置规则来完全禁止单个发现，这样它们就不会再出现。有关更多信息，请参阅[抑制规则](#)。

修复 EKS 审计日志监控调查发现

当您的账户启用 EKS 审计日志监控时，Amazon GuardDuty 会生成[发现](#)潜在的 Kubernetes 安全问题。有关更多信息，请参阅[EKS 审计日志监控](#)。以下各节介绍了针对这些场景的建议修复步骤。该特定调查发现类型的条目中描述了具体的修复措施。您可以从[活动调查发现类型](#)表中选择某一调查发现类型，即可获取该类型的完整信息。

如果有任何按预期生成的 EKS 审计日志监控调查发现类型，您可以考虑添加[抑制规则](#)以防止未来发出警报。

不同类型的攻击和配置问题可能会触发 GuardDuty Kubernetes 的发现。本指南可帮助您确定针对您的集群的 GuardDuty 发现的根本原因，并概述了相应的补救指南。以下是导致 GuardDuty Kubernetes 发现的主要根本原因：

- [潜在的配置问题](#)

- [修复可能受到威胁的 Kubernetes 用户](#)
- [修复可能遭到入侵的 Kubernetes 吊舱](#)
- [修复可能受到威胁的 Kubernetes 节点](#)
- [修复可能受损的容器镜像](#)

Note

在 Kubernetes 版本 1.14 之前，该 `system:unauthenticated` 群组与默认关联且处于关联状态。 `system:discovery` `system:basic-user` ClusterRoles 此操作可能允许来自匿名用户的意外访问。 集群更新不会撤销这些权限，这意味着即使您已将集群更新到 1.14 或更高版本，这些权限可能仍然存在。我们建议您取消这些权限与 `system:unauthenticated` 组的关联。

有关移除这些权限的更多信息，请参阅 Amazon EKS 用户指南中的 Amazon E [KS 安全最佳实践](#)。

潜在的配置问题

如果调查发现表明存在配置问题，请参阅调查发现的修复部分，以获取有关解决该问题的指导。有关更多信息，请参阅以下指示配置问题的调查发现类型：

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- 任何以结尾的发现 `SuccessfulAnonymousAccess`

修复可能受到威胁的 Kubernetes 用户

当 GuardDuty 发现中识别的用户执行了意外的 API 操作时，发现可能表明 Kubernetes 用户受到了攻击。您可以在调查发现详细信息的 Kubernetes 用户详细信息部分（位于控制台），或调查发现 JSON 的 `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` 中识别用户。这些用户详细信息包括 `user name`、`uid` 和用户所属的 Kubernetes 组。

如果用户使用 IAM 实体访问工作负载，则可以使用 `Access Key details` 部分来识别 IAM 角色或用户的详细信息。请参阅以下用户类型及其修复指南。

Note

您可以使用 Amazon Detective，以进一步调查调查发现中识别的 IAM 角色或用户。在 GuardDuty 控制台中查看发现的详细信息时，选择“在 Detective 中进行调查”。然后从列出的项目中选择 AWS 用户或角色，在 Detective 中进行调查。

内置 Kubernetes 管理员：Amazon EKS 分配给创建集群的 IAM 身份的默认用户。此用户类型由用户名 `kubernetes-admin` 标识。

要撤销内置 Kubernetes 管理员的访问权限：

- 从 Access Key details 部分中识别 userType。
 - 如果 userType 是角色，并且该角色属于 EC2 实例角色：
 - 识别该实例，然后按照 [修复可能遭到入侵的 Amazon 实例 EC2](#) 中的说明操作。
 - 如果 userType 是用户，或者是用户承担的角色：
 1. [轮换该用户的访问密钥](#)。
 2. 轮换用户有权访问的任何密钥。
 3. 查看“[我的 AWS 账户可能被泄露](#)”中的信息，了解更多详情。

OIDC 验证的用户：通过 OIDC 提供程序授予访问权限的用户。通常，OIDC 用户使用电子邮件地址作为用户名。您可以使用以下命令查看您的集群是否使用 OIDC：`aws eks list-identity-provider-configs --cluster-name your-cluster-name`

要撤销 OIDC 验证的用户的访问权限：

1. 在 OIDC 提供程序中轮换该用户的凭证。
2. 轮换用户有权访问的任何密钥。

AWS-Auth ConfigMap 定义的用户 — 通过 `-auth` 获得访问权限的 IAM 用户。AWSConfigMap 有关更多信息，请参阅 EKS 用户指南中的 [管理集群的用户或 IAM 角色](#)。您可以使用以下命令查看其权限：`kubectl edit configmaps aws-auth --namespace kube-system`

要撤销 AWS ConfigMap 用户的访问权限，请执行以下操作：

1. 使用以下命令打开 ConfigMap。

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. 标识 mapRoles 或 MapUsers 部分下的角色或用户条目，其用户名与调查结果的 Kubernetes 用户详细信息部分中报告的用户名相同。GuardDuty 参见以下示例，示例显示在调查发现中已识别管理员用户。

```

apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
  
```

3. 将该用户从 ConfigMap。参见以下示例，示例显示已识别管理员用户。

```

apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
  
```

4. 如果 userType 是用户，或者是用户承担的角色：
 - a. [轮换该用户的访问密钥](#)。

- b. 轮换用户有权访问的任何密钥。
- c. 查看 [“我的 AWS 账户可能被泄露”](#) 中的信息，了解更多详情。

如果调查发现没有 `resource.accessKeyDetails` 部分，则用户是 Kubernetes 服务账户。

服务账户：服务账户为容器组提供身份，可以通过以下格式的用户名进行识别：

别：`system:serviceaccount:namespace:service_account_name`。

要撤销对服务账户的访问权限：

1. 轮换服务账户凭证。
2. 在以下部分查看有关容器组受攻击的指南。

修复可能遭到入侵的 Kubernetes 吊舱

当在该 `resource.kubernetesDetails.kubernetesWorkloadDetails` 部分中 GuardDuty 指定 pod 或工作负载资源的详细信息时，该 pod 或工作负载资源可能已受到威胁。GuardDuty 发现可能表明单个 Pod 已被入侵，或者多个 Pod 已通过更高级别的资源遭到入侵。有关如何识别已被盗用的一个或多个容器组的指南，请参阅以下盗用场景。

单个容器组盗用

如果 `resource.kubernetesDetails.kubernetesWorkloadDetails` 部分中的 `type` 字段是容器组，则调查发现将识别单个容器组。名称字段是容器组的 `name`，`namespace` 字段是其命名空间。

有关识别运行 Pod 的工作节点的信息，请参阅 [识别违规的 Pod 和工作节点](#)。

容器组通过工作负载资源被盗用

如果 `resource.kubernetesDetails.kubernetesWorkloadDetails` 部分中的 `type` 字段识别工作负载资源（例如 Deployment），则该工作负载资源中的所有容器组很可能都已被盗用。

有关识别工作负载资源的所有 Pod 及其运行的节点的信息，请参阅 [使用工作负载名称识别违规的 Pod 和工作节点](#)。

容器组通过服务账户被盗用

如果调查结果在该 `resource.kubernetesDetails.kubernetesUserDetails` 部分中 GuardDuty 发现了服务帐户，则使用已识别服务帐户的 pod 很可能遭

到入侵。如果调查发现报告的用户名具有以下格式，则该用户名为服务账户：`system:serviceaccount:namespace:service_account_name`。

有关使用服务账号识别所有 Pod 以及它们正在运行的节点的信息，请参阅[使用服务账号名称识别违规的 Pod 和工作节点](#)。

确定所有受感染的 Pod 及其运行的节点后，请参阅[Amazon EKS 最佳实践指南](#)，了解如何隔离 Pod、轮换其证书并收集数据以进行取证分析。

要修复可能受损的 pod，请执行以下操作：

1. 识别攻击容器组的漏洞。
2. 实施针对该漏洞的修复程序并启动新的替换容器组。
3. 删除易受攻击的容器组。

有关更多信息，请参阅[重新部署受感染的 Pod 或工作负载资源](#)。

如果已为工作节点分配了一个允许 Pod 访问其他 AWS 资源的 IAM 角色，请将这些角色从实例中移除，以防止攻击造成进一步损害。同样，如果已为容器组分配了 IAM 角色，请评估您是否可以在不影响其他工作负载的情况下，从该角色安全删除 IAM 策略。

修复可能受损的容器镜像

当 GuardDuty 发现发现有 pod 受损时，用于启动 pod 的图像可能是恶意的或已被泄露的。GuardDuty 调查结果可识

别 `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` 现场内的容器映像。您可以通过扫描恶意软件来确定映像是否是恶意的。

要修复可能受损的容器镜像，请执行以下操作：

1. 立即停止使用该映像，并将其从映像存储库中删除。
2. 使用可能受损的图像识别所有 pod。

有关更多信息，请参阅[识别包含可能存在漏洞或受损容器镜像的 pod 和工作节点](#)。

3. 隔离可能受到威胁的 Pod，轮换凭证，并收集数据进行分析。有关更多信息，请参阅[Amazon EKS 最佳实践指南](#)。
4. 使用可能受损的镜像删除所有 pod。

修复可能受到威胁的 Kubernetes 节点

如果 GuardDuty 发现结果中标识的用户代表节点身份，或者发现结果表明使用了特权容器，则发现可能表示节点受损。

如果用户名字段具有以下格式，则用户身份是 Worker 节点：`system:node:node name`。例如，`system:node:ip-192-168-3-201.ec2.internal`。这表明攻击者已获得对节点的访问权限，并且正在使用节点的凭证与 Kubernetes API 端点进行通信。

如果调查发现中列出的一个或多个容器的

`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext`。调查发现字段设置为 `True`，则调查发现表明使用了特权容器。

要修复可能受损的节点，请执行以下操作：

1. 隔离 Pod，轮换其凭证，并收集数据进行取证分析。

有关更多信息，请参阅 [Amazon EKS 最佳实践指南](#)。

2. 确定在可能遭到入侵的节点上运行的所有 Pod 所使用的服务帐户。查看其权限，并根据需要轮换服务帐户。
3. 终止可能受到威胁的节点。

修复运行时监控结果

当您为账户启用运行时监控时，Amazon GuardDuty 可能会生成[运行时监控查找类型](#)指明您的 AWS 环境中存在潜在安全问题的信息。潜在的安全问题表明您的 AWS 环境中的 Amazon EC2 实例、容器工作负载、Amazon EKS 集群或一组凭证遭到入侵。安全代理监控来自多种资源类型的运行时事件。要识别可能受到威胁的资源，请在 GuardDuty 控制台中生成的查找结果详细信息中查看资源类型。以下部分介绍了针对每种资源类型的建议修复步骤。

Instance

如果调查发现详细信息中的资源类型为 Instance，则表示 EC2 实例或 EKS 节点可能受到攻击。

- 要修复受攻击的 EKS 节点，请参阅 [修复可能受到威胁的 Kubernetes 节点](#)。
- 要修复受攻击的 EC2 实例，请参阅 [修复可能遭到入侵的 Amazon 实例 EC2](#)。

EKSCluster

如果调查发现详细信息中的资源类型为 EKSCluster，则表示 EKS 集群中的容器组或容器可能受到攻击。

- 要修复受攻击的容器组，请参阅 [修复可能遭到入侵的 Kubernetes 吊舱](#)。
- 要修复受攻击的容器映像，请参阅 [修复可能受损的容器镜像](#)。

ECSCluster

如果调查结果详细信息中的资源类型为 ecsCluster，则表示 ECS 任务或 ECS 任务中的容器可能受到威胁。

1. 确定受影响的 ECS 集群

GuardDuty 运行时监控结果在调查结果的详细信息面板或调查结果 JSON 的 `resource.ecsClusterDetails` 部分中提供 ECS 集群的详细信息。

2. 确定受影响的 ECS 任务

GuardDuty 运行时监控结果在查找结果的详细信息面板或调查结果 JSON 的 `resource.ecsClusterDetails.taskDetails` 部分中提供 ECS 任务的详细信息。

3. 隔离受影响的任务

通过拒绝任务的所有入口和出口流量来隔离受影响的任务。拒绝所有流量规则可以切断与任务的所有连接，从而帮助阻止已经开始的攻击。

4. 修复受损的任务

- a. 找出危及任务的漏洞。
- b. 实施该漏洞的修复程序，然后开始新的替换任务。
- c. 停止有漏洞的任务。

Container

如果调查发现详细信息中的资源类型为 Container，则表示独立容器可能受到攻击。

- 要进行修复，请参阅 [修复可能受损的独立容器](#)。
- 如果调查发现是使用同一容器映像跨多个容器生成的，请参阅 [修复可能受损的容器镜像](#)。

- 如果容器访问了底层 EC2 主机，则其关联的实例凭证可能已泄露。有关更多信息，请参阅 [修复可能被泄露的凭证 AWS](#)。
- 如果潜在的恶意行为者访问了底层 EKS 节点或 EC2 实例，请参阅 EKSCluster 和 Instance 选项卡下的修复建议。

修复被盗用的容器映像

当 GuardDuty 发现发现任务受损时，用于启动任务的图像可能是恶意的或已被泄露的。GuardDuty 调查结果可识别 `resource.ecsClusterDetails.taskDetails.containers.image` 现场内的容器映像。您可以通过扫描图像中是否存在恶意软件来确定图像是否为恶意图像。

修复受损的容器镜像

1. 立即停止使用该映像，并将其从映像存储库中删除。
2. 确定使用此图像的所有任务。
3. 停止所有正在使用受损图像的任务。更新他们的任务定义，以便他们停止使用受损的图像。

修复可能受损的数据库

GuardDuty 在您启用 [支持的数据库](#) 后生成的 [RDS 保护查找类型](#)，表明您的登录行为可能存在可疑和异常。[RDS 保护](#) 使用 RDS 登录活动，通过识别登录尝试中的异常模式来 GuardDuty 分析和描述威胁。

Note

您可以从 [调查发现表](#) 中选择某个调查发现类型来访问其完整信息。

请按照以下建议步骤修复您的 AWS 环境中可能遭到入侵的 Amazon Aurora 数据库。

主题

- [通过成功登录事件修复可能受攻击的数据库](#)
- [通过失败登录事件修复可能受攻击的数据库](#)
- [修复可能遭泄露的凭证](#)
- [限制网络访问](#)

通过成功登录事件修复可能受攻击的数据库

以下建议的步骤可以帮助您修复可能受攻击的 Aurora 数据库，该数据库表现出与成功登录事件相关的异常行为。

1. 确定受影响的数据库和用户。

生成的 GuardDuty 结果提供了受影响数据库的名称和相应的用户详细信息。有关更多信息，请参阅[调查发现详细信息](#)。

2. 确认这种行为是预期的还是意外的。

以下列表列出了可能导致生成调查结果 GuardDuty 的潜在场景：

- 经过很长时间后才登录到其数据库的用户。
- 偶尔登录数据库的用户，例如，每个季度登录一次的财务分析师。
- 尝试登录成功的潜在可疑攻击者可能会攻击数据库。

3. 如果行为出乎意料，请开始此步骤。

1. 限制数据库访问

限制可疑账户和登录活动源的数据库访问。有关更多信息，请参阅[修复可能遭泄露的凭证](#)和[限制网络访问](#)。

2. 评测影响并确定访问了哪些信息。

- 请查看审计日志（如果有），以确定可能被访问的信息片段。有关更多信息，请参阅《Amazon Aurora 用户指南》中的[监控 Amazon Aurora 数据库集群中的事件、日志和流](#)。
- 确定是否访问或修改了任何敏感或受保护信息。

通过失败登录事件修复可能受攻击的数据库

以下建议的步骤可以帮助您修复可能受攻击的 Aurora 数据库，该数据库表现出与失败登录事件相关的异常行为。

1. 确定受影响的数据库和用户。

生成的 GuardDuty 结果提供了受影响数据库的名称和相应的用户详细信息。有关更多信息，请参阅[调查发现详细信息](#)。

2. 确定失败登录尝试源。

生成的 GuardDuty 调查结果在调查结果面板的“Actor”部分下提供 IP 地址和 ASN 组织（如果是公共连接）。

自治系统（AS）是由一个或多个网络运营商运行的一个或多个 IP 前缀（可在网络上访问的 IP 地址列表）组成的群组，这些运营商维护单一、明确定义的路由策略。网络运营商需要自治系统号（ASN）来控制其网络中的路由，并与其他互联网服务提供商（ISP）交换路由信息。

3. 确认这种行为是否是意料之外的。

检查此活动是否表示试图获得对数据库的其他未经授权的访问，如下所示：

- 如果源是内部的，请检查应用程序是否配置错误并重复尝试连接。
- 如果是外部攻击者，则检查相应的数据库是否面向公众或配置错误，从而允许潜在的恶意行为者暴力破解常用用户名。

4. 如果行为出乎意料，请开始此步骤。

1. 限制数据库访问

限制可疑账户和登录活动源的数据库访问。有关更多信息，请参阅 [修复可能遭泄露的凭证](#) 和 [限制网络访问](#)。

2. 执行根本原因分析并确定可能导致此活动的步骤。

设置警报，以便在活动修改网络策略并造成不安全状态时收到通知。有关更多信息，请参阅《AWS Network Firewall 开发人员指南》中 [AWS Network Firewall 的防火墙策略](#)。

修复可能遭泄露的凭证

GuardDuty 调查结果可能表明，当调查结果中确定的用户执行了意外的数据库操作时，受影响数据库的用户凭据已被泄露。您可以在控制台的调查发现面板中的 RDS DB 用户详细信息部分或调查发现 JSON 的 `resource.rdsDbUserDetails` 中识别用户。这些用户详细信息包括用户名、使用的应用程序、访问的数据库、SSL 版本和身份验证方法。

- 要对调查发现中涉及的特定用户撤销访问权限或轮换密码，请参阅《Amazon Aurora 用户指南》中的 [Amazon Aurora MySQL 的安全性](#) 或 [Amazon Aurora PostgreSQL 的安全性](#)。
- 用于 AWS Secrets Manager 安全存储和自动轮换 Amazon Relational Database Service (RDS) 数据库的密钥。有关更多信息，请参阅《AWS Secrets Manager 开发人员指南》中的 [AWS Secrets Manager 教程](#)。

- 使用 IAM 数据库身份验证来管理数据库用户的访问权限，无需密码。有关更多信息，请参阅《Amazon Aurora 用户指南》中的 [IAM 数据库身份验证](#)。

有关更多信息，请参阅《Amazon RDS 用户指南》中的 [Amazon Relational Database Service 安全最佳实践](#)。

限制网络访问

GuardDuty 调查结果可能表明，除了您的应用程序或虚拟私有云 (VPC) 之外，还可以访问数据库。如果调查发现中的远程 IP 地址是意外的连接源，请对安全组进行审计。附加到数据库的安全组列表可在 <https://console.aws.amazon.com/rds/> 控制台的安全组下或调查发现 JSON 的 `resource.rdsDbInstanceDetails.dbSecurityGroups` 中找到。有关配置安全组的更多信息，请参阅《Amazon RDS 用户指南》中的 [使用安全组控制访问](#)。

如果使用的是防火墙，请通过重新配置网络访问控制列表 (NACL) 来限制对数据库的网络访问。有关更多信息，请参阅《AWS Network Firewall 开发人员指南》中 [AWS Network Firewall 的防火墙](#)。

修复可能受损的 Lambda 函数

当 GuardDuty 生成 Lambda Protection 调查结果且活动出乎意料时，您的 Lambda 函数可能会受到损害。我们建议完成以下步骤来修复遭到盗用的 Lambda 函数。

修复 Lambda 保护调查发现

1. 确定可能受到威胁的 Lambda 函数版本。

Lambda Protection 的 GuardDuty 调查结果提供了与调查结果详细信息中列出的 Lambda 函数相关的名称、亚马逊资源名称 (ARN)、函数版本和修订版 ID。

2. 确定潜在可疑活动的来源。
 - a. 查看与调查发现中涉及的 Lambda 函数版本相关的代码。
 - b. 查看调查发现中涉及的 Lambda 函数版本的导入库和层。
 - c. 如果您已 [使用 Amazon Inspector 启用扫描 AWS Lambda 功能](#)，请查看与 [调查结果中涉及的 Lambda 函数相关的亚马逊检查结果](#)。
 - d. 查看日 AWS CloudTrail 志，确定导致函数更新的主体，并确保该活动已获得授权或预期。
3. 修复可能受损的 Lambda 函数。

- a. 禁用调查发现中涉及的 Lambda 函数的执行触发器。有关更多信息，请参阅 [DeleteFunctionEventInvokeConfig](#)。
- b. 查看 Lambda 代码并更新库导入和 Lambda [函数层](#)，以移除可能可疑的库和层。
- c. 缓解与调查发现中涉及的 Lambda 函数相关的 Amazon Inspector 调查发现。

估算成本 GuardDuty

在 30 天免费试用期间，您可以使用 GuardDuty 控制台或 API 操作来估算的每日平均使用成本。GuardDuty 成本估算预测试用期结束后的估计成本。但是，要在免费试用期间查看准确的成本估算，GuardDuty 建议使用 AWS Billing <https://console.aws.amazon.com/billing/>。

当您在多账户环境中操作时，GuardDuty 管理员账户可以监控所有成员账户的成本指标。

关于 S3 恶意软件防护使用费用的注意事项

S3 恶意软件防护的使用费用不包含在 GuardDuty 控制台的“使用量”项下。有关更多信息，请参阅 [查看 S3 恶意软件防护的使用情况和费用](#)。

您可以根据以下指标查看成本估算：

- 账户 ID — 列出您的账户的预估费用，如果您以 GuardDuty 管理员账户的身份运营，则列出您的成员账户的预估费用。
- 数据源-列出每个基础数据源（AWS CloudTrail 管理事件、VPC 流日志和 Route53 Resol DNS ver 查询日志）的估计成本。
- 功能-列出功能的估计成本，即 S3 CloudTrail 的数据事件、EKS 审计日志监控、EBS 卷数据、RDS 登录活动、运行时监控、Fargat EKS e 运行时监控、运行时监控或 Lambda 网络活动监控。
GuardDuty EC2
- S3 存储桶：列出指定存储桶上的 S3 数据事件的预计成本，或环境中账户最昂贵的存储桶。只有在为启用 [S3 防护](#) 时，此统计数据才可用 AWS 账户。

了解如何 GuardDuty 计算使用成本

控制台中显示的估计值可能与 GuardDuty 主机中显示的估计值略有不同。AWS Billing and Cost Management 以下列表说明了如何 GuardDuty 估算使用成本：

- 预计的 GuardDuty 使用量仅适用于当前区域。
- GuardDuty 使用费用基于最近 30 天的使用量。
- 试用成本估算包括目前处于试用期的基础数据来源和功能的估算。其中的 GuardDuty 每个功能和数据来源都有自己的试用期，但可能与同时启用的其他功能的 GuardDuty 试用期重叠。

- 预计 GuardDuty 使用 GuardDuty 量包括每个地区的批量定价折扣，详情请参阅 [Amazon P GuardDuty pricing](#) 页面，但仅适用于符合批量定价套餐的个人账户。在组织内账户之间的总使用量估计值中，不包括批量定价折扣。有关组合使用量折扣定价的信息，请参阅 [AWS 账单：批量折扣](#)。
- 组织 AWS 账户 中每种方法的使用成本总和可能并不总是与所选数据源的最近 30 天预估成本相同。随着 GuardDuty 处理更多事件或数据，定价等级可能会发生变化。有关更多信息，请参阅《AWS Billing 用户指南》中的[定价套餐](#)。

此场景解释说，要停止产生运行时监控的使用成本，必须同时禁用运行时监控和EKS运行时监控功能。

GuardDuty 已将EKS运行时监控的控制台体验整合到运行时监控中。GuardDuty 推荐[检查EKS运行时监控配置状态](#)和[从EKS运行时监控迁移到运行时监控](#)。

作为迁移到运行时监控的一部分，请确保[禁用EKS运行时监控](#)。这一点很重要，因为如果您稍后选择禁用“运行时监控”，但未禁用“EKS运行时监控”，则将继续产生EKS运行时监控的使用成本。

运行时监控 — 来自EC2实例的VPC流日志如何影响使用成本

当您在“运行时监控”或“EKS运行时监控”中管理EC2实例的安全代理（手动或通过 GuardDuty），并且GuardDuty 目前部署在 Amazon EC2 实例上并[收集的运行时事件类型](#)从该实例接收时，GuardDuty 不会向您 AWS 账户 收取分析来自此 Amazon EC2 实例的VPC流日志的费用。这有助于 GuardDuty 避免账户中的双重使用成本。

如何 GuardDuty 估算 CloudTrail 活动的使用成本

启用后 GuardDuty，它会自动开始使用所选账户中记录 AWS CloudTrail 的事件日志 AWS 区域。GuardDuty 复制[全球服务事件](#)日志，然后在您已 GuardDuty 启用的每个区域中独立处理这些事件。这有助于 GuardDuty 维护每个区域的用户和角色资料，以识别异常情况。

您的 CloudTrail 配置不会影响 GuardDuty 使用成本或事件日志的 GuardDuty 处理方式。您的 GuardDuty 使用成本受您使用 AWS APIs哪个日志的影响 CloudTrail。有关更多信息，请参阅 [AWS CloudTrail 管理事件](#)。

查看 GuardDuty 使用情况统计信息

选择您的首选访问方式以查看您 GuardDuty账户的使用情况统计信息。如果您是 GuardDuty 管理员帐户，则以下方法将帮助您查看所有成员的使用情况统计信息。

Console

1. 打开 GuardDuty 控制台，网址为<https://console.aws.amazon.com/guardduty/>。
请务必使用 GuardDuty 管理员帐户帐户。
2. 在导航窗格中，选择使用量。
3. 在“使用情况”页面上，拥有成员帐户的 GuardDuty 管理员帐户可以查看过去 30 天的预估组织成本。这是贵组织的估计总使用成本。
4. GuardDuty 拥有成员的管理员帐户可以按数据源或帐户查看使用成本明细。个人或独立帐户可以按数据源查看明细。

如果您有成员账户，则可以通过在账户表中选择该账户来查看该账户的统计信息。

在“按数据源”选项卡下，当您选择与其关联使用成本的数据源时，账户层相应的成本明细总和可能并不总是相同的。

API/CLI

使用 GuardDuty 管理员帐户帐户的凭据运行[GetUsageStatistics](#) API 操作。提供以下信息以运行命令：

- (必填) 提供您要检索其统计数据的账户的区域 GuardDuty 探测器 ID。
- (必需) 提供要检索的统计数据类型之一：SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE。

目前，TOP_ACCOUNTS_BY_FEATURE 不支持检索的使用情况统计信息。RDS_LOGIN_EVENTS

- (必需) 提供一个或多个数据源或功能来查询您的使用情况统计信息。
- (可选) 提供您要检索其使用情况统计信息的账户 IDs 列表。

您也可以使用 AWS Command Line Interface。以下命令是检索按账户计算的所有数据源和功能的使用情况统计信息的示例。务必将 `detector-id` 替换为您自己的有效检测器 ID。对于独立账户，此命令仅返回您的账户在过去 30 天内的使用成本。如果您是拥有成员账户的 GuardDuty 管理员账户，则可以看到按账户列出的所有成员的费用。

要查找与您的账户和当前地区 `detectorId` 对应的，请参阅<https://console.aws.amazon.com/guardduty/> 控制台中的“设置”页面，或者运行[ListDetectors](#) API。

SUM_BY_ACCOUNT 替换为要用来计算使用情况统计数据的数据类型。

仅监控数据源的成本

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
"EC2_MALWARE_SCAN"]}'
```

监控功能成本

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
"EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
"EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Amazon Guardduty 中的安全

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是AWS和您的共同责任。[责任共担模式](#)将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 [AWS 合规性计划](#) 的一部分，第三方审计人员将定期测试和验证安全措施的有效性。要了解适用于 Amazon EMR 的合规性计划，请参阅[按合规性计划提供的范围内 AWS 服务](#)。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用时应用责任共担模式。它说明了如何配置以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 IAM 资源。

目录

- [Amazon 的数据保护 GuardDuty](#)
- [使用记录亚马逊 GuardDuty API 调用 AWS CloudTrail](#)
- [适用于亚马逊的身份和访问管理 GuardDuty](#)
- [Amazon 合规性验证 GuardDuty](#)
- [Amazon GuardDuty 中的恢复能力](#)
- [Amazon 的基础设施安全 GuardDuty](#)

Amazon 的数据保护 GuardDuty

分 AWS [担责任模式](#)适用于亚马逊的数据保护 GuardDuty。如本模型所述 AWS，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私FAQ](#)。有关欧洲数据保护的信息，请参阅[责任AWS 共担模型和AWS安全GDPR](#)博客上的博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭据并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用SSL/TLS与 AWS 资源通信。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或访问时需要 FIPS 140-3 经过验证的加密模块API，请使用端点。FIPS有关可用FIPS端点的更多信息，请参阅[联邦信息处理标准 \(FIPS\) 140-3](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用 GuardDuty 或以其他 AWS 服务方式使用控制台时API、AWS CLI、或 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

静态加密

使用加密解决方案对所有 GuardDuty 客户数据进行静 AWS 态加密。

GuardDuty 使用客户 AWS 拥有的托管密钥使用 AWS Key Management Service (AWS KMS) 对数据（例如调查结果）进行静态加密。

传输中加密

GuardDuty 分析来自其他服务的日志数据。它使用和对从这些服务传输的所有数据HTTPS进行KMS加密。从日志中 GuardDuty 提取所需信息后，这些信息就会被丢弃。有关如何 GuardDuty 使用来自其他服务的信息的更多信息，请参阅[GuardDuty 数据源](#)。

GuardDuty 数据在服务之间传输时会被加密。

选择不使用您的数据来改善服务

您可以使用选择退出政策，AWS Organizations 选择不将您的数据用于开发 GuardDuty 和改进以及其他 AWS 安全服务。即使目前 GuardDuty 未收集任何此类数据，您也可以选择退出。有关如何选择退出的更多信息，请参阅《AWS Organizations 用户指南》中的 [AI 服务选择退出政策](#)。

Note

要使用选择退出政策，您的 AWS 账户必须由集中管理。AWS Organizations 如果您尚未为自己的 AWS 账户创建组织，请参阅《AWS Organizations 用户指南》中的[创建和管理组织](#)。

选择退出会带来以下影响：

- GuardDuty 将在您选择退出（如果有）之前删除其为改善服务而收集和存储的数据。
- 在您选择退出后，GuardDuty 将不再出于服务改进目的收集或存储这些数据。

以下主题说明了其中的每项功能 GuardDuty 可能如何处理您的数据以改进服务。

内容

- [GuardDuty 运行时监控](#)
- [GuardDuty 恶意软件防护](#)

GuardDuty 运行时监控

GuardDuty 运行时监控为您环境中的亚马逊弹性 Kubernetes Service (EKS 亚马逊) 集群 AWS Fargate (Fargate)、仅限亚马逊弹性容器服务 (ECS 亚马逊) 和亚马逊弹性计算云 (EC2 亚马逊) 实例提供运行时威胁检测。AWS 启用 Runtime Monitor GuardDuty 并为资源部署安全代理后，GuardDuty 开始监控和分析与您的资源关联的运行时事件。这些运行时事件类型包括流程事件、容器 DNS 事件、事件等。有关更多信息，请参阅[收集的 GuardDuty 使用运行时事件类型](#)。

尽管 GuardDuty 现在会收集命令行参数，您可以将其定向到您的工作负载，但它目前并未将这些参数用于服务改进目的（将来可能会这样做）。我们已经开始收集命令行参数，以备不久将发布新的威胁检测规则和发现。您的信任、隐私和内容安全是我们的首要任务，并确保我们对数据的使用符合对您的承诺。有关更多信息，请参阅[数据隐私FAQ](#)。

GuardDuty 恶意软件防护

GuardDuty 恶意软件保护会扫描和检测附加到可能受损的 Amazon EC2 实例和容器工作负载的 EBS 卷中包含的恶意软件，以及您选定的 Amazon S3 存储桶中新上传的文件中包含的恶意软件。目前，GuardDuty 不收集或使用检测到的恶意软件来改善服务。但是，将来，当 GuardDuty 恶意软件防护将 EBS 卷文件或 S3 文件识别为恶意文件或有害文件时，GuardDuty 恶意软件防护将收集并存储此文件，以开发和改进其恶意软件检测和 GuardDuty 服务。此文件还可用于开发和改进其他 AWS 安全服

务。您的信任、隐私和内容安全是我们的首要任务，并确保我们对数据的使用符合对您的承诺。有关更多信息，请参阅[数据隐私FAQ](#)。

使用记录亚马逊 GuardDuty API 调用 AWS CloudTrail

GuardDuty Amazon 与AWS CloudTrail一项服务集成，该服务可记录用户、角色或AWS服务在中执行的操作 GuardDuty。CloudTrail 将所有 API 调用捕获 GuardDuty 为事件，包括来自 GuardDuty 控制台的调用和对 GuardDuty API 的代码调用。如果您创建跟踪，则可以允许持续向亚马逊简单存储服务 (Amazon S3) Storage Service 存储桶传送 CloudTrail 事件，包括的事件。GuardDuty如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集到的信息 CloudTrail，您可以确定向哪个请求发出 GuardDuty、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关更多信息 CloudTrail，包括如何配置和启用它，请参阅《[AWS CloudTrail用户指南](#)》。

GuardDuty 信息在 CloudTrail

CloudTrail 在您创建AWS账户时已在您的账户上启用。当支持的事件活动发生在中时 GuardDuty，该活动会与其他AWS服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅[使用事件历史查看 CloudTrail 事件](#)。

要持续记录您AWS账户中的事件，包括的事件 GuardDuty，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service (Amazon S3) 存储桶。此外，您可以配置其他AWS服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅：

- [创建跟踪概览](#)
- [CloudTrail 支持的服务和集成](#)
- [配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)和[接收来自多个账户的 CloudTrail 日志文件](#)

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证发出，还是使用 IAM 用户的登录凭证发出。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其它 AWS 服务发出

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

GuardDuty 控制飞机事件 CloudTrail

默认情况下，将 [Amazon GuardDuty API 参考中提供的所有 GuardDuty API](#) 操作作为事件 CloudTrail 记录在 CloudTrail 文件中。

GuardDuty 中的数据事件 CloudTrail

[GuardDuty 运行时监控](#) 使用部署到您的亚马逊 Elastic Kubernetes Service (Amazon EKS) 集群、亚马逊弹性计算云 (Amazon EC2) 实例 AWS Fargate 和 (仅限亚马逊弹性容器服务 (Amazon ECS)) 任务 GuardDuty 的安全代理来收集针对您的工作负载收集的 aws-guardduty-agent 附加组件 ([收集的运行时事件类型](#))，然后将其发送到 AWS 进行威胁检测和分析。GuardDuty

记录和监控数据事件

您可以选择配置日 AWS CloudTrail 志，以查看 GuardDuty 安全代理的数据事件。

要创建和配置 CloudTrail，请参阅《AWS CloudTrail 用户指南》中的 [数据事件](#)，并按照中有关使用高级事件选择器记录数据事件的说明进行操作。AWS Management Console 记录跟踪时，请确保进行以下更改：

- 对于数据事件类型，选择 GuardDuty 探测器。
- 对于日志选择器模板，请选择记录所有事件。
- 展开 JSON 视图进行配置。应该类似于以下 JSON：

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

```
    }
  ]
}
]
```

启用跟踪选择器后，请导航至 Amazon S3 控制台 <https://console.aws.amazon.com/s3/>。您可以从配置 CloudTrail 日志时选择的 S3 存储桶下载数据事件。

示例：GuardDuty 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示数据平面事件的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
    "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333:aws:ec2-instance",
        "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
        "accountId": "111122223333",
        "userName": "aws:ec2-instance"
      },
      "attributes": {
        "creationDate": "2023-03-05T04:00:21Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "2.0"
    }
  },
  "eventTime": "2023-03-05T06:03:49Z",
```



```

    "eventSource": "guardduty.amazonaws.com",
    "eventName": "SendSecurityTelemetry",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEbbbb",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::GuardDuty::Detector",
      "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
    }
  }
}

```

以下示例显示了演示CreateIPThreatIntelSet操作（控制平面事件）的 CloudTrail 日志条目。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      },
      "sessionIssuer": {

```

```
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "userName": "Alice"
    }
}
},
"eventTime": "2018-06-14T22:57:56Z",
"eventSource": "guardduty.amazonaws.com",
"eventName": "CreateThreatIntelSet",
"awsRegion": "us-west-2",
"sourceIPAddress": "54.240.230.177",
"userAgent": "console.amazonaws.com",
"requestParameters": {
    "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
    "name": "Example",
    "format": "TXT",
    "activate": false,
    "location": "https://s3.amazonaws.com/bucket.name/file.txt"
},
"responseElements": {
    "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
},
"requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
"eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "444455556666"
}
```

通过此事件信息，您可以确定已发出请求，以便在 GuardDuty 中创建威胁列表 Example。您还可以看到，该请求是由名为 Alice 的用户在 2018 年 6 月 14 日发出的。

适用于亚马逊的身份和访问管理 GuardDuty

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 GuardDuty 资源。IAM 无需支付额外费用即可使用。AWS 服务

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [亚马逊是如何 GuardDuty 与之合作的 IAM](#)
- [Amazon 基于身份的政策示例 GuardDuty](#)
- [使用适用于 Amazon 的服务相关角色 GuardDuty](#)
- [AWS Amazon 的托管政策 GuardDuty](#)
- [对 Amazon GuardDuty 身份和访问进行故障排除](#)

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你所做的工作 GuardDuty。

服务用户-如果您使用该 GuardDuty 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多 GuardDuty 功能来完成工作时，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问中的功能 GuardDuty，请参阅[对 Amazon GuardDuty 身份和访问进行故障排除](#)。

服务管理员-如果您负责公司的 GuardDuty 资源，则可能拥有完全访问权限 GuardDuty。您的工作是确定您的服务用户应访问哪些 GuardDuty 功能和资源。然后，您必须向IAM管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM与配合使用 GuardDuty，请参阅[亚马逊是如何 GuardDuty 与之合作的 IAM](#)。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写用于管理访问权限的策略 GuardDuty。要查看可在中使用的 GuardDuty 基于身份的策略示例IAM，请参阅。[Amazon 基于身份的政策示例 GuardDuty](#)

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户、IAM用户身份或通过担任IAM角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。AWS IAM Identity Center（IAM身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用IAM角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的[如何登录到您 AWS 账户的](#)。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅[《IAM用户指南》中的对 AWS API请求进行签名](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的[多重身份验证](#)和AWS IAM Identity Center 用户指南 AWS中的[使用多因素身份验证 \(MFA\)](#)。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的[“需要根用户凭据的IAM任务”](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity Center 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 Ident IAM ity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关IAM身份中心的信息，请参阅[什么是IAM身份中心？](#)在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

[IAM用户](#)是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的[定期轮换需要长期凭证的用例的访问密钥](#)。

[IAM 群组](#)是指定IAM用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并授予该群组管理IAM资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《[IAM 用户指南](#)》中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

[IAM 角色](#)是您内部具有特定权限 AWS 账户 的身份。它与IAM用户类似，但与特定人员无关。您可以通过[切换IAM角色 AWS Management Console 来临时担任中的角色](#)。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《[IAM 用户指南](#)》中的[使用IAM角色](#)。

IAM具有临时证书的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《[IAM 用户指南](#)》中的[为第三方身份提供商创建角色](#)。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅《[AWS IAM Identity Center 用户指南](#)》中的[权限集](#)。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
 - 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。
- 服务角色-服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《[IAM 用户指南](#)》AWS 服务中的[创建角色以向委派权限](#)。

- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 AWS CLI 或 AWS API请求的应用程序的临时证书。这比在EC2实例中存储访问密钥更可取。要为EC2实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在EC2实例上运行的程序获得临时证书。有关更多信息，请参阅IAM用户指南中的[使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用IAM角色还是使用IAM用户，请参阅[《用户指南》中的何时创建IAM角色（而不是IAM用户）](#)。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS，当与身份或资源关联时，它会定义其权限。AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以JSON文档的 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅[《IAM用户指南》中的JSON策略概述](#)。

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 iam:GetRole 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[创建IAM策略](#)。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括

AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的[在托管策略和内联策略之间进行选择](#)。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或AWS服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用AWS托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人 (账户成员、用户或角色) 有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的[访问控制列表 \(ACL\) 概述](#)。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体 (IAM用户或角色) 授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的[IAM实体的权限边界](#)。
- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。对成员账户中的实体 (包括每个实体) 的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的[策略评估逻辑](#)。

亚马逊是如何 GuardDuty 与之合作的 IAM

在使用管理IAM访问权限之前 GuardDuty，请先了解哪些IAM功能可供使用 GuardDuty。

IAM您可以在 Amazon 上使用的功能 GuardDuty

IAM功能	GuardDuty 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	不支持
ABAC (策略中的标签)	部分
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	是

要全面了解大多数IAM功能 GuardDuty 以及其他 AWS 服务是如何使用的，请参阅《IAM用户指南》IAM中[与之配合使用的AWS 服务](#)。

基于身份的策略 GuardDuty

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[创建IAM策略](#)。

使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

基于身份的策略示例 GuardDuty

要查看 GuardDuty 基于身份的策略的示例，请参阅。[Amazon 基于身份的政策示例 GuardDuty](#)

内部基于资源的政策 GuardDuty

支持基于资源的策略：否

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或AWS服务。

要启用跨账户访问权限，您可以将整个账户或另一个账户中的IAM实体指定为基于资源的策略中的委托人。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时AWS账户，可信账户中的IAM管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM用户指南》IAM中的[跨账户资源访问权限](#)。

的政策行动 GuardDuty

支持策略操作：是

管理员可以使用AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 GuardDuty 操作列表，请参阅《服务授权参考》GuardDuty中的 [Amazon 定义的操作](#)。

正在执行的策略操作在操作前 GuardDuty 使用以下前缀：

```
guardduty
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [  
  "guardduty:action1",  
  "guardduty:action2"  
]
```

要查看 GuardDuty 基于身份的策略的示例，请参阅 [Amazon 基于身份的政策示例 GuardDuty 的政策资源 GuardDuty](#)

支持策略资源：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 [Amazon 资源名称 \(ARN\)](#) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 GuardDuty 资源类型及其列表ARNs，请参阅《服务授权参考》GuardDuty中的 [Amazon 定义的资源](#)。要了解您可以为每种资源指定哪些操作，请参阅 [Amazon 定义的操作 GuardDuty](#)。ARN

要查看 GuardDuty 基于身份的策略的示例，请参阅 [Amazon 基于身份的政策示例 GuardDuty](#)

的策略条件密钥 GuardDuty

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素 (或 Condition 块) 中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#) (例如，等于或小于) 的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。有关更多信息，请参阅《IAM用户指南》中的[IAM策略元素：变量和标签](#)。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的[AWS 全局条件上下文密钥](#)。

要查看 GuardDuty 条件密钥列表，请参阅《服务授权参考》GuardDuty中的 [Amazon 条件密钥](#)。要了解您可以使用条件键的操作和资源，请参阅 [Amazon 定义的操作 GuardDuty](#)。

要查看 GuardDuty 基于身份的策略的示例，请参阅。 [Amazon 基于身份的政策示例 GuardDuty](#)

中的访问控制列表 (ACLs) GuardDuty

支持ACLs：否

访问控制列表 (ACLs) 控制哪些委托人 (账户成员、用户或角色) 有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

基于属性的访问控制 () ABAC GuardDuty

支持ABAC (策略中的标签)：部分

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在中 AWS，这些属性称为标签。您可以为IAM实体 (用户或角色) 和许多 AWS 资源附加标签。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关的更多信息ABAC，请参阅[什么是ABAC？](#)在《IAM用户指南》中。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的[使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证与 GuardDuty

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关其他信息，包括哪些 AWS 服务 适用于临时证书 [AWS 服务](#)，请参阅《IAM用户指南》IAM中的“[适用于临时证书](#)”。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM用户指南》中的[切换到角色 \(控制台\)](#)。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅[中的临时安全证书IAM](#)。

的跨服务主体权限 GuardDuty

支持转发访问会话 (FAS)：是

当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。

GuardDuty 的服务角色

支持服务角色：是

服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。

⚠ Warning

更改服务角色的权限可能会中断 GuardDuty 功能。只有在 GuardDuty 提供操作指导时才编辑服务角色。

的服务相关角色 GuardDuty

支持服务相关角色：是

服务相关角色是一种与服务相关联的 AWS 服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的 AWS 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 GuardDuty 服务相关角色的详细信息，请参阅[使用适用于 Amazon 的服务相关角色 GuardDuty](#)。

有关创建或管理服务相关角色的详细信息，请参阅与之[配合 IAM 使用的 AWS 服务](#)。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Amazon 基于身份的政策示例 GuardDuty

默认情况下，用户和角色无权创建或修改 GuardDuty 资源。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或执行任务 AWS API。要授予用户对其所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以将 IAM 策略添加到角色中，用户可以代入角色。

要了解如何使用这些示例策略文档创建 IAM 基于身份的 JSON 策略，请参阅 IAM 用户指南中的[创建 IAM 策略](#)。

有关由 GuardDuty 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》GuardDuty 中的[Amazon 操作、资源和条件密钥](#)。ARNs

主题

- [策略最佳实践](#)
- [使用控制 GuardDuty 台](#)
- [启用 GuardDuty 所需的权限](#)
- [允许用户查看他们自己的权限](#)
- [授予只读访问权限的自定义 IAM 策略 GuardDuty](#)

- [拒绝访问 GuardDuty 调查结果](#)
- [使用自定义IAM策略限制对 GuardDuty 资源的访问权限](#)

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 GuardDuty 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM用户指南》中的[工作职能AWS 托管策略或托管策略](#)。
- 应用最低权限权限-使用IAM策略设置权限时，仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限IAM的更多信息，请参阅《IAM用户指南》IAM[中的策略和权限](#)。
- 使用IAM策略中的条件进一步限制访问权限-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — IAM Access Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAM Access Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的[IAM Access Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的[配置MFA受保护的API访问权限](#)。

有关最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM[中的安全最佳实践](#)。

使用控制 GuardDuty台

要访问 Amazon GuardDuty 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 GuardDuty 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

您无需为仅拨打 AWS CLI 或的用户设置最低控制台权限 AWS API。相反，只允许访问与他们尝试执行的API操作相匹配的操作。

为确保用户和角色仍然可以使用 GuardDuty 控制台，还需要将 GuardDuty ConsoleAccess或ReadOnly AWS 托管策略附加到实体。有关更多信息，请参阅《[用户指南](#)》中的[向IAM用户添加权限](#)。

启用 GuardDuty 所需的权限

要授予各种IAM身份（用户、群组和角色）必须拥有的权限，请附加所需的[AWS 托管策略](#)：[AmazonGuardDutyFullAccess](#)策略以启用 GuardDuty。

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用或以编程方式完成此操作的 AWS CLI 权限。AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    }
  ]
}

```

授予只读访问权限的自定义IAM策略 GuardDuty

要授予只读访问权限，GuardDuty 您可以使用AmazonGuardDutyReadOnlyAccess托管策略。

要创建向IAM角色、用户或组授予只读访问权限的自定义策略 GuardDuty，可以使用以下语句：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:ListMembers",
        "guardduty:GetMembers",
        "guardduty:ListInvitations",
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "guardduty:ListFindings",
        "guardduty:GetFindings",
        "guardduty:ListIPSets",
        "guardduty:GetIPSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetInvitationsCount",
        "guardduty:GetFindingsStatistics",
        "guardduty:DescribeMalwareScans",
        "guardduty:UpdateMalwareScanSettings",
        "guardduty:GetMalwareScanSettings"
      ],
      "Resource": "*"
    }
  ]
}

```

拒绝访问 GuardDuty 调查结果

您可以使用以下策略拒绝IAM角色、用户或群组访问 GuardDuty 调查结果。用户无法查看调查结果或有关调查结果的详细信息，但他们可以访问所有其他 GuardDuty 操作：


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty>DeleteDetector",
        "guardduty:UpdateDetector",
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:CreateIPSet",
        "guardduty>DeleteIPSet",
        "guardduty:UpdateIPSet",
        "guardduty:GetIPSet",
        "guardduty:ListIPSets",
        "guardduty:CreateThreatIntelSet",
        "guardduty>DeleteThreatIntelSet",
        "guardduty:UpdateThreatIntelSet",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:ArchiveFindings",
        "guardduty:UnarchiveFindings",
        "guardduty:CreateSampleFindings",
        "guardduty:CreateMembers",
        "guardduty:InviteMembers",
        "guardduty:GetMembers",
        "guardduty>DeleteMembers",
        "guardduty:DisassociateMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:ListMembers",
        "guardduty:GetMasterAccount",
        "guardduty:DisassociateFromMasterAccount",
        "guardduty:AcceptAdministratorInvitation",
        "guardduty:ListInvitations",
        "guardduty:GetInvitationsCount",
        "guardduty:DeclineInvitations",
        "guardduty>DeleteInvitations"
      ],
      "Resource": "*"
    },
    {
```

```
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "guardduty.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  }
]
```

使用自定义IAM策略限制对 GuardDuty 资源的访问权限

要 GuardDuty 根据检测器 ID 定义用户的访问权限，您可以使用自定义IAM策略中的所有[GuardDutyAPI操作](#)，但以下操作除外：

- guardduty:CreateDetector
- guardduty:DeclineInvitations
- guardduty>DeleteInvitations
- guardduty:GetInvitationsCount
- guardduty>ListDetectors
- guardduty>ListInvitations

在IAM策略中使用以下操作 GuardDuty根据 IPSet ID 和 ThreatIntelSet ID 定义用户的访问权限：

- guardduty>DeleteIPSet
- guardduty>DeleteThreatIntelSet

- guardduty:GetIPSet
- guardduty:GetThreatIntelSet
- guardduty:UpdateIPSet
- guardduty:UpdateThreatIntelSet

以下示例说明如何使用之前的一些操作来创建策略：

- 此策略允许用户在 us-east-1 区域中使用检测器 ID 1234567 运行 guardduty:UpdateDetector 操作：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- 此策略允许用户在 us-east-1 区域中使用探测器 ID 为 1234567 和 000000 的 IPSet ID 来运行 guardduty:UpdateIPSet 操作：

Note

确保用户具有访问中可信 IP 列表和威胁列表所需的权限 GuardDuty。有关更多信息，请参阅 [上传可信 IP 列表和威胁列表所需的权限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
  }
]
}

```

- 此策略允许用户在 us-east-1 区域中使用任何探测器 IPSet ID 和 000000 的 ID 来运行 guardduty:UpdateIPSet 操作：

Note

确保用户具有访问中可信 IP 列表和威胁列表所需的权限 GuardDuty。有关更多信息，请参阅 [上传可信 IP 列表和威胁列表所需的权限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
    }
  ]
}

```

- 此策略允许用户使用其探测器 ID 和 us-east-1 区域中的任何 IPSet ID 运行 guardduty:UpdateIPSet 操作：

Note

确保用户具有访问中可信 IP 列表和威胁列表所需的权限 GuardDuty。有关更多信息，请参阅 [上传可信 IP 列表和威胁列表所需的权限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
    }
  ]
}
```

使用适用于 Amazon 的服务相关角色 GuardDuty

Amazon GuardDuty 使用 AWS Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色 (SLR) 是一种直接关联的独特 IAM 角色类型。GuardDuty 服务相关角色由您预定义 GuardDuty，包括代表您调用其他 AWS 服务 GuardDuty 所需的所有权限。

使用服务相关角色，GuardDuty 无需手动添加必要权限即可进行设置。GuardDuty 定义其服务相关角色的权限，除非另行定义权限，否则 GuardDuty 只能担任该角色。定义的权限包括信任策略和权限策略，并且该权限策略不能附加到任何其他 IAM 实体。

GuardDuty 支持在所有可用的区域中使用服务相关角色。GuardDuty 有关更多信息，请参阅 [区域和端点](#)。

只有在启用 GuardDuty 服务相关角色的所有区域 GuardDuty 中首次禁用该角色后，您才能将其删除。这样可以保护您的 GuardDuty 资源，因为您不会无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅《IAM 用户指南》中 [与之配合使用的 AWS 服务](#)，并在 IAM 在“服务相关角色”列中查找标有“是”的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 GuardDuty

GuardDuty 使用名 `AWSServiceRoleForAmazonGuardDuty` 为的服务相关角色 (SLR)。SLR GuardDuty 允许执行以下任务。它还允许 GuardDuty 将检索到的属于该 EC2 实例的元数据包含在 GuardDuty 可能产生的有关潜在威胁的调查结果中。`AWSServiceRoleForAmazonGuardDuty` 服务相关角色信任 `guardduty.amazonaws.com` 服务来代入角色。

权限策略有助于 GuardDuty 执行以下任务：

- 使用 Amazon EC2 操作管理和检索有关您的 EC2 实例、映像和网络组件（例如 VPCs 子网和传输网关）的信息。
- 当您启用带有亚马逊自动代理的 GuardDuty 运行时监控时，使用 AWS Systems Manager 操作来管理亚马逊 EC2 实例上的 SSM 关联 EC2。禁用 GuardDuty 自动代理配置后，仅 GuardDuty 考虑那些 EC2 带有包含标签 (GuardDutyManaged:true) 的实例。
- 使用 AWS Organizations 操作来描述关联的账户和组织 ID。
- 使用 Amazon S3 操作检索有关 S3 存储桶和对象的信息。
- 使用 AWS Lambda 操作来检索有关您的 Lambda 函数和标签的信息。
- 使用 Amazon EKS 操作管理和检索有关集群的信息，并管理 EKS 集群上的 [Amazon EKS EKS 插件](#)。这些 EKS 操作还会检索与之关联的标签的相关信息 GuardDuty。
- IAM 用于在启用恶意软件防护 [恶意软件防护的服务相关角色权限 EC2](#) 之后创建。EC2
- 使用亚马逊 ECS 操作管理和检索有关亚马逊 ECS 集群的信息，并使用管理亚马逊 ECS 账户设置 guarddutyActivate。与 Amazon 相关的操作 ECS 还会检索与之关联的标签的相关信息 GuardDuty。

该角色使用以下 [AWS 托管策略](#)（名为 AmazonGuardDutyServiceRolePolicy）配置。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GuardDutyGetDescribeListPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",

```

```

        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
    ],
    "Resource": "*"
},
{
    "Sid": "GuardDutyCreateSLRPolicy",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
        }
    }
},
{
    "Sid": "GuardDutyCreateVpcEndpointPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateVpcEndpoint",
    "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyManaged"
        },
        "StringLike": {
            "ec2:VpceServiceName": [
                "com.amazonaws.*.guardduty-data",
                "com.amazonaws.*.guardduty-data-fips"
            ]
        }
    }
}
}

```

```

    },
    {
      "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyVpcEndpoint",
        "ec2>DeleteVpcEndpoints"
      ],
      "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet*"
      ]
    },
    {
      "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "GuardDutyManaged"
        }
      }
    },
    {
      "Sid": "GuardDutySecurityGroupManagementPolicy",

```



```

    "Effect": "Allow",
    "Action": [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "GuardDutyCreateSecurityGroupPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateSecurityGroup",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringLike": {
        "aws:RequestTag/GuardDutyManaged": "*"
      }
    }
  },
  {
    "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateSecurityGroup",
    "Resource": "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateSecurityGroup"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  }
}

```

```
    }
  },
  {
    "Sid": "GuardDutyCreateEksAddonPolicy",
    "Effect": "Allow",
    "Action": "eks:CreateAddon",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyEksAddonManagementPolicy",
    "Effect": "Allow",
    "Action": [
      "eks:DeleteAddon",
      "eks:UpdateAddon",
      "eks:DescribeAddon"
    ],
    "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
  },
  {
    "Sid": "GuardDutyEksClusterTagResourcePolicy",
    "Effect": "Allow",
    "Action": "eks:TagResource",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
    "Effect": "Allow",
    "Action": "ecs:PutAccountSettingDefault",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ecs:account-setting": [
          "guardDutyActivate"
        ]
      }
    }
  }
}
```

```

    }
  }
},
{
  "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeAssociation",
    "ssm>DeleteAssociation",
    "ssm:UpdateAssociation",
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce"
  ],
  "Resource": "arn:aws:ssm:*:*:association/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/GuardDutyManaged": "true"
    }
  }
},
{
  "Sid": "SsmAddTagsToResourcePermission",
  "Effect": "Allow",
  "Action": [
    "ssm:AddTagsToResource"
  ],
  "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "aws:TagKeys": [
        "GuardDutyManaged"
      ]
    },
    "StringEquals": {
      "aws:ResourceTag/GuardDutyManaged": "true"
    }
  }
},
{
  "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
  "Effect": "Allow",
  "Action": [
    "ssm:CreateAssociation",
    "ssm:UpdateAssociation"
  ]
}

```

```

    ],
    "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
  },
  {
    "Sid": "SsmSendCommandPermission",
    "Effect": "Allow",
    "Action": "ssm:SendCommand",
    "Resource": [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    ]
  },
  {
    "Sid": "SsmGetCommandStatus",
    "Effect": "Allow",
    "Action": "ssm:GetCommandInvocation",
    "Resource": "*"
  }
]
}

```

下面是附加到 `AWSServiceRoleForAmazonGuardDuty` 服务相关角色的信任策略：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

有关 `AmazonGuardDutyServiceRolePolicy` 策略更新的详细信息，请参阅 [GuardDuty AWS 托管策略的更新](#)。要获得有关此政策变更的自动提醒，请订阅 [文档历史记录](#) 页面上的 RSS 提要。

为创建服务相关角色 GuardDuty

当您首次启用AWSServiceRoleForAmazonGuardDuty服务相关角色或在以前未启用 GuardDuty 服务的受支持 GuardDuty 地区启用服务相关角色时，系统会自动创建该角色。您也可以使用IAM控制台、AWS CLI、或手动创建服务相关角色。IAM API

Important

为 GuardDuty 委派管理员账户创建的服务相关角色不适用于成员 GuardDuty 账户。

您必须配置权限以允许IAM委托人（例如用户、组或角色）创建、编辑或删除服务相关角色。要成功创建AWSServiceRoleForAmazonGuardDuty服务相关角色，您使用的IAM委托人必须 GuardDuty 具有所需的权限。要授予所需的权限，请将以下策略附加到此用户、组或角色：

Note

更换样本 *account ID* 在以下示例中，使用您的实际 AWS 账户 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  }
]
```

有关手动创建角色的更多信息，请参阅《IAM用户指南》中的[创建服务相关角色](#)。

编辑的服务相关角色 GuardDuty

GuardDuty 不允许您编辑AWSServiceRoleForAmazonGuardDuty服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是，您可以使用编辑角色的描述IAM。有关更多信息，请参阅《IAM用户指南》中的[编辑服务相关角色](#)。

删除的服务相关角色 GuardDuty

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

Important

如果您为启用了恶意软件防护EC2，则删除AWSServiceRoleForAmazonGuardDuty不会自动删除AWSServiceRoleForAmazonGuardDutyMalwareProtection。如果要删除AWSServiceRoleForAmazonGuardDutyMalwareProtection，请参阅[删除恶意软件防护的EC2服务相关角色](#)。

要删除，您必须先 GuardDuty 在所有启用该功能的区域中将其禁用AWSServiceRoleForAmazonGuardDuty。如果您在尝试删除 GuardDuty 服务相关角色时未禁用该服务，则删除将失败。有关更多信息，请参阅[暂停或禁用 GuardDuty](#)。

禁用后 GuardDuty，AWSServiceRoleForAmazonGuardDuty不会自动删除。如果您 GuardDuty 再次启用，它将开始使用现有的AWSServiceRoleForAmazonGuardDuty。

使用手动删除服务相关角色 IAM

使用IAM控制台、AWS CLI、或删除AWSServiceRoleForAmazonGuardDuty服务相关角色。IAM API有关更多信息，请参阅《IAM用户指南》中的[删除服务相关角色](#)。

支持的 AWS 区域

Amazon GuardDuty 支持在所有可用 AWS 区域 的地方 GuardDuty 使用AWSServiceRoleForAmazonGuardDuty服务相关角色。有关当前可用区域的列表，请参阅中的[Amazon GuardDuty 终端节点和配额Amazon Web Services 一般参考](#)。GuardDuty

恶意软件防护的服务相关角色权限 EC2

的恶意软件防护EC2使用名AWSServiceRoleForAmazonGuardDutyMalwareProtection为的服务相关角色 (SLR)。这SLR允许恶意软件防护执行无代理扫描，以检测您 GuardDuty 帐户中的恶意软件。EC2它 GuardDuty 允许在您的帐户中创建EBS卷快照，并与 GuardDuty 服务帐户共享该快照。GuardDuty 评估快照后，它会在恶意软件防护中包含检索到的EC2实例和容器工作负载元数据以供EC2发现。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服务相关角色信任malware-protection.guardduty.amazonaws.com 服务来代入角色。

此角色的权限策略可帮助恶意软件防护执行以下任务：EC2

- 使用亚马逊弹性计算云 (AmazonEC2) 操作来检索有关您的亚马逊EC2实例、卷和快照的信息。的恶意软件防护EC2还提供访问亚马逊EKS和亚马逊ECS集群元数据的权限。
- 为GuardDutyExcluded标签未设置为的EBS卷创建快照true。默认情况下，创建的快照带有GuardDutyScanId 标签。请勿删除此标签，否则恶意软件防护EC2将无法访问快照。

Important

将设置为true，该 GuardDuty服务将无法在将来访问这些快照。GuardDutyExcluded这是因为此服务相关角色中的其他语句会 GuardDuty 阻止对GuardDutyExcluded设置为的快照执行任何操作。true

- 仅当 GuardDutyScanId 标签存在且 GuardDutyExcluded 标签未设置为 true 时，才允许共享和删除快照。

Note

不允许恶意软件防护EC2将快照公开。

- 访问客户托管的密钥 (GuardDutyExcluded标签设置为的密钥除外) true , 通过调用CreateGrant创建和访问与 GuardDuty 服务帐号共享的加密快照中的加密EBS卷。有关每个地区的 GuardDuty 服务帐号列表, 请参阅[GuardDuty 服务账号由 AWS 区域](#)。
- 访问客户的 CloudWatch 日志, 为EC2日志组创建恶意软件防护, 并将恶意软件扫描事件日志放在 /aws/guardduty/malware-scan-events 日志组下。
- 由客户决定是否要在其账户中保留检测到的恶意软件快照。如果扫描检测到恶意软件, 则服务相关角色允许 GuardDuty 向快照添加两个标签-GuardDutyFindingDetected 和GuardDutyExcluded。

Note

GuardDutyFindingDetected 标签指定快照包含恶意软件。

- 确定卷是否使用EBS托管密钥加密。 GuardDuty 执行DescribeKey操作以确定您账户中key IdEBS托管密钥的类型。
- 从您的中获取使用加密的EBS卷的快照 AWS 托管式密钥, AWS 账户 然后将其复制到[GuardDuty 服务账号](#)。为此, 我们使用权限GetSnapshotBlock和ListSnapshotBlocks。 GuardDuty 然后将扫描服务帐号中的快照。目前, EC2支持使用加密的扫描EBS卷的恶意软件防护 AWS 托管式密钥可能并非所有版本都可用 AWS 区域。有关更多信息, 请参阅 [特定于区域的功能可用性](#)。
- 允许 Amaz AWS KMS on EC2 代表恶意软件防护部门呼叫EC2对客户托管的密钥执行多项加密操作。共享使用客户管理密钥加密的快照, 需要执行 kms:ReEncryptTo 和 kms:ReEncryptFrom 等操作。只有那些 GuardDutyExcluded 标签未设置为 true 的密钥才可访问。

该角色使用以下 [AWS 托管策略](#) (名为 AmazonGuardDutyMalwareProtectionServiceRolePolicy) 配置。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DescribeAndListPermissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeVolumes",
      "ec2:DescribeSnapshots",
      "ecs:ListClusters",
      "ecs:ListContainerInstances",
      "ecs:ListTasks",
```



```
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
    ],
    "Resource": "*"
},
{
    "Sid": "CreateSnapshotVolumeConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
        "Null": {
            "aws:ResourceTag/GuardDutyExcluded": "true"
        }
    }
},
{
    "Sid": "CreateSnapshotConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyScanId"
        }
    }
},
{
    "Sid": "CreateTagsPermission",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateSnapshot"
        }
    }
},
{
    "Sid": "AddTagsToSnapshotPermission",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
```

```
        "StringLike": {
            "ec2:ResourceTag/GuardDutyScanId": "*"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyExcluded",
                "GuardDutyFindingDetected"
            ]
        }
    }
},
{
    "Sid": "DeleteAndShareSnapshotPermission",
    "Effect": "Allow",
    "Action": [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GuardDutyScanId": "*"
        },
        "Null": {
            "aws:ResourceTag/GuardDutyExcluded": "true"
        }
    }
},
{
    "Sid": "PreventPublicAccessToSnapshotPermission",
    "Effect": "Deny",
    "Action": [
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
        "StringEquals": {
            "ec2:Add/group": "all"
        }
    }
},
{
    "Sid": "CreateGrantPermission",
    "Effect": "Allow",
```

```

    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/GuardDutyExcluded": "true"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:ebs:id": "snap-*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "Decrypt",
          "CreateGrant",
          "GenerateDataKeyWithoutPlaintext",
          "ReEncryptFrom",
          "ReEncryptTo",
          "RetireGrant",
          "DescribeKey"
        ]
      },
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  },
  {
    "Sid": "ShareSnapshotKMSPermission",
    "Effect": "Allow",
    "Action": [
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "ec2.*.amazonaws.com"
      },
      "Null": {
        "aws:ResourceTag/GuardDutyExcluded": "true"
      }
    }
  },
  {
    "Sid": "DescribeKeyPermission",

```

```

    "Effect": "Allow",
    "Action": "kms:DescribeKey",
    "Resource": "arn:aws:kms:*:*:key/*"
  },
  {
    "Sid": "GuardDutyLogGroupPermission",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogGroups",
      "logs:CreateLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
  },
  {
    "Sid": "GuardDutyLogStreamPermission",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
  },
  {
    "Sid": "EBSDirectAPIPermissions",
    "Effect": "Allow",
    "Action": [
      "ebs:GetSnapshotBlock",
      "ebs:ListSnapshotBlocks"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/GuardDutyScanId": "*"
      },
      "Null": {
        "aws:ResourceTag/GuardDutyExcluded": "true"
      }
    }
  }
]
}

```

以下信任策略附加到 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

为恶意软件防护创建服务相关角色 EC2

当您首次启用恶意软件防护或EC2在以前未启用恶意软件防护EC2的受支持区域启用恶意软件防护时，系统会自动创建 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色。您也可以使用IAM控制台IAMCLI、或手动创

建 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色。IAM API

Note

默认情况下，如果您是 Amazon 的新用户 GuardDuty，EC2则会自动启用恶意软件防护。

Important

为委派 GuardDuty 管理员账户创建的服务相关角色不适用于成员 GuardDuty 账户。

您必须配置权限以允许IAM委托人（例如用户、组或角色）创建、编辑或删除服务相关角色。要成功创建 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色，您使用的IAM身份必须 GuardDuty 具有所需的权限。要授予所需的权限，请将以下策略附加到此用户、组或角色：

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

```

    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
  }
]
}

```

有关手动创建角色的更多信息，请参阅《IAM用户指南》中的[创建服务相关角色](#)。

编辑恶意软件防护的服务相关角色 EC2

的恶意软件防护EC2不允许您编

辑AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色。在创建服务相关

角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是，您可以使用编辑角色的描述IAM。有关更多信息，请参阅《IAM用户指南》中的[编辑服务相关角色](#)。

删除恶意软件防护的服务相关角色 EC2

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

Important

要删除AWSServiceRoleForAmazonGuardDutyMalwareProtection，必须先EC2在所有启用恶意软件防护的区域禁用该保护。

如果您在尝试删除服务相关角色时EC2未禁用恶意软件防护，则删除操作将失败。有关更多信息，请参阅[启用或禁用 GuardDuty启动的恶意软件扫描](#)。

当您选择“禁用”来停止恶意软件防护EC2服

务AWSServiceRoleForAmazonGuardDutyMalwareProtection时，不会自动删除。

如果您随后选择“启用”再次启动恶意软件防护EC2服务，则 GuardDuty 将开始使用现有的AWSServiceRoleForAmazonGuardDutyMalwareProtection。

使用手动删除服务相关角色 IAM

使用IAM控制台 AWS CLI、或删

除AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色。IAM API有关更多信息，请参阅《IAM用户指南》中的[删除服务相关角色](#)。

支持的 AWS 区域

Amazon GuardDuty 支持在所有提供恶意软件防护 AWS 区域 的地方使

用AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色。EC2

有关当前可用区域的列表，请参阅中的[Amazon GuardDuty 终端节点和配额Amazon Web Services 一般参考](#)。GuardDuty

Note

AWS GovCloud (美国东部) 和 AWS GovCloud (美国西部) 的恶意软件防护目前不可用。EC2

AWS Amazon 的托管策略 GuardDuty

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。[创建IAM客户托管策略](#)以仅向您的团队提供他们所需的权限需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅《IAM用户指南》中的[AWS 托管策略](#)。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅《IAM用户指南》中的[工作职能AWS 托管策略](#)。

Version 策略元素指定用于处理策略的语言语法规则。以下策略包括IAM支持的当前版本。有关更多信息，请参阅[IAMJSON策略元素：版本](#)。

AWS 托管策略：AmazonGuardDutyFullAccess

您可以将该AmazonGuardDutyFullAccess策略附加到您的IAM身份。

此策略授予管理权限，允许用户完全访问所有 GuardDuty 操作。

权限详细信息

该策略包含以下权限。

- GuardDuty— 允许用户完全访问所有 GuardDuty操作。
- IAM:
 - 允许用户创建 GuardDuty 服务相关角色。
 - 允许管理员帐户 GuardDuty 为成员帐户启用。
 - 允许用户将角色传递给使用 GuardDuty 此角色以启用 S3 GuardDuty 恶意软件防护功能。无论您如何为 S3 启用恶意软件防护（在 GuardDuty 服务内还是单独启用），这都是如此。
- Organizations— 允许用户为 GuardDuty 组织指定委派管理员和管理成员。

对执行iam:GetRole操作的权限AWSServiceRoleForAmazonGuardDutyMalwareProtection确定了账户中是否EC2存在恶意软件防护的服务相关角色 (SLR)。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AmazonGuardDutyFullAccessSid1",
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Sid": "CreateServiceLinkedRoleSid1",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "guardduty.amazonaws.com",
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "ActionsForOrganizationsSid1",
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IamGetRoleSid1",
    "Effect": "Allow",
```

```
        "Action": "iam:GetRole",
        "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
        "Sid": "AllowPassRoleToMalwareProtectionPlan",
        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::*:role/*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
            }
        }
    }
]
}
```

AWS 托管策略 : AmazonGuardDutyReadOnlyAccess

您可以将该AmazonGuardDutyReadOnlyAccess策略附加到您的IAM身份。

此策略授予只读权限，允许用户查看您 GuardDuty 组织的 GuardDuty 调查结果和详细信息。

权限详细信息

该策略包含以下权限。

- GuardDuty— 允许用户查看 GuardDuty 调查结果并执行以GetList、或开头的API操作Describe。
- Organizations— 允许用户检索有关您的 GuardDuty 组织配置的信息，包括委派管理员帐户的详细信息。

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

```

    "Effect": "Allow",
    "Action": [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
]
}

```

AWS 托管策略：AmazonGuardDutyServiceRolePolicy

你无法附着AmazonGuardDutyServiceRolePolicy在你的IAM实体上。此 AWS 托管策略附加 GuardDuty 到允许代表您执行操作的服务相关角色。有关更多信息，请参阅 [的服务相关角色权限 GuardDuty](#)。

GuardDuty AWS 托管策略的更新

查看 GuardDuty 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅“GuardDuty 文档历史记录”页面上的订阅RSS源。

更改	描述	日期
AmazonGuardDutyServiceRolePolicy – 对现有策略的更新	添加了ec2:DescribeVpcs 权限。这 GuardDuty 允许跟踪VPC更新，例如检索。VPC CIDR	2024年8月22日

更改	描述	日期
<p>AmazonGuardDutyServiceRolePolicy – 更新到现有策略</p>	<p>添加了允许您在启用 S3 恶意软件防护 GuardDuty 时将IAM角色传递给的权限。</p> <pre data-bbox="597 394 1026 1390"> { "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } } </pre>	<p>2024 年 6 月 10 日</p>
<p>AmazonGuardDutyServiceRolePolicy – 对现有策略的更新。</p>	<p>当您启用带有亚马逊自动代理的 GuardDuty 运行时监控时，使用 AWS Systems Manager 操作来管理亚马逊EC2实例上的SSM关联EC2。禁用 GuardDuty 自动代理配置后，仅 GuardDuty 考虑那些EC2带有包含标签 (GuardDutyManaged :true) 的实例。</p>	<p>2024 年 3 月 26 日</p>

更改	描述	日期
AmazonGuardDutyServiceRolePolicy – 对现有策略的更新。	GuardDuty 添加了一项新权限，即检索共享亚马逊VPC账户的组织 ID 并使用组织 ID 设置亚马逊VPC终端节点政策。 <code>organization:DescribeOrganization</code>	2024 年 2 月 9 日
AmazonGuardDutyMalwareProtectionServiceRolePolicy – 对现有策略的更新。	的恶意软件防护EC2增加了两个权限GetSnapshotBlock , ListSnapshots 即在开始恶意软件扫描之前，从您获取EBS卷的快照（使用加密 AWS 托管式密钥）AWS 账户 并将其复制到 GuardDuty 服务帐户。	2024年1月25日
AmazonGuardDutyServiceRolePolicy – 更新到现有策略	添加了新的权限， GuardDuty 允许添加guardduty Activate 亚马逊ECS账户设置，以及在亚马逊ECS集群上执行列出和描述操作。	2023年11月26日
AmazonGuardDutyReadOnlyAccess – 更新到现有策略	GuardDuty 为添加了新策略ListAccounts 。organizations	2023 年 11 月 16 日
AmazonGuardDutyFullAccess – 更新到现有策略	GuardDuty 为添加了新策略ListAccounts 。organizations	2023 年 11 月 16 日
AmazonGuardDutyServiceRolePolicy – 更新到现有策略	GuardDuty 添加了新的权限以支持即将推出的 GuardDuty EKS运行时监控功能。	2023 年 3 月 8 日

更改	描述	日期
AmazonGuardDutyServiceRolePolicy – 更新到现有策略	<p>GuardDuty 添加了新的权限，允许 GuardDuty 为恶意软件防护创建服务相关角色。EC2 这将有助于 GuardDuty 简化启用恶意软件防护的流程 EC2。</p> <p>GuardDuty 现在可以执行以下 IAM 操作：</p> <pre> { "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSManagedServiceName": "malware-protection.guardduty.amazonaws.com" } } } </pre>	2023 年 2 月 21 日
AmazonGuardDutyFullAccess – 更新到现有策略	<p>GuardDuty 已更新 ARN iam:GetRole 为 *AWSManagedServiceRoleForAmazonGuardDutyMalwareProtection。</p>	2022 年 7 月 26 日

更改	描述	日期
AmazonGuardDutyFullAccess – 更新到现有策略	<p>GuardDuty 添加了一个新功能，AWSServiceName 允许使用iam:CreateServiceLinkedRole 服务 GuardDuty 恶意软件防护创建EC2服务相关角色。</p> <p>GuardDuty 现在可以执行iam:GetRole 操作来获取相关信息AWSServiceRole 。</p>	2022 年 7 月 26 日
AmazonGuardDutyServiceRolePolicy – 更新到现有策略	<p>GuardDuty 添加了新的权限，GuardDuty 允许使用 Amazon EC2 联网操作来改善调查结果。</p> <p>GuardDuty 现在可以执行以下 EC2操作来获取有关您的EC2实例如何通信的信息。此信息用于提高调查发现准确性。</p> <ul style="list-style-type: none"> • ec2:DescribeVpcEndpoints • ec2:DescribeSubnets • ec2:DescribeVpcPeeringConnections • ec2:DescribeTransitGatewayAttachments 	2021 年 8 月 3 日
GuardDuty 已开始跟踪更改	GuardDuty 开始跟踪其 AWS 托管策略的更改。	2021 年 8 月 3 日

对 Amazon GuardDuty 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 GuardDuty 时可能遇到的常见问题IAM。

主题

- [我无权在以下位置执行操作 GuardDuty](#)
- [我无权执行 iam:PassRole.](#)
- [我想允许我以外的人 AWS 账户 访问我的 GuardDuty 资源。](#)

我无权在以下位置执行操作 GuardDuty

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当mateojacksonIAM用户尝试使用控制台查看虚构*my-example-widget*资源的详细信息但没有虚构权限时，就会出现以下示例错误。guardduty:*GetWidget*

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 guardduty:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam:PassRole.

如果您收到错误消息，提示您无权执行iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 GuardDuty。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的IAM用户marymajor尝试使用控制台在中执行操作时，会出现以下示例错误 GuardDuty。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```


在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 GuardDuty 资源。

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 GuardDuty 支持这些功能，请参阅[亚马逊是如何 GuardDuty 与之合作的 IAM](#)。
- 要了解如何提供对您拥有的资源的[访问权限](#)，请参阅《IAM用户指南》中的[AWS 账户 向其他IAM用户 提供访问权限](#)。AWS 账户
- 要了解如何向第三方提供对您的资源的[访问权限 AWS 账户](#)，请参阅IAM用户指南中的[向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的[向经过外部身份验证的用户提供访问权限 \(联合身份验证\)](#)。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅《IAM用户指南》[IAM中的跨账户资源访问权限](#)。

Amazon 合规性验证 GuardDuty

要了解是否属于特定合规计划的范围，请参阅AWS 服务“[按合规计划划分的范围](#)”，然后选择您感兴趣的合规计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的“[下载报告](#)”中的“[AWS Artifact](#)”。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#) — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- [在 Amazon Web Services 上进行HIPAA安全与合规架构](#) — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

Note

并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《[HIPAA符合条件的服务参考](#)》。

- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [AWS 客户合规指南](#) — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践，AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)) 的安全控制。
- [使用AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- [AWS Security Hub](#)— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 [Security Hub 控件参考](#)。
- [Amazon GuardDuty](#) — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- [AWS Audit Manager](#)— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Amazon GuardDuty 中的恢复能力

AWS全球基础设施围绕AWS区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 [AWS 全球基础设施](#)。

Amazon 的基础设施安全 GuardDuty

作为一项托管服务，Amazon GuardDuty 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅[AWS 云安全](#)。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的[基础设施保护](#)。

您可以使用 AWS 已发布的API呼叫 GuardDuty 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic C DHE urve Ephemeral Diffie-Hellman)。ECDHE大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与IAM委托人关联的私有访问密钥对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

将 AWS 服务与 GuardDuty

GuardDuty 可以与其他 AWS 安全服务集成。这些服务可以从中提取数据 GuardDuty，使您能够以新的方式查看发现。查看以下集成选项，详细了解该服务的设置方式 GuardDuty。

GuardDuty 与集成 AWS Security Hub

AWS Security Hub 从您的 AWS 账户、服务和支持的第三方合作伙伴产品中收集安全数据，以便根据行业标准和最佳实践评估您环境的安全状态。除了评估您的安全态势外，Security Hub 还为所有集成 AWS 服务和 AWS 合作伙伴产品的调查结果提供了一个中心位置。启用 Security Hub GuardDuty 将自动允许 Security Hub 提取 GuardDuty 发现数据。

有关将 Security Hub 与配合使用的更多信息，GuardDuty 请参阅[与集成 AWS Security Hub](#)。

GuardDuty 与 Amazon Detective 集成

Amazon Detective 使用您 AWS 账户中的日志数据，为您的资源和 IP 地址与您的环境交互创建数据可视化效果。Detective 的可视化功能可帮助您快速轻松地调查安全问题。启用这两项服务后，您可以在 Detective 控制台中从 GuardDuty 查找详细信息转向信息。

有关将 Detective 与配合使用的更多信息，GuardDuty 请参阅[与 Amazon Detective 集成](#)。

与集成 AWS Security Hub

[AWS Security Hub](#) 提供了您在 AWS 中的安全状态的全面视图，可帮助您检查环境是否符合安全行业标准和最佳实践。Security Hub 从 AWS 账户、服务和支持的第三方合作伙伴产品中收集安全数据，并帮助您分析安全趋势并确定优先级最高的安全问题。

亚马逊与 Security Hub 的 GuardDuty 集成使您可以将调查结果从发送 GuardDuty 到 Security Hub。随后，Security Hub 可以在对您的安全状况进行分析时使用这些调查发现。

目录

- [亚马逊如何 GuardDuty 将调查结果发送至 AWS Security Hub](#)
 - [GuardDuty 发送到 Security Hub 的发现类型](#)
 - [发送新发现的延迟](#)

- [Security Hub 不可用时重试](#)
- [更新 Security Hub 中的现有结果](#)
- [在中查看 GuardDuty 调查结果 AWS Security Hub](#)
 - [解释在中 GuardDuty 查找的名字 AWS Security Hub](#)
 - [来自 GuardDuty 的典型结果](#)
- [启用和配置集成](#)
- [在 Security Hub 中使用 GuardDuty 控件](#)
- [停止向 Security Hub 发布调查发现](#)

亚马逊如何 GuardDuty 将调查结果发送至 AWS Security Hub

在中 AWS Security Hub，安全问题作为发现结果进行跟踪。一些发现来自其他 AWS 服务或第三方合作伙伴检测到的问题。Security Hub 还有一套用于检测安全问题和生成结果的规则。

Security Hub 提供了管理来自所有这些来源的结果的工具。您可以查看和筛选结果列表，并查看结果的详细信息。有关更多信息，请参阅 AWS Security Hub 用户指南中的[查看结果](#)。您还可以跟踪调查发现的调查状态。有关更多信息，请参阅 AWS Security Hub 用户指南中[对结果采取行动](#)。

Security Hub 中的所有发现都使用一种称为 AWS 安全调查结果格式 (ASFF) 的标准JSON格式。ASFF 包括有关问题来源、受影响的资源以及发现的当前状态的详细信息。请参阅《AWS Security Hub 用户指南》中的[AWS 安全调查结果格式 \(ASFF\)](#)。

亚马逊 GuardDuty 是向Security Hub发送调查结果的 AWS 服务之一。

GuardDuty 发送到 Security Hub 的发现类型

一旦你启用了 Security Hub，GuardDuty 并且在同一个账户中使用同一个账户 AWS 区域，GuardDuty就会开始将所有生成的结果发送到 Security Hub。这些发现使用安全调查结果格式 (ASFF) [发送到 S AWS securit y Hub](#)。在中ASFF，该Types字段提供了查找结果类型。

发送新发现的延迟

GuardDuty 创建新发现时，通常会在五分钟内将其发送到 Security Hub。

Security Hub 不可用时重试

如果 Security Hub 不可用，则 GuardDuty 会重试发送发现结果，直到收到为止。

更新 Security Hub 中的现有 结果

在向 Security Hub GuardDuty 发送调查结果后，会向 Security Hub 发送更新以反映对发现活动的其他观察结果。根据您的[步骤 5-导出调查结果的频率](#)设置，对这些发现的新观察结果将发送到 Security Hub AWS 账户。

存档或取消存档查找结果时，GuardDuty 不会将该发现发送到 Security Hub。任何手动取消存档但后来变为活动状态的查找结果都不会发送到 GuardDuty Security Hub。

在中查看 GuardDuty 调查结果 AWS Security Hub

要在 Security Hub 中查看您的 GuardDuty 发现，请 GuardDuty 从摘要页面中选择亚马逊下方的查看调查结果。或者，您可以从导航面板中选择 Findings，然后通过选择值为 Product name: 字段来筛选 GuardDuty 结果以仅显示调查结果 **GuardDuty**。

解释在中 GuardDuty 查找的名字 AWS Security Hub

GuardDuty 使用安全调查结果 [格式 \(ASFF\) 将发现结果发送到 S AWS ec urity Hub](#)。在中 ASFF，该 Types 字段提供了查找结果类型。ASFF 类型使用的命名方案与 GuardDuty 类型不同。下表详细列出了所有 GuardDuty 查找类型及其在 Security Hub 中显示的 ASFF 对应类型。

Note

对于某些 GuardDuty 查找类型，Security Hub 会根据 ASFF 查找结果详细信息的资源角色是 ACTOR 还是 TARGET 分配不同的查找名称。有关更多信息，请参阅 [调查发现详细信息](#)。

GuardDuty 查找类型	ASFF 查找类型
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp

GuardDuty 查找类型	ASFF查找类型
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom

GuardDuty 查找类型	ASFF查找类型
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B

GuardDuty 查找类型	ASFF查找类型
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace

GuardDuty 查找类型	ASFF查找类型
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
发现 : IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller

GuardDuty 查找类型	ASFF查找类型
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller

GuardDuty 查找类型	ASFF查找类型
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded

GuardDuty 查找类型	ASFF查找类型
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
影响 : IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation

GuardDuty 查找类型	ASFF查找类型
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputation
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux

GuardDuty 查找类型	ASFF查找类型
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/Pentoolinux	TTPs/PenTest:S3-Pentoolinux
持久性 : IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled

GuardDuty 查找类型	ASFF查找类型
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccess Granted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape

GuardDuty 查找类型	ASFF查找类型
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified

GuardDuty 查找类型	ASFF查找类型
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint

GuardDuty 查找类型	ASFF查找类型
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay

GuardDuty 查找类型	ASFF查找类型
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay

GuardDuty 查找类型	ASFF查找类型
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

来自 GuardDuty 的典型结果

GuardDuty 使用安全调查结果格式 (ASFF) 将发现结果发送到 [Sec AWS urity Hub](#)。

以下是典型发现的示例 GuardDuty。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
```

```
"SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
"ProductFields": {
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
  "Unknown",
  "aws/guardduty/service/archived": "false",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/lat": "42.5122",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4": "199.241.229.197",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/lon": "-90.7384",
  "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port": "46717",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/countryName": "United States",
  "aws/guardduty/service/serviceName": "guardduty",
  "aws/guardduty/service/evidence": "",
  "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4": "172.31.43.6",
  "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/org": "CenturyLink",
  "aws/guardduty/service/action/networkConnectionAction/connectionDirection": "INBOUND",
  "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
  "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
  "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName": "SSH",
  "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/cityName": "Dubuque",
  "aws/guardduty/service/additionalInfo": "",
  "aws/guardduty/service/resourceRole": "TARGET",
  "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
  "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
  "aws/guardduty/service/count": "74",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/asn": "209",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/isp": "CenturyLink",
```

```
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubect1"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

启用和配置集成

要使用与的集成 AWS Security Hub，必须启用 Security Hub。有关如何启用 Security Hub 的信息，请参阅 AWS Security Hub 用户指南中的[设置 Security Hub](#)。

当你同时启用两者 GuardDuty 和 Security Hub 时，集成将自动启用。GuardDuty 立即开始向 Security Hub 发送调查结果。

在 Security Hub 中使用 GuardDuty 控件

AWS Security Hub 使用安全控制来评估您的 AWS 资源，并检查您是否符合安全行业标准和最佳实践。您可以使用与 GuardDuty 资源和选定保护计划相关的控件。有关更多信息，请参阅《AWS Security Hub 用户指南》中的 [Amazon GuardDuty 控件](#)。

有关跨 AWS 服务和资源的所有控件的列表，请参阅《AWS Security Hub 用户指南》中的 [Security Hub 控件参考](#)。

停止向 Security Hub 发布调查发现

要停止向 Security Hub 发送调查结果，你可以使用 Security Hub 控制台或 API。

请参阅《AWS Security Hub 用户指南》中的 [禁用和启用集成（控制台）](#) 中的 [查找结果流或禁用集成（Security Hub API，AWS CLI）](#) 中的查找结果流。

与 Amazon Detective 集成

[Amazon Detective](#) 通过生成数据可视化来帮助您快速分析和调查一个或多个 AWS 账户的安全事件，这些数据可视化表示您的资源随时间推移的行为和交互方式。Detective 创建了 GuardDuty 调查结果的可视化效果。

Detective 会提取所有调查发现类型的详细信息，并提供对实体配置文件的访问权限，以调查与调查发现相关的不同实体。实体可以是 AWS 账户、账户内的 AWS 资源或与您的资源交互的外部 IP 地址。GuardDuty 控制台支持从以下实体转向 Amazon Detective，具体取决于查找类型：IAM 角色 AWS 账户、用户或角色会话、用户代理、联合用户、Amazon EC2 实例或 IP 地址。

目录

- [启用集成](#)
- [从一项发现转向 Amazon Detective GuardDuty](#)
- [使用与 GuardDuty 多账户环境的集成](#)

启用集成

要使用 Amazon Detective，GuardDuty 必须先启用 Amazon Detective。有关如何启用 Detective 的信息，请参阅 [《Amazon Detective 管理指南》](#) 中的设置 Amazon Detective。

当您同时启用 Detective GuardDuty 和 Detective 时，集成会自动启用。启用后，Detective 将立即提取您的 GuardDuty 发现数据。

Note

GuardDuty 根据调查结果的导出频率将 GuardDuty 调查结果发送给 Detective。默认情况下，现有调查发现更新的导出频率为 6 小时。为确保 Detective 收到最新发现的更新，建议您在使用 Detective 的每个区域将导出频率更改为 15 分钟 GuardDuty。有关更多信息，请参阅[步骤 5-设置导出更新的活动发现的频率](#)。

从一项发现转向 Amazon Detective GuardDuty

1. 登录<https://console.aws.amazon.com/guardduty/>控制台。
2. 从您的调查发现表中选择一个调查发现。
3. 从调查发现详细信息窗格中选择使用 Detective 调查。
4. 选择调查发现的某个方面，使用 Amazon Detective 调查。这将为该调查发现或实体打开 Detective 控制台。

如果数据透视的行为不符合预期，请参阅《Amazon Detective 用户指南》中的[数据透视问题排查](#)。


Note

如果您将 GuardDuty 发现存档到 Detective 控制台中，则该发现也会存档在 GuardDuty 控制台中。

使用与 GuardDuty 多账户环境的集成

如果您在中管理多账户环境 GuardDuty，则必须将您的成员账户添加到 Amazon Detective，才能查看这些账户中的发现和实体的侦探数据可视化效果。

建议您使用与 Detective 管理员帐户相同的 GuardDuty 管理员帐户。有关在 Detective 中添加成员账户的更多信息，请参阅[邀请成员账户](#)。

 Note

Detective 是一项区域性服务，这意味着您必须在要使用该集成的每个地区启用 Detective 并添加成员账户。

暂停或禁用 GuardDuty

您可以使用 GuardDuty 控制台暂停或禁用该 GuardDuty 服务。当服务暂停 GuardDuty 时，您不会因为使用而被收取任何费用。

- 必须先取消关联或删除所有成员帐户，然后才能暂停或禁用 GuardDuty。
- 如果您暂停 GuardDuty，它将不再监控您的 AWS 环境安全性或生成新的调查结果。您的现有发现保持不变，不受 GuardDuty 暂停的影响。您可以选择 GuardDuty 稍后重新启用。
- 当您在某个帐户 GuardDuty 中禁用时，将仅对当前选定的帐户禁用该帐户 AWS 区域。如果要完全禁用 GuardDuty，则必须在启用该功能的每个区域将其禁用。
- 如果禁用 GuardDuty，则现有发现和 GuardDuty 配置将丢失且无法恢复。如果要保存现有调查结果，则必须先将其导出，然后再确认禁用 GuardDuty。有关如何导出调查发现的信息，请参阅 [导出调查发现](#)。
- 如果您已为账户中的一个或多个受保护存储桶启用了 S3 恶意软件防护，则暂停或禁用 GuardDuty 不会影响 S3 恶意软件防护下受保护存储桶的状态。即使在暂停或禁用之后 GuardDuty，您的账户仍会产生与 S3 恶意软件防护功能相关的使用费用。有关禁用 S3 恶意软件保护的信息，请参阅 [为受保护的存储桶禁用 S3 的恶意软件防护](#)。

暂停或禁用 GuardDuty

1. 打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择 Settings (设置)。
3. 在“暂停 GuardDuty”部分，选择“暂停” GuardDuty 或“禁用” GuardDuty，然后选择确认您的操作。

暂停 GuardDuty 后重新启用

1. 打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。
2. 在导航窗格中，选择 Settings (设置)。
3. 选择“重新启用 GuardDuty”。

订阅 Amazon 公告 SNS GuardDuty

本节提供有关订阅 Amazon SNS (简单通知服务) 以接收有关新发布的查找类型、现有查找类型更新以及其他功能变更的通知的信息。GuardDuty 通知以 Amazon SNS 支持的所有格式提供。

会向任何订阅的账户 GuardDuty SNS 发送有关 GuardDuty 服务 AWS 更新的公告。要接收有关您账户中调查发现的通知，请参阅 [使用 Amazon CloudWatch Events 创建对 GuardDuty 调查结果的自定义响应](#)。

Note

您的 IAM 用户必须拥有订阅的 `sns::subscribe` 权限 SNS。

您可以在 Amazon SQS 队列中订阅此通知主题 ARN，但必须使用位于同一区域的主题。有关更多信息，请参阅 [亚马逊简单 SQS 队列服务开发者指南中的教程：为亚马逊队列订阅亚马逊 SNS 主题](#)。

您还可以使用 AWS Lambda 函数在收到通知时触发事件。有关更多信息，请参阅亚马逊简单队列服务开发者指南中的 [使用 SNS 亚马逊通知调用 Lambda 函数](#)。

每个区域的 Amazon SNS 主题 ARNs 如下所示。

AWS 区域	亚马逊 SNS 话题 ARN
us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements

AWS 区域	亚马逊SNS话题 ARN
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements

AWS 区域	亚马逊SNS话题 ARN
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements

AWS 区域	亚马逊SNS话题 ARN
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements

AWS 区域	亚马逊SNS话题 ARN
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements

AWS 区域	亚马逊SNS话题 ARN
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

要订阅 GuardDuty 更新通知电子邮件，请访问 AWS Management Console

1. 在 <https://console.aws.amazon.com/sns/v3/> 上打开亚马逊主机。
2. 在区域列表中，选择与ARN要订阅的主题相同的区域。此示例使用us-west-2区域。
3. 在左侧导航窗格中，依次选择订阅和创建订阅。
4. 在“创建订阅”对话框中，在“主题 ARN”中粘贴主题ARN：arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements。
5. 对于协议，选择电子邮件。对于终端节点，请键入您可用于接收通知的电子邮件地址。
6. 选择创建订阅。
7. 在您的电子邮件应用程序中，打开“AWS 通知”中的消息，然后打开链接以确认您的订阅。

您的网络浏览器会显示来自亚马逊的确认回复SNS。

要订阅 GuardDuty 更新通知电子邮件，请使用 AWS CLI

1. 使用 AWS CLI运行以下命令：

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. 在您的电子邮件应用程序中，打开“AWS 通知”中的消息，然后打开链接以确认您的订阅。

您的网络浏览器会显示来自亚马逊的确认回复SNS。

Amazon SNS 消息格式

GuardDuty 一般通知消息示例：

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\": \"1\", \"type\": \"GENERAL\", \"message\": [{\"title\": \"Updated AmazonGuardDutyFullAccess policy\", \"body\": \"Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.\", \"links\": [\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess\"]}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析的 Message 值 (去掉转义引号) 如下所示 :

```
{
  "version": "1",
  "type": "GENERAL",
  "message": [
    {
      "title": "Updated AmazonGuardDutyFullAccess policy",
      "body": "Added permission that allows you to pass an IAM role to
GuardDuty when you enable Malware Protection for S3.",
      "links": [
        "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess"
      ]
    }
  ]
}
```

有关新发现的 GuardDuty 更新通知消息示例如下所示：

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FINDINGS\", \"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\", \"findingDescription\":\"This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance is acting as a client on a Tor network. A common use for a Tor client is to circumvent network monitoring and filter for access to unauthorized or illicit content. Tor clients can also generate nefarious Internet traffic, including attacking SSH servers. This activity can indicate that your EC2 instance is compromised.\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnctPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyr1j1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析的 Message 值 (去掉转义引号) 如下所示：

```
{
  "version": "1",
  "type": "NEW_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "findingDescription": "This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is
```

```
software for enabling anonymous communication. Tor Guards and Authority nodes act as
initial gateways into a Tor network. This traffic can indicate that this EC2 instance
is acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised."
  ]]
}
```

有关 GuardDuty 功能 GuardDuty 更新的更新通知消息示例如下所示：

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FEATURES\", \"featureDetails\": [{\"featureDescription\": \"Customers with high-volumes of global CloudTrail events should see a net positive impact on their GuardDuty costs.\", \"featureLink\": \"https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html#guardduty_controlplane\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhob1sdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyr1j1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

解析的 Message 值 (去掉转义引号) 如下所示：

```
{
  "version": "1",
  "type": "NEW_FEATURES",
  "featureDetails": [{
    "featureDescription": "Customers with high-volumes of global CloudTrail events
should see a net positive impact on their GuardDuty costs.",
```

```

    "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
  ]]
}

```

有关 GuardDuty 更新结果的更新通知消息示例如下所示：

```

{
  "Type": "Notification",
  "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\\\"findingDetails\\\": [{\\\"link\\\": \"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\", \\\"findingType\\\": \"UnauthorizedAccess:EC2/TorClient\",
\\\"description\\\": \"Increased severity value from 5 to 8.\\\"}]}\",
  "Timestamp": "2018-03-09T00:25:43.483Z",
  "SignatureVersion": "1",
  "Signature": "XWox8GDGLRiCgD0X1o/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnctPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}

```

解析的 Message 值 (去掉转义引号) 如下所示：

```

{
  "version": "1",
  "type": "UPDATED_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "description": "Increased severity value from 5 to 8."
  }]
}

```

亚马逊 GuardDuty 配额

您的每个配额 AWS 账户 都有默认配额，以前称为限制 AWS 服务。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看的配额 GuardDuty，请打开 [Service Quotas 控制台](#)。在导航窗格中，选择 AWS 服务并选择 Amazon GuardDuty。

要请求提高限额，请参阅《服务限额用户指南》中的 [请求提高限额](#)。

GuardDuty 每个地区的亚马逊配额如下。AWS 账户

Note

- 有关 EC2 GuardDuty 恶意软件防护的特定配额，请参阅 [EC2 配额恶意软件防护](#)。
- 有关 S3 恶意软件防护的特定配额，请参阅 [S3 恶意软件防护配额](#)。

GuardDuty 每个区域的配额

资源	默认值	注释
探测器	1	您可以为每个区域的每个 AWS 账户创建的最大检测器资源数量。 您不能申请增加配额。
筛选条件	100	每个区域每个 AWS 账户保存的最大筛选条件数量。 您不能申请增加配额。
调查发现保留期	90 天	保留调查发现的最大的天数。

资源	默认值	注释
		您不能申请增加配额。 。
每个可信 IP 列表的 IP 地址和 CIDR 范围	2000	可以包含在单个可信 IP 列表中的 IP 地址和 CIDR 范围的最大数量。 您不能申请增加配额。 。
每个威胁列表的 IP 地址和 CIDR 范围	250,000	可以包含在威胁列表中的 IP 地址和 CIDR 范围的最大数量。 您不能申请增加配额。 。
最大文件大小	35 MB	用于上传可信 IP 列表或威胁列表中包含的 IP 地址和 CIDR 范围列表的文件的最大文件大小 您不能申请增加配额。 。
成员账户 (通过邀请)	5000	与管理员账户账户关联的最大成员账户数量。 您不能申请增加配额。 。

资源	默认值	注释
成员账户	50000	<p>与管理员账户账户关联的成员账户的最大数量 AWS Organizations。这包括通过邀请添加到组织的成员账户。</p> <p>此默认值取决于您当前的成员账户配额 AWS Organizations。通过添加的成员账户数量 AWS Organizations 不能超过组织中的成员账户数量。GuardDuty 有关组织 AWS 账户中数量的信息，请参阅《AWS Organizations 用户指南》中的最大值和最小值。</p>
威胁情报集	6	<p>您可以为每个区域的每个 AWS 账户添加的最大威胁情报集数量。</p> <p>。</p> <p>您不能申请增加配额。</p> <p>。</p>
可信 IP 集	1	<p>每个区域每个 AWS 账户可以上传和激活的最大可信 IP 集数。</p> <p>您不能申请增加配额。</p> <p>。</p>

对亚马逊进行故障排除 GuardDuty

当您收到与执行特定于的操作相关的问题时 GuardDuty，请查阅本节的主题。

主题

- [中的一般问题 GuardDuty](#)
- [EC2 问题的恶意软件防护](#)
- [运行时监控问题](#)
- [管理多个账户问题](#)
- [对其他问题进行故障排除](#)

中的一般问题 GuardDuty

导出 GuardDuty 结果时出现访问错误。我该如何解决这个问题？

配置导出查找结果的设置后，如果 GuardDuty 无法导出调查结果，则会在 GuardDuty 控制台的“设置”页面上显示一条错误消息。当无法再访问目标资源时 GuardDuty，可能会发生这种情况，例如，如果您的 Amazon S3 存储桶已删除或访问存储桶的权限已修改。当 GuardDuty 无法再访问用于加密您的 Amazon S3 存储桶中的数据的密 AWS KMS 钥时，也可能发生这种情况。GuardDuty 当无法导出时，它会向与该账户关联的电子邮件发送通知，以提供有关此问题的信息。

要解决此问题，请确保相应的资源存在并且 GuardDuty 具有访问所需资源的权限。如果您在 90 天的查找结果保留期结束之前没有解决问题 GuardDuty，则您的发现结果将不会被导出。GuardDuty 将禁用在特定区域中查找此账户的导出设置。即使在此保留日期之后，您也可以更新配置设置以重新开始导出特定区域中的调查结果。

有关更多信息，请参阅 [导出调查发现](#)。

EC2 问题的恶意软件防护

我正在启动按需恶意软件扫描，但出现了缺少所需权限错误。

如果您收到错误消息，提示您没有在 Amazon EC2 实例上启动按需恶意软件扫描所需的权限，请确认您已将 [AWS 托管策略：AmazonGuardDutyFullAccess](#) 策略附加到您的 IAM 角色。

如果您是某个 AWS 组织的成员，但仍收到相同的错误，请使用您的管理账号进行连接。有关更多信息，请参阅 [AWS Organizations SCP— 拒绝访问](#)。

我在使用 EC2 恶意软件防护时收到 `iam:GetRole` 错误。

如果您收到此错误 —Unable to get role:

`AWSServiceRoleForAmazonGuardDutyMalwareProtection`，则表示您缺少启用 GuardDuty 启动的恶意软件扫描或使用按需恶意软件扫描的权限。确认您已将 [AWS 托管策略：AmazonGuardDutyFullAccess](#) 策略附加到 IAM 角色。

我是 GuardDuty 管理员帐户，需要启用 GuardDuty 启动的恶意软件扫描，但不使用 AWS 托管策略：`AmazonGuardDutyFullAccess` 进行管理 GuardDuty。

- 将与您一起使用的 IAM 角色配置 GuardDuty 为具有启用 GuardDuty 启动的恶意软件扫描所需的权限。有关所需权限的更多信息，请参阅 [EC2 恶意软件防护创建服务相关角色](#)。
- 将 [AWS 托管策略：AmazonGuardDutyFullAccess](#) 附加到您的 IAM 角色。这将帮助您为成员帐户 GuardDuty 启用启动的恶意软件扫描。

运行时监控问题

我的 AWS Step Functions 工作流程意外失败

如果 GuardDuty 容器是导致工作流程失败的原因，请参阅 [排查覆盖问题](#)。如果问题仍然存在，则为防止工作流程因 GuardDuty 容器而失败，请执行以下步骤之一：

- 将 `GuardDutyManaged:false` 标签添加到关联的 Amazon ECS 集群。
- 在账户级别禁用 AWS Fargate（仅限 ECS）的自动代理配置。将包含标签 `GuardDutyManaged: true` 添加到要继续使用 GuardDuty 自动代理监控的关联的 Amazon ECS 集群中。

对运行时监控中的内存不足错误进行故障排除（仅限 Amazon EC2 支持）

本节根据手动部署 GuardDuty 安全代理提供遇到内存不足错误时的故障排除步骤。 [CPU 和内存限制](#)

如果由于 `out-of-memory` 问题而 `systemd` 终止 GuardDuty 代理，并且您认为向 GuardDuty 代理提供更多内存是合理的，则可以更新限制。

1. 使用 root 权限打开 `/lib/systemd/system/amazon-guardduty-agent.service`。
2. 查找 `MemoryLimit` 和 `MemoryMax`，然后更新这两个值。

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. 更新值后，使用以下命令重新启动 GuardDuty 代理：

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. 运行以下命令以查看状态：

```
sudo systemctl status amazon-guardduty-agent
```

预期的输出将显示新的内存限制：

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

管理多个账户问题

我想管理多个账户，但没有所需的 AWS Organizations 管理权限。

如果您收到此错误-The request failed because you do not have required AWS Organization master permission.，则表示您没有权限为组织中的多个帐户启用 GuardDuty 启动的恶意软件扫描。有关向管理账户提供权限的更多信息，请参阅[建立可信访问权限以启用 GuardDuty 启动的恶意软件扫描](#)。

对其他问题进行故障排除

如果您找不到适合您的问题的场景，请查看以下故障排除选项：

- 有关访问 <https://console.aws.amazon.com/guardduty/> 时的 IAM 一般问题，请参阅 [对 Amazon GuardDuty 身份和访问进行故障排除](#)。
- 有关访问时的身份验证和授权问题 AWS AWS Console Home，请参阅 [IAM 疑难解答](#)。

区域和端点

要查看亚马逊在 AWS 区域哪里可用 GuardDuty，请参阅中的[亚马逊 GuardDuty 终端节点 Amazon Web Services 一般参考](#)。

我们建议您在所有支持 GuardDuty 中启用 AWS 区域。这样 GuardDuty，即使在您未积极使用的区域，也可以生成有关未经授权或异常活动的调查结果。这还 GuardDuty 允许监控受支持者的 AWS CloudTrail 事件 AWS 区域，降低了其检测涉及全球服务的活动的的能力。

特定于区域的功能可用性

区域差异列表，用于指定 GuardDuty 功能的可用性。

ListFindings 和 GetFindingsStatistics API

[GetFindingsStatistics](#)和 [ListFindings](#)API 有一个临时consoleOnly标志。当您使用这些 API 中的任何一个或两个时，该consoleOnly标志表示 API 可以提取结果的最大限制为 1000。

GuardDuty 具有区域差异的功能

[恶意软件防护 EC2](#)

GuardDuty 支持 Dedicated Local Zones 中的 EC2 恶意软件防护功能。AWS

常规 API 支持

由于之前指定的 AWS 区域某些数据源或功能不可用，Amazon GuardDuty API 参考中的以下 API 可能存在地区差异：

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Amazon EC2 调查发现类型：[DefenseEvasion:EC2/UnusualDoHActivity](#) 和 [DefenseEvasion:EC2/UnusualDoTActivity](#)

下表显示了 AWS 区域何处可用 GuardDuty，但尚不支持这两种 Amazon EC2 查找类型。

AWS 区域	区域代码
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
亚太地区 (雅加达)	ap-southeast-3

AWS GovCloud (US) 区域

有关最新信息，请参阅《AWS GovCloud (US) 用户指南》GuardDuty中的 [Amazon](#)。

中国地区

有关最新信息，请参阅[功能可用性和实施差异](#)。

GuardDuty 旧版操作和参数

Amazon GuardDuty 已弃用一些 API 操作和参数，但仍支持它们。最佳实践是使用新的 API 操作和参数来替换旧的选项。下表比较了新版和旧版操作和参数。

旧版操作/参数	新版操作/参数	比较
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	在两个操作中的实现方式相同，Administrator 在 GuardDuty 使用术语 DisassociateFromAdministratorAccount 。
autoEnable DescribeOrganizationConfiguration 和中的参数 UpdateOrganizationConfiguration	autoEnableOrganizationMembers	使用 autoEnableOrganizationMembers，GuardDuty 管理员帐户可以 GuardDuty 对所有成员帐户进行审计并强制执行任一值。使用 API 更新所有成员账户的配置最长可能需要 24 小时。有关该 autoEnableOrganizationMembers 字段可能值的更多信息，请参阅 autoEnableOrganizationMembers
GuardDuty API 2023 年 3 月的变化 中列出的 API 中的 dataSources 参数。	features	从 2023 年 3 月起，您可以使用配置 GuardDuty 恶意软件防护 EC2 和新的 GuardDuty 保护计划 features。2023 年 3 月之前推出的保护计划，包括适用于 EC2 的恶意软件防护，仍然支持使用进行配置 dataSources。如果您使用 API 配置保护计划，则每个 API 请求可以包含 dataSources 或 features，但不能同时包含两者。

Amazon 的文档历史记录 GuardDuty

下表描述了自上次发布 Amazon GuardDuty 用户指南以来对文档所做的重要更改。要获得有关本文档更新的通知，您可以订阅 RSS Feed。

变更	说明	日期
更新了 GuardDuty 服务相关角色 () SLR	GuardDuty 已更新，SLR 将 <code>ec2:Describe:Vpcs</code> 权限包含在 Amazon EC2 操作中。有关更多信息，请参阅的 服务相关角色权限 。 GuardDuty	2024年8月22日
大量新增内容	GuardDuty 为 S3 恶意软件防护功能添加了重要内容更新。 <ul style="list-style-type: none">• 添加了新的示例通知架构示例，用于设置 Amazon EventBridge 规则以接收与恶意软件防护计划资源状态和 S3 对象扫描结果相关的通知。有关更多信息，请参阅使用 Amazon 监控 S3 对象扫描 EventBridge。• 添加了有关排除 S3 对象扫描后标签故障的信息。	2024年8月20日
更新了 GuardDuty 运行时监控中的功能-Amazon EC2	运行时监控发布了适用于亚马逊EC2资源的新代理版本 1.3.0。有关发行说明的更多信息，请参阅 Amazon GuardDuty 安全代理EC2 。	2024年8月19日
更新了 GuardDuty 运行时监控中的功能-Amazon EKS	运行时监控为亚马逊EKS资源发布了新的代理版本 1.7.0。有关发行说明的更多信息，请参	2024年8月17日

	阅 <u>Amazon EKS 集群GuardDuty 安全代理</u> 。	
大量新增内容	GuardDuty 添加了有关恶意软件检测方法及其用于 S3 恶意软件防护和恶意软件防护EC2功能的扫描引擎的新信息。有关更多信息，请参阅 GuardDuty 恶意软件检测扫描引擎 。	2024 年 8 月 15 日
新功能-保护 AI 工作负载	GuardDuty 基础威胁检测和 Lambda Protection 可帮助您更好地保护和检测构建的 AI 工作负载所面临的威胁。AWS有关更多信息，请参阅使用 保护 AI 工作负载 GuardDuty 。	2024年8月14日
更新了“GuardDuty 运行时监控-Fargate”中的功能（仅限亚马逊ECS）	运行时监控发布了适用于 AWS Fargate（ECS仅限亚马逊）资源的新代理版本 1.3.0。有关发行说明的更多信息，请参阅 Fargate-GuardDuty 的安全代理 。ECS	2024 年 8 月 9 日
更新了功能-适用于 S3 的恶意软件防护	GuardDuty S3 恶意软件防护将 S3 存储桶配额的最大数量从 10 增加到 25 个存储桶。此配额适用于 AWS 账户 每人一个 AWS 区域。有关更多信息，请参阅 S3 恶意软件防护 。	2024 年 8 月 8 日

[更新-运行时监控中的新查找类型](#)

GuardDuty 添加了两种新的 Runtime Monitoring 查找类型，它们可以帮助您检测威胁，这些威胁涉及在受监控的资源上创建可疑 shell，以及进程可疑地将其权限提升为 root 权限时权限升级。

2024年8月6日

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[已更新-与集成 AWS Security Hub](#)

AWS Security Hub 提供了 GuardDuty 安全控制措施列表，用于评估您的资源，并检查您是否符合安全行业标准和最佳实践。有关更多信息，请参阅在 [Security Hub 中使用 GuardDuty 控件](#)。

2024年7月11日

[更新了 GuardDuty 测试结果的测试器脚本](#)

GuardDuty 现在支持在专用帐户中使用不同 AWS 资源的 100 多个调查结果使用 [amazon-guardduty-tester](#) 存储库并按照步骤测试发现结果并对其进行审查以了解发现的详细信息。有关更多信息，请参阅 [专用账户中的测试 GuardDuty 结果](#)。

2024年6月28日

[更新了运行时监控中的功能](#)

运行时监控为亚马逊EC2资源发布了新的安全代理版本1.2.0。有关发行说明的信息，请参阅 [Amazon EC2 实例 GuardDuty 安全代理](#)。有关手动将安全代理更新到此版本的信息，请参阅 [手动管理 Amazon EC2 实例的安全代理](#)。

2024 年 6 月 13 日

[新功能-适用于 S3 区域的恶意软件防护](#)

GuardDuty S3 恶意软件防护现已在所有可用的商业区域 GuardDuty 推出。此功能可帮助您扫描新上传到 Amazon S3 存储桶中的对象，以查找潜在的恶意软件和可疑上传，并在它们被摄入下游进程之前采取措施将其隔离。有关为 S3 启用恶意软件防护的信息，请参阅 [适用于 S3 的 GuardDuty 恶意软件防护](#)。

2024 年 6 月 12 日

[新功能-适用于 S3 的恶意软件防护](#)

2024 年 6 月 11 日

GuardDuty 宣布正式推出适用于 S3 的恶意软件防护，它可以帮助您扫描新上传到 Amazon S3 存储桶中的对象，以查找潜在的恶意软件和可疑上传，并在它们被摄入下游进程之前采取措施对其进行隔离。此功能完全由管理 AWS。GuardDuty 将 S3 对象扫描结果发布到您的 EventBridge 默认事件总线。您可以允许 GuardDuty 向扫描的 S3 对象添加标签。您可以构建下游工作流程，例如隔离到隔离存储桶，也可以使用标签定义存储桶策略，以防止用户或应用程序访问某些对象。有关更多信息，请参阅 [S3 GuardDuty 恶意软件防护](#)。目前，它已在以下地区推出：

- 美国东部 (弗吉尼亚州北部)
- 美国东部 (俄亥俄州)
- 美国西部 (俄勒冈州)
- 欧洲地区 (爱尔兰)
- 欧洲地区 (法兰克福)
- 欧洲地区 (斯德哥尔摩)
- 亚太地区 (悉尼)
- 亚太地区 (东京)
- 亚太地区 (新加坡)

[更新了AmazonGuardDuty FullAccess政策](#)

添加了允许您在启用 S3 恶意软件防护 GuardDuty 时将IAM角色传递给的权限。有关此策略更新的更多信息，请参阅[AWS 托管策略GuardDuty 更新](#)。

2024 年 6 月 10 日

[更新了“GuardDuty RDS保护”中的功能](#)

RDS保护扩展了对监视您的 For Postgre SQL 数据库RDS的登录活动的支持。作为此扩展的一部分，GuardDuty 将自动开始监视已启用 GuardDuty RDS保护的帐户RDS的 Postgre SQL 数据库的登录数据。有关更多信息，请参阅[RDS保护](#)。

2024 年 6 月 6 日

[更新了“GuardDuty 运行时监控-Fargate”中的功能（仅限亚马逊ECS）](#)

运行时监控发布了适用于 AWS Fargate（ECS仅限亚马逊）资源的新代理版本 1.2.0。有关发行说明的更多信息，请参阅[Fargate-GuardDuty 的安全代理](#)。ECS

2024年5月31日

[更新了 GuardDuty 恶意软件防护中的功能 EC2](#)

对于连接到您的亚马逊EC2实例和容器工作负载的每个 Amazon EBS 卷，GuardDuty 恶意软件防护EC2已将其扫描的EBS卷大小增加到 2048 GB。有关扫描挂载到您的实例的 Amazon EBS 卷的信息，请参阅[GuardDuty 恶意软件防护 EC2](#)。

2024 年 5 月 29 日

[更新了运行时监控中的功能](#)

Amazon ECS-Fargate 资源的运行时监控现在支持检测和启动的任务中存在的 AWS Batch 潜在威胁。AWS CodePipeline 有关更多信息，请参阅[运行时监控如何与 Fargate 配合使用 \(ECS 仅限亚马逊\)](#)。

2024 年 5 月 28 日

[更新了运行时监控中的功能](#)

运行时监控发布了适用于亚马逊 EKS 资源的新代理版本 1.6.1。有关发行说明的信息，请参阅[EKS 插件代理发布历史记录](#)。

2024 年 5 月 14 日

[扩展了对运行时监控的区域支持](#)

GuardDuty 将对运行时监控的支持扩展到加拿大西部 (卡尔加里) 区域。有关开始使用运行时监控的信息，请参阅[启用运行时监控](#)。

2024 年 5 月 7 日

[扩展了对 RDS 保护的区域支持](#)

GuardDuty 将 RDS 保护支持扩展到以下内容 AWS 区域：

2024 年 5 月 3 日

- 加拿大西部 (卡尔加里)
- 亚太地区 (海得拉巴)
- 欧洲 (西班牙)
- 欧洲 (苏黎世)
- 中东 (UAE)
- 以色列 (特拉维夫)
- 亚太地区 (墨尔本)

有关启用此功能的信息，请参阅[RDS 保护](#)。

更新了运行时监控中的功能	运行时监控发布了适用于 AWS Fargate (ECS 仅限亚马逊) 资源的新代理版本 1.1.0。有关发行说明的更多信息, 请参阅 Fargate-GuardDuty 的安全代理 。ECS	2024 年 5 月 1 日
更新了运行时监控中的功能	运行时监控为亚马逊 EKS 资源发布了新的代理版本 1.6.0。有关发行说明的信息, 请参阅 EKS 插件代理发布历史记录 。	2024 年 4 月 29 日
Support IPAddressv6	GuardDuty 增加了对本地和远程 IP 详细信息的 IPAddressv6 支持。您可以使用关联的“ 筛选器 ”属性来筛选 GuardDuty 结果或 创建抑制规则 。	2024 年 4 月 18 日
更新了控制台体验以配置导出结果	GuardDuty 已更新控制台体验, 将您在 AWS 账户中生成的调查结果导出到 Amazon S3 存储桶。有关更多信息, 请参阅 导出 GuardDuty 调查结果 。	2024 年 4 月 1 日
更新了运行时监控中的功能	运行时监控为亚马逊 EC2 资源发布了新的安全代理版本 1.1.0。此版本支持在 Amazon EC2 实例的运行时监控中 GuardDuty 自动配置代理。有关发行说明的信息, 请参阅 Amazon EC2 实例 GuardDuty 安全代理 。	2024 年 3 月 28 日

[Amazon EC2 实例运行时监控正式上线](#)

GuardDuty 宣布亚马逊EC2实例运行时监控正式上线 (GA)。现在，您可以选择[启用自动代理配置](#)，GuardDuty 允许代表您安装和管理您的 Amazon EC2 实例的安全代理。借助 GuardDuty 自动代理，您还可以使用包含或排除标签通知 GuardDuty 仅在选定的 Amazon EC2 实例上安装和管理安全代理。有关更多信息，请参阅[运行时监控如何与 Amazon EC2 实例配合使用](#)。

2024 年 3 月 28 日

与此 GA 一起发布的新发现类型列表

- [执行：运行时/ SuspiciousTool](#)
- [执行：运行时/ SuspiciousCommand](#)
- [DefenseEvasion:运行时/ SuspiciousCommand](#)
- [DefenseEvasion:运行时/ PtraceAntiDebugging](#)
- [执行：运行时/ MaliciousFileExecuted](#)

[Amazon GuardDuty 已更新服务相关角色 \(\) SLR](#)

2024 年 3 月 26 日

当您启用带有亚马逊自动代理的 GuardDuty 运行时监控时，使用 AWS Systems Manager 操作来管理亚马逊 EC2 实例上的 SSM 关联 EC2。禁用 GuardDuty 自动代理配置后，仅 GuardDuty 考虑那些 EC2 带有包含标签 (GuardDuty Managed :true) 的实例。

- 以下列表显示了新的权限：

```
"ssm:DescribeAssociation",
"ssm:DeleteAssociation",
"ssm:UpdateAssociation",
"ssm:CreateAssociation",
"ssm:StartAssociationsOnce",
"ssm:AddTagsToResource",
"ssm:CreateAssociation",
"ssm:UpdateAssociation",
"ssm:SendCommand",
"ssm:GetCommandInvocation"
```


更新了运行时监控中的功能	在 Amazon 的最新 GuardDuty 安全代理 (附加组件) v1.5.0 版本中 EKS，运行时监控现在支持配置 GuardDuty 安全代理的特定参数，例如 CPU 内存设置、PriorityClass 设置和 DNS 策略设置。有关更多信息，请参阅 配置 GuardDuty 安全代理 (EKS 附加组件) 参数 。	2024 年 3 月 7 日
更新了运行时监控中的功能	运行时监控发布了 Amazon EKS 资源的新代理版本 1.5.0。有关发行说明的信息，请参阅 EKS 插件代理发布历史记录 。	2024 年 3 月 7 日
支持加拿大西部 (卡尔加里)	Amazon GuardDuty 现已在加拿大西部 (卡尔加里) 地区上市。其中的某些保护计划 GuardDuty 可能无法在该地区使用。有关最新信息，请参阅 区域和终端节点 。	2024 年 3 月 6 日
更新了运行时监控中的功能	从 2024 年 5 月 14 日起，将不再支持适用于亚马逊 EKS 集群 GuardDuty 的安全代理版本 1.0.0 和 1.1.0。有关在标准支持终止之前可以采取哪些步骤的信息，请参阅 Amazon EKS 集群 GuardDuty 安全代理 。	2024 年 2 月 16 日

[更新了运行时监控中的功能](#)

运行时监控支持最新的 [Kubernetes 版本 1.29](#) 和现有的安全代理版本 1.4.1。自此 Kubernetes 版本发布以来，该支持一直可用。有关支持的 Kubernetes 版本的信息，请参阅安全代理支持的 [Kubernetes](#) 版本。GuardDuty

2024 年 2 月 16 日

[更新了运行时监控中的功能-区域可用性](#)

GuardDuty 运行时监控现在支持同一个共享的 VPC Amazon AWS Organizations。 [GuardDuty 服务相关角色 \(SLR\)](#) 具有新权限 `organizations:DescribeOrganization`，可帮助检索共享亚马逊 VPC 账户的组织 ID 以设置终端节点策略。有关在运行时监控中使用共享亚马逊 VPC 终端节点的先决条件的信息，请参阅 [对共享亚马逊的支持 VPC](#)。此功能适用于所有 GuardDuty 支持运行时监控的区域。

2024 年 2 月 12 日

[更新了运行时监控中的功能-区域可用性](#)

GuardDuty 运行时监控现在支持同一个共享的 VPC Amazon AWS Organizations。 [GuardDuty 服务相关角色 \(SLR\)](#) 具有新权限 `organizations:DescribeOrganization`，可帮助检索共享亚马逊 VPC 账户的组织 ID 以设置终端节点策略。有关在运行时监控中使用共享亚马逊 VPC 终端节点的先决条件的信息，请参阅 [对共享亚马逊的支持 VPC](#)。目前，此功能在某些版本中可用 AWS 区域。有关更多信息，请参阅 [区域和端点](#)。

2024 年 2 月 9 日

[更新了功能，支持新功能 AWS 区域 — 恶意软件防护 EC2](#)

恶意软件防护 EC2 目前支持扫描美国西部（俄勒冈）AWS 托管式密钥 地区使用加密的 EBS 卷。

2024 年 2 月 6 日

[更新了功能，支持新功能 AWS 区域 — 恶意软件防护 EC2](#)

恶意软件防护EC2目前支持扫描[以下内容](#) [AWS 托管式密钥中使用加密的EBS卷](#) [AWS 区域](#)：

2024年2月5日

- 亚太地区 (新加坡) (ap-southeast-1)
- 欧洲地区 (法兰克福) (eu-central-1)
- 亚太地区 (大阪) (ap-northeast-3)
- 美国东部 (俄亥俄州) (us-east-2)
- 欧洲 (米兰) (eu-south-1)
- 亚太地区 (东京) (ap-northeast-1)
- 亚太地区 (首尔) (ap-northeast-2)
- 加拿大 (中部) (ca-central-1)
- 欧洲地区 (爱尔兰) (eu-west-1)
- 美国东部 (弗吉尼亚州北部) (us-east-1)

[更新了运行时监控中的功能](#)

GuardDuty 运行时监控发布了适用于亚马逊 GuardDuty EC2实例的新安全代理版本 (v1.0.2)。此代理版本包括对最新 Amazon 的支持ECSAMIs。有关代理发布历史的更多信息，请参阅 [Amazon EC2 实例 GuardDuty 的安全代理](#)。

2024 年 2 月 2 日

[更新了功能，支持新功能 AWS 区域 — 恶意软件防护 EC2](#)

恶意软件防护 EC2 目前支持扫描以下加密的 A AWS 托管式密钥 [amazon EBS 卷 AWS 区域](#)：

2024 年 1 月 31 日

- 欧洲 (伦敦) (eu-west-2)
- 欧洲 (斯德哥尔摩) (eu-north-1)
- 亚太地区 (香港) (ap-east-1)
- 非洲 (开普敦) (af-south-1)
- 中东 (巴林) (me-south-1)
- 亚太地区 (海得拉巴) (ap-south-2)
- 欧洲 (西班牙) (eu-south-2)
- 亚太地区 (墨尔本) (ap-southeast-4)
- 亚太地区 (悉尼) (ap-southeast-2)
- 以色列 (特拉维夫) (il-central-1)

[更新了使用管理账户 AWS Organizations](#)

在“使用[管理账户](#)”下重新整理了 [AWS Organizations](#) 内容。 ，添加了更改委派 GuardDuty 管理员账户的步骤，并更新了[了解 GuardDuty 管理员账户和成员账户之间的关系](#)。

2024 年 1 月 30 日

[更新了功能，支持新功能 AWS 区域](#)

恶意软件防护EC2目前支持扫描[以下内容](#) [AWS 托管式密钥中使用加密的EBS卷](#) [AWS 区域](#)：

2024 年 1 月 29 日

- 亚太地区（雅加达）（ap-southeast-3）
- 美国西部（加利福尼亚北部）（us-west-1）
- 中东 (UAE) (me-central-1)
- 欧洲（苏黎世）（eu-central-2）
- 亚太地区（孟买）（ap-south-1）
- 南美洲（圣保罗）（sa-east-1）

[更新了恶意软件防护中的功能 EC2](#)

恶意软件防护EC2现在支持扫描使用加密的EBS卷 [AWS 托管式密钥](#)。[EC2服务相关角色的恶意软件防护 \(SLR\)](#) 有两个新权限——GetSnapshotBlock 和 ListSnapshotBlocks 在开始恶意软件扫描之前，这些权限将有助于从您 AWS 账户 那里 GuardDuty 获取EBS卷的快照（使用加密 AWS 托管式密钥）并将其复制到[GuardDuty 服务帐户](#)。目前，此功能仅在欧洲（巴黎）（eu-west-3）可用。有关更多信息，请参[阅支持的恶意软件扫描卷](#)。

2024 年 1 月 25 日

更新了运行时监控中的功能	GuardDuty Runtime Monitoring 发布了新的 GuardDuty 安全代理版本 (v1.0.1)，其中包含常规性能调整和增强功能。有关代理发布历史的更多信息，请参阅 Amazon EC2 实例 GuardDuty 的安全代理 。	2024 年 1 月 23 日
更新了运行时监控中的功能	运行时监控发布了适用于亚马逊EKS资源的新代理版本 1.4.1。有关更多信息，请参阅 EKS插件代理发布历史记录 。	2024 年 1 月 16 日
运行时监控发布了适用于亚马逊资源的新代理 v1.4.0 EKS	运行时监控发布了适用于亚马逊EKS资源的新代理版本 1.4.0。有关更多信息，请参阅 EKS插件代理发布历史记录 。	2023 年 12 月 21 日

[在欧洲（苏黎世）、欧洲（西班牙）、亚太地区（海得拉巴）、亚太地区（墨尔本）和以色列（特拉维夫）中添加了基于 S3 和 AWS CloudTrail 机器学习 \(ML\) 的结果类型](#)

以下 S3 和使用异常检测机器学习 (ML) 模型识别异常行为的 CloudTrail 发现现已在欧洲（苏黎世）、欧洲（西班牙）、亚太地区（海得拉巴）、亚太地区（墨尔本）和以色列（特拉维夫）地区推出：GuardDuty

2023 年 12 月 21 日

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)

- [Discovery:IAMUser/
AnomalousBehavior](#)

[GuardDuty 通过以下方式支持 50,000 个会员账户 AWS Organizations](#)

委托 GuardDuty 管理员现在可以通过管理最多 50,000 个成员账户 AWS Organizations。这还包括最多 5000 个通过邀请与 GuardDuty 管理员账户关联的成员账户。

2023 年 12 月 20 日

[GuardDuty 运行时监控支持扩展到 19 AWS 区域](#)

运行时监控现已在亚太地区（雅加达）、欧洲（巴黎）、亚太地区（大阪）、亚太地区（首尔）、中东（巴林）、欧洲（西班牙）、亚太地区（海得拉巴）、亚太地区（墨尔本）、以色列（特拉维夫）、美国西部（加利福尼亚北部）、欧洲（伦敦）、亚太地区（香港）、欧洲（米兰）、中东（）、南美洲（圣保罗）、亚洲（圣保罗）、亚洲（伦敦）、亚太地区（香港）、欧洲（米兰）、中东（）、南美洲（圣保罗）、亚洲（圣保罗UAE）、亚洲（圣保罗）、亚洲（香港）、欧洲（米兰）、中东（太平洋（孟买）、加拿大（中部）、非洲（开普敦）、欧洲（苏黎世）

2023 年 12 月 6 日

。

[GuardDuty 扩展了运行时监控功能](#)

除了检测对您的 Amazon EKS 集群的威胁外，还 GuardDuty 宣布正式推出运行时监控功能，用于检测对您的 Amazon ECS 工作负载的威胁，以及用于检测对您的 Amazon EC2 实例的威胁的预览版。有关 AWS 区域 目前支持运行时监控的更多信息，请参阅[区域和终端节点](#)。

2023 年 11 月 26 日

[Amazon GuardDuty 已更新服务相关角色 \(\) SLR](#)

GuardDuty 增加了使用亚马逊 ECS 操作管理和检索有关亚马逊 ECS 集群的信息以及使用管理亚马逊 ECS 账户设置的新权限 `guardduty:Activate`。与 Amazon 相关的操作 ECS 还会检索与之关联的标签的相关信息 GuardDuty。

2023 年 11 月 26 日

- 作为 GuardDuty 扩展“[运行时监控](#)”功能的一部分，添加了以下权限：

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[更新了 AWS 托管策略](#)

GuardDuty 在[AmazonGuardDutyFullAccessPolicy](#)和 `organizations:ListAccounts` 添加了新权限 [AmazonGuardDutyReadOnlyAccess](#)。

2023 年 11 月 16 日

[GuardDuty 发布了使用EKS审计日志监控的新查找类型。](#)

EKS审计日志监控现在支持亚太地区（墨尔本）的以下查找类型（ap-southeast-4）。

2023 年 11 月 11 日

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty 发布了使用EKS审计日志监控的新查找类型。](#)

2023 年 11 月 10 日

EKS 审计日志监控现在支持亚太地区（海得拉巴）(ap-south-2)、欧洲（苏黎世）(eu-central-2) 和欧洲（西班牙）(eu-south-2) 地区的以下查找类型。

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty 发布了使用EKS审计日志监控的新查找类型。](#)

2023 年 11 月 8 日

EKS 审计日志监控现在支持以下查找类型。这些查找类型尚不适用于亚太地区（海得拉巴）(ap-south-2)、欧洲（苏黎世）(eu-central-2)、欧洲（西班牙）(eu-south-2) 和亚太地区（墨尔本）(ap-southeast-4) 区域。

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

- Discovery:Kubernetes/
AnomalousBehavior.PermissionChecked

[EKS运行时监控发布了新代理 v1.3.1](#)

EKS运行时监控发布了新的代理版本 1.3.1，其中包括重要的安全补丁和更新。

2023 年 10 月 23 日

[用于调查发现的新过滤器属性](#)

GuardDuty 添加了用于筛选生成的发现结果的新标准。DNSrequest domain 后缀提供提示 GuardDuty 生成调查结果的活动中的涉及的第二和顶级域名。

2023 年 10 月 17 日

[EKS运行时监控发布了支持 Kubernetes 版本 1.28 的新代理 v1.3.0](#)

EKS运行时监控发布了支持 Kubernetes 版本 1.28 的新代理版本 1.3.0。增加了对 Ubuntu 的支持。有关更多信息，请参阅[EKS插件代理发布历史记录](#)。

2023 年 10 月 5 日

[向亚太地区（雅加达）和中东（）区域添加了基于 S3 和 AWS CloudTrail 机器学习 \(MLUAE\) 的结果类型](#)

以下 S3 和使用异常检测机器学习 (ML) 模型识别异常行为的 CloudTrail 发现现已在亚太地区（雅加达）和中东 (UAE) 地区推出：GuardDuty

2023 年 9 月 20 日

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty EKS运行时监控引入了在集群级别管理 GuardDuty 安全代理](#)

EKS Runtime Monitoring 增加了对管理单个EKS集群 GuardDuty 的安全代理的支持，以仅监控这些选定集群的运行时间事件。EKS运行时监控通过标签的支持扩展了此功能。

2023 年 9 月 13 日

[GuardDuty 恶意软件防护EC2将支持扩展到更多 AWS 区域](#)

恶意软件防护EC2现已在亚太地区（海得拉巴）、亚太地区（墨尔本）、欧洲（苏黎世）和欧洲（西班牙）推出。

2023 年 9 月 11 日

[GuardDuty 现已在以色列（特拉维夫）地区上市](#)

将以色列（特拉维夫）地区添加到 GuardDuty 现在可用的区域列表中。AWS 区域 以下保护计划也已在以色列（特拉维夫）地区推出：

2023 年 8 月 24 日

- [EKS保护](#) 包括EKS审计日志监控和EKS运行时监控。
- [Lambda 保护](#).
- [恶意软件防护 EC2](#).
- [S3 防护](#).

有关在以色列（特拉维夫）地区推出的更多信息，请参阅 [区域和端点](#)。

[GuardDuty 为您的组织添加了保护计划级别的自动启用配置](#)

更新您所在地区的保护计划的组织配置。可配置的选项包括为所有账户启用、为新账户自动启用，或者不为组织中的任何账户自动启用。

2023 年 8 月 16 日

[使用异常检测机器学习 \(ML\) 模型识别异常行为 GuardDuty的 S3 查找类型现已在亚太地区 \(大阪\) 推出](#)

以下调查发现类型现已在亚太地区 (大阪) 地区提供：

2023 年 8 月 10 日

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[EKS运行时监控现已在亚太地区 \(墨尔本\) 推出](#)

EKS GuardDuty EKS保护中的运行时监控为您的 AWS 环境中的 Amazon EKS 集群提供运行时威胁检测。该功能现已在亚太地区 (墨尔本) 推出。

2023 年 8 月 8 日

[更新了调用 GuardDuty启动的恶意软件扫描的 GuardDuty 结果列表](#)

某些 EKS Runtime Monitoring 查找类型现在可以在您的 AWS 账户中调用 GuardDuty启动的恶意软件扫描。

2023 年 7 月 19 日

[GuardDuty 通过以下方式支持 10,000 个会员账户 AWS Organizations](#)

GuardDuty 管理员账户现在最多可以通过管理 10,000 个成员账户 AWS Organizations。这还包括最多 5000 个通过邀请与 GuardDuty管理员账户关联的成员账户。

2023 年 6 月 29 日

[EKS运行时监控宣布了三种新的发现类型。](#)

EKS运行时监控支持三种基于流程注入技术的新查找类型。新的查找类型是:runtime/ DefenseEvasion .Proc、 :runtime/ .Ptrace和:runtime/。 ProcessInjection DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite。

2023 年 6 月 22 日

[EKS运行时监控发布了支持 Kubernetes 版本 1.27 的新代理 v1.2.0](#)

EKS运行时监控发布了新的代理版本 1.2.0，该版本还支持 ARM64基于实例的实例。增加了对 Bottlerocket 的支持。有关更多信息，请参阅[EKS插件代理发布历史记录](#)。

2023 年 6 月 16 日

[GuardDuty 控制台提供了您的发现的摘要视图。](#)

GuardDuty 控制台中的摘要仪表板提供了 GuardDuty调查结果的汇总视图。目前，控制面板通过各种小组件显示当前地区针对您的账户（或成员账户，如果您是 GuardDuty 管理员账户）生成的最近 10,000 条调查结果的数据。

2023 年 6 月 12 日

[EKS审计日志监控现已在亚太地区（海得拉巴）、亚太地区（墨尔本）、欧洲（苏黎世）和欧洲（西班牙）推出](#)

为您的账户启用EKS审计日志监控（在“EKS保护”中），以监控来自您的 Amazon EKS 集群的EKS审计日志，并分析这些日志中是否存在潜在的恶意和可疑活动。

2023 年 6 月 1 日

[EKS 审计日志监控现已在中东推出 \(UAE\)](#)

EKS“审计日志监控”现已在中东推出 (UAE)。为您的账户启用“EKS 审计日志监控”，以监控来自您的 Amazon EKS 集群的 EKS 审计日志，并分析这些日志中是否存在潜在的恶意和可疑活动。

2023 年 5 月 3 日

[GuardDuty 针对 EC2 公告的恶意软件防护按需恶意软件扫描](#)

恶意软件防护可 EC2 帮助您检测附加到您的 Amazon EC2 实例和容器工作负载的 Amazon EBS 卷中是否存在恶意软件。它现在提供两种类型的扫描：GuardDuty 启动扫描和按需扫描。GuardDuty 只有在 GuardDuty 生成 [调用 GuardDuty 启动的恶意软件扫描的发现结果](#) 之一时，启动的恶意软件扫描才会自动在 Amazon EBS 卷中启动无代理扫描。您可以通过提供与该亚马逊 EC2 实例关联的亚马逊资源名称 (ARN)，对账户中的亚马逊 EC2 实例启动按需恶意软件扫描。有关两种扫描类型有何差异的更多信息，请参阅 [恶意软件防护 EC2](#)。

2023 年 4 月 27 日

- [GuardDuty-启动的恶意软件扫描](#)
- [按需恶意软件扫描](#)

[GuardDuty 宣布 Lambda 保护](#)

Lambda 保护可帮助您识别 AWS Lambda 函数中的潜在安全威胁。

2023 年 4 月 20 日

- [Lambda Protection 查找类型](#)
- [修复可能受损的 Lambda 函数](#)

[GuardDuty 现已在亚太地区 \(墨尔本\) 地区推出](#)

将亚太地区 (墨尔本) 添加到可用区域列表中。AWS 区域 GuardDuty 如要了解此区域中提供哪些功能, 请参阅[区域和端点](#)。

2023 年 4 月 19 日

[GuardDuty 添加了 3 种新的 EC2 发现类型](#)

GuardDuty 引入了新的查找类型来检测外部解 DNS 析器和加密 DNS 技术的使用情况。有关 AWS 区域 何处支持这些查找类型的信息, 请参阅[区域和终端节点](#)。

2023 年 4 月 5 日

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty 宣布EKS保护中的EKS运行时监控](#)

EKSEKS保护中的运行时监控为您的 AWS 环境中的 Amazon EKS 集群提供运行时威胁检测。它使用 Amazon EKS 插件代理 (aws-guard-duty-agent) 从您的EKS工作负载中收集[运行时事件](#)。在 GuardDuty 收到这些运行时事件后，它会对其进行监控和分析，以识别潜在的可疑安全威胁。有关更多信息，请参阅[查找详细信息](#)和[EKS运行时监控查找类型](#)。

2023 年 3 月 30 日

[GuardDuty 添加了新功能 — autoEnableOrganizationMembers](#)

Amazon GuardDuty 添加了一个新的组织配置选项，该选项可帮助 GuardDuty 管理员账户对其组织成员启用的ALL审计和强制执行（如果需要）。GuardDuty 现在的最佳实践是使用 autoEnableOrganizationMembers 而不是 autoEnable 。autoEnable 已弃用但仍受支持。以下内容APIs受此新功能的影响：

2023 年 3 月 23 日

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[Amazon 中的“RDS保护”功能 GuardDuty 现已正式上线](#)

GuardDuty RDS保护监控和分析RDS登录活动，以识别您的 Amazon Aurora 数据库实例上的可疑登录行为。有关哪些 AWS 区域支持RDS保护的信息，请参阅[区域和终端节点](#)。

2023 年 3 月 16 日

[GuardDuty 宣布功能激活](#)

过去，GuardDuty API允许配置功能和数据源，但现在，所有新的 GuardDuty 保护类型都将配置为功能而不是数据源。GuardDuty 仍然支持通过的数据源API，但不会添加新的数据源API。功能激活会影响APIs用于启用 GuardDuty 或其中的保护类型的行为 GuardDuty。如果您通过API、或CFN模板管理 GuardDuty 账户SDK，请参阅[2023 年 3 月的GuardDuty API 变更](#)。

2023 年 3 月 16 日

[GuardDuty 的恶意软件防护EC2 现已在中东 \(UAE\) 区域推出](#)

中东 (UAE) 区域支持中的恶意软件防护EC2功能。GuardDuty 有关更多信息，请参阅[区域和端点](#)。

2023 年 3 月 13 日

[Amazon GuardDuty 已更新服务相关角色 \(\) SLR](#)

GuardDuty 添加了以下新权限以支持即将推出的 GuardDuty EKS运行时监控功能。

2023 年 3 月 8 日

- 使用 Amazon EKS 操作管理和检索有关EKS集群的信息，并管理集EKS群上的EKS插件。这些EKS操作还会检索与之关联的标签的相关信息 GuardDuty。

```
"eks:ListClusters",
"eks:DescribeCluster",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty 已更新服务相关角色 \(\) SLR](#)

GuardDuty SLR已更新，允许在启用恶意软件防护EC2SLR后创建恶意软件防护。EC2

2023 年 2 月 21 日

[GuardDuty 需要 TLS v1.2 或更高版本](#)

要与 AWS 资源通信，GuardDuty 需要并支持 TLS v1.2 或更高版本。有关更多信息，请参阅[数据保护](#)和[基础设施安全](#)。

2023 年 2 月 14 日

[GuardDuty 现已在亚太地区 \(海得拉巴\) 地区推出](#)

将亚太地区 (海得拉巴) 添加到可用区域列表中。AWS 区域 GuardDuty 有关更多信息，请参阅[区域和端点](#)。

2023 年 2 月 14 日

[Amazon GuardDuty 用户指南符合IAM最佳实践](#)

更新了指南以符合IAM最佳实践。有关更多信息，请参阅[中的安全最佳实践IAM](#)。

2023 年 2 月 10 日

[GuardDuty 现已在欧洲 \(西班牙 \) 地区上市](#)

将欧洲 (西班牙) 添加到可用 AWS 区域 地区 GuardDuty 列表中。有关更多信息，请参阅 [区域和端点](#)。

2023 年 2 月 8 日

[GuardDuty 现已在欧洲 \(苏黎世 \) 地区上市](#)

将欧洲 (苏黎世) 添加到可用 AWS 区域 区域 GuardDuty 列表中。有关更多信息，请参阅 [区域和端点](#)。

2022 年 12 月 12 日

[一项新功能的预览版 — GuardDuty RDS 保护](#)

GuardDuty RDS 保护监控和分析 RDS 登录活动，以识别您的 Amazon Aurora 数据库实例上的可疑登录行为。目前，该功能在五个 AWS 区域中的预览版中可用。有关更多信息，请参阅 [区域和端点](#)。

2022 年 11 月 30 日

[GuardDuty 现已在中东 \(UAE\) 区域上市](#)

将中东 (UAE) 添加到可用 AWS 区域 GuardDuty 位置列表中。有关更多信息，请参阅 [区域和端点](#)。

2022 年 10 月 6 日

[为一项新功能添加了内容 — GuardDuty 恶意软件防护 EC2](#)

2022 年 7 月 26 日

GuardDuty 的恶意软件防护 EC2 是 Amazon 的一项可选增强功能 GuardDuty。在 GuardDuty 识别风险资源的同时，恶意软件防护 EC2 会检测可能成为入侵来源的恶意软件。EC2 启用恶意软件保护后，每当在 Amazon EC2 实例或容器工作负载上 GuardDuty 检测到有恶意软件迹象的可疑行为时，GuardDuty 恶意软件防护都会对连接到受影响 EC2 实例或容器工作负载的 EBS 卷 EC2 启动无代理扫描，以检测是否存在恶意软件。有关恶意软件防护 EC2 的工作原理和配置此功能的信息，请参阅 [GuardDuty 恶意软件防护 EC2](#)。

- 有关 EC2 发现的恶意软件防护的信息，请参阅 [查找详细信息](#)。
 - 有关修复受损 EC2 实例和独立容器的信息，请参阅 [修复发现的安全问题](#)。
- GuardDuty
- 有关恶意软件扫描的审计 CloudWatch 日志以及在恶意软件扫描期间跳过资源的原因的信息，请参阅 [了解 CloudWatch 日志和跳过原因](#)。
 - 有关误报威胁检测的信息，请参阅 [GuardDuty 恶意软件防护中的报告误报](#)。EC2

[停用了一种调查发现](#)

[Exfiltration:S3/ObjectRead.Unusual](#) 已停用。

2022 年 7 月 5 日

[添加了新的 S3 查找类型，这些类型使用 GuardDuty 异常检测机器学习 \(ML\) 模型识别异常行为。](#)

添加了以下新的 S3 调查发现类型。这些发现类型可以识别 API 请求是否以异常方式调用了 IAM 实体。机器学习模型会评估您账户中的所有 API 请求，并识别与对手使用的技术相关的异常事件。要详细了解每项新调查发现，请参阅 [S3 调查发现类型](#)。

2022 年 7 月 5 日

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[添加了 GuardDuty EKS 保护内容 GuardDuty](#)

GuardDuty 现在可以通过监控 EKS 审计日志为您的 Amazon EKS 资源生成调查结果。要了解如何配置此功能，请参阅 [Amazon 中的 EKS 保护 GuardDuty](#)。有关 GuardDuty 可以为亚马逊 EKS 资源生成的调查结果列表，请参阅 [Kubernetes](#) 的调查结果。添加了新的修复指南，以支持修复 [Kubernetes 调查发现修复指南](#) 中的这些调查发现。

2022 年 1 月 25 日

添加了 1 个新调查发现	已添加一个新调查发现 UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.InsideAWS。当您的 AWS 环境之外的 AWS 账户访问您的 实例证书时，该发现会通知 您。	2022 年 1 月 20 日
更新了调查发现类型以帮助识别与 log4j 相关的问题	亚马逊更新 GuardDuty 了以 下查找类型，以帮助识别与 CVE -2021-44228和-2021- 4 CVE 5046相关的问题并对 其进行优先排序：Backdoor ：/C & .B; Backdoor：EC2/C & .B! CActivity EC2 CActivity DNS; 行为:EC2/NetworkPort Unusual。	2021 年 12 月 22 日
调查发现变化	UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltration 已更改为 UnauthorizedAccess :IAMUser/InstanceCredential Exfiltration.OutsideAWS。 该调查发现的改进版本可以 了解您凭证通常在哪些位置 使用，以减少通过本地网络 路由的流量中的调查发现。 UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS	2021 年 9 月 7 日
更新到 GuardDuty SLR	GuardDuty SLR已使用新的操 作进行了更新，以提高查找准 确性。	2021 年 8 月 3 日

[为每种调查发现类型添加了数据来源信息。](#)

查找结果描述现在包含有关 GuardDuty 用于生成该结果的数据源的信息。

2021 年 5 月 10 日

[停用了 13 个调查发现类型。](#)

13项调查结果已停用，取而代之的是新的 Anomalous Behaviour 发现。[Persistence:IAMUser/NetworkPermissions](#), [Persistence:IAMUser/ResourcePermissions](#), [Persistence:IAMUser/UserPermissions](#), [PrivilegeEscalation:IAMUser/AdministrativePermissions](#), [Recon:IAMUser/NetworkPermissions](#), [Recon:IAMUser/ResourcePermissions](#), [Recon:IAMUser/UserPermissions](#), [ResourceConsumption:IAMUser/ComputeResources](#), [Stealth:IAMUser/LoggingConfigurationModified](#), [Discovery:S3/BucketEnumeration.Unusual](#), [Impact:S3/ObjectDelete.Unusual](#), [Impact:S3/PermissionsModification.Unusual](#)。

2021 年 3 月 12 日

为异常行为添加了 8 种新的调查发现类型。

添加了 8 种基于委托人异常行为的新IAMUser发现类型。IAM [CredentialAccess:IAMUser/AnomalousBehavior](#) , [DefenseEv](#)
[asion:IAMUser/AnomalousBehavior](#) , [Discovery:IAMUser/AnomalousBehavior](#) , [Exfiltration:IAMUser/AnomalousBehav](#)
[ior](#) , , [Impact:IAMUser/AnomalousBehavior](#) , [InitialAccess:IAMUser/AnomalousBehavior](#) , [Persisten](#)
[ce:IAMUser/AnomalousBehavior](#) , [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)。

2021 年 3 月 12 日

添加了基于域名信誉的EC2调查结果。

添加了 4 种基于域信誉的新 Impact 调查发现类型 : [Impact:EC2/AbusedDomainRequest.Reputation](#) , [Impact:EC2/BitcoinDomainRequest.Reputation](#) , [Impact:EC2/MaliciousDomainRequest.Reputation](#)。还为C & CActivity添加了一个新EC2发现。 [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

2021 年 1 月 27 日

添加了 4 个新调查发现类型。	添加了 3 个新的 S3 MaliciousIPCaller 调查结果。 Discovery:S3/MaliciousIPCaller , Exfiltration:S3/MaliciousIPCaller , Impact:S3/MaliciousIPCaller 。还为 C&CActivity 添加了一个新 EC2 发现。 Backdoor:EC2/C&CActivity.B	2020 年 12 月 21 日
已停用 UnauthorizedAccess:EC2/TorIPCaller 调查发现类型。	UnauthorizedAccess:EC2/TorIPCaller 查找类型现已从中停用 GuardDuty。 了解更多 。	2020 年 10 月 1 日
添加了 Impact:EC2/WinRmBruteForce 调查发现类型。	添加了新的 Impact 调查发现 Impact:EC2/WinRmBruteForce。 了解更多 。	2020 年 9 月 17 日
添加了 Impact:EC2/PortSweep 调查发现类型。	添加了新的 Impact 调查发现 Impact:EC2/PortSweep。 了解更多 。	2020 年 9 月 17 日
GuardDuty 现已在非洲 (开普敦) 和欧洲 (米兰) 地区推出。	将非洲 (开普敦) 和欧洲 (米兰) 添加到可用 AWS 区域列表中 GuardDuty。 了解更多	2020 年 7 月 31 日
为监控 GuardDuty 费用添加了新的使用细节。	现在，您可以使用新指标来查询您的账户和您管理的账户的 GuardDuty 使用成本数据。控制台中提供了新的使用成本概览，网址为 https://console.aws.amazon.com/guardduty/ 。更多详细信息可通过 API。	2020 年 7 月 31 日

[在中添加了涵盖通过 S3 数据事件监控 S3 保护的内容 GuardDuty。](#)

GuardDuty S3 保护现在可通过监控 S3 数据平面事件作为新数据源提供。新账户将自动启用此功能。如果您已经在使用 GuardDuty ，则可以为自己或您的成员账户启用新的数据源。

2020 年 7 月 31 日

[添加了 14 个新的 S3 调查发现。](#)

已为 S3 控制面板和数据面板源添加了 14 种新的 S3 调查发现类型。

2020 年 7 月 31 日

[添加了对 S3 调查发现的额外支持，并更改了 2 个现有的调查发现类型名称。](#)

GuardDuty 调查结果现在包括涉及 S3 存储桶的调查结果的更多详细信息。与 S3 活动相关的现有调查发现类型已重命名：Policy:IAMUser/S3BlockPublicAccessDisabled 已更改为 Policy:S3/BucketBlockPublicAccessDisabled ，Stealth:IAMUser/S3ServerAccessLoggingDisabled 已更改为 Stealth:S3/ServerAccessLoggingDisabled。

2020 年 5 月 28 日

[添加了用于 AWS Organizations 集成的内容。](#)

GuardDuty 现在与 AWS Organizations 授权管理员集成，允许您管理组织内的 GuardDuty 帐户。当您将委托管理员设置为 GuardDuty 管理员帐户时，您可以自动启用 GuardDuty 由委派管理员帐户管理任何组织成员。您也可以在新的 AWS Organizations 成员账户 GuardDuty 中自动启用。[了解更多。](#)

2020 年 4 月 20 日

添加了“导出调查发现”功能的内容。	添加了描述的“导出调查结果”功能的内容 GuardDuty。	2019 年 11 月 14 日
添加了 UnauthorizedAccess:EC2/MetadataDNSRebind 调查发现类型。	添加了新的 Unauthorized 调查发现UnauthorizedAccess:EC2/MetadataDNSRebind。 了解更多 。	2019 年 10 月 10 日
添加了 Stealth:IAMUser/S3ServerAccessLoggingDisabled 调查发现类型。	添加了新的 Stealth 调查发现 Stealth:IAMUser/S3ServerAccessLoggingDisabled。 了解更多 。	2019 年 10 月 10 日
添加了 Policy:IAMUser/S3BlockPublicAccessDisabled 调查发现类型。	添加了新的 Policy 调查发现 Policy:IAMUser/S3BlockPublicAccessDisabled。 了解更多 。	2019 年 10 月 10 日
已停用 Backdoor:EC2/XORDD OS 调查发现类型。	Backdoor:EC2/XORDD OS查找类型现已从中停用 GuardDuty。 了解更多	2019 年 6 月 12 日
添加了 PrivilegeEscalation 调查发现类型。	PrivilegeEscalation 调查发现类型会检测用户尝试为其账户分配经过提升的更宽松权限的情形。 了解更多	2019 年 5 月 14 日
GuardDuty 现已在欧洲 (斯德哥尔摩) 区域上市。	将欧洲 (斯德哥尔摩) 添加到可用 AWS 地区列表 GuardDuty 中。 了解更多	2019 年 5 月 9 日
添加了新的调查发现类型 Recon:EC2/PortProbeEMRUnprotectedPort。	这一发现告诉您，EC2实例上的EMR相关敏感端口未被阻塞，并且正在积极探测中。 了解更多	2019 年 5 月 8 日

[添加了 5 种新的查找类型，用于检测您的 EC2 实例是否可能被用于拒绝服务 \(DoS\) 攻击。](#)

这些发现会告知您环境中的 EC2 实例，这些实例的行为方式可能表明它们正被用来执行拒绝服务 (DoS) 攻击。[了解更多](#)

2019 年 3 月 8 日

[添加了新的调查发现类型：Policy:IAMUser/RootCredentialUsage](#)

Policy:IAMUser/RootCredentialUsage finding type 会通知您，您的根用户登录凭据 AWS 账户正被用于向服务发出编程请求。AWS [了解更多](#)

2019 年 1 月 24 日

[UnauthorizedAccess:IAMUser/UnusualASNCaller 调查发现类型已停用](#)

UnauthorizedAccess:IAMUser/UnusualASNCaller 调查发现类型已停用。现在，您将收到有关通过其他活跃 GuardDuty 查找类型从异常网络调用的活动的通知。生成的查找类型将基于从异常网络调用的类别。API [了解更多](#)

2018 年 12 月 21 日

[添加了两种新的调查发现类型：PenTest:IAMUser/ParrotLinux 和 PenTest:IAMUser/PentooLinux](#)

PenTest:IAMUser/ParrotLinux 查找类型会通知您，运行 Parrot Security Linux 的计算机正在使用属于您 AWS 帐户的凭据进行 API 呼叫。PenTest:IAMUser/PentooLinux 查找类型会通知您运行 Pentoo Linux 的计算机正在使用属于您 AWS 帐户的凭据进行 API 呼叫。[了解更多](#)

2018 年 12 月 21 日

[增加了对 Amazon GuardDuty 公告 SNS 主题的支持](#)

现在，您可以订阅 GuardDuty 公告 SNS 主题，以接收有关新发布的查找类型、现有查找类型更新以及其他功能变更的通知。通知以 Amazon SNS 支持的所有格式提供。[了解更多](#)

2018 年 11 月 21 日

[添加了两种新的调查发现类型：UnauthorizedAccess:EC2/TorClient 和 UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClient 查找类型会通知您 AWS 环境中的某个 EC2 实例正在与 Tor Guard 或 Authority 节点建立连接。UnauthorizedAccess:EC2/TorRelay 查找类型会告知您 AWS 环境中的某个 EC2 实例正在与 Tor 网络建立连接，这表明它正在充当 Tor 中继。[了解更多](#)

2018 年 11 月 16 日

[添加了新的调查发现类型：CryptoCurrency:EC2/BitcoinTool.B](#)

这一发现告诉您，您的 AWS 环境中的一个 EC2 实例正在查询与比特币或其他加密货币相关活动关联的域名。[了解更多](#)

2018 年 11 月 9 日

[增加了对更新发送到 CloudWatch 事件的通知频率的支持](#)

现在，您可以更新向 CloudWatch 事件发送通知的频率，以了解后续出现的现有调查结果。可能的值为 15 分钟、1 小时或 6 小时（默认值）。[了解更多](#)

2018 年 10 月 9 日

[添加了区域支持](#)

增加了对 AWS GovCloud（美国西部）的区域支持。[了解更多](#)

2018 年 7 月 25 日

[增加了对 in AWS CloudFormation StackSets 的支持 GuardDuty](#)

您可以使用启用 Amazon GuardDuty 模板在多个账户中 GuardDuty 同时启用。[了解更多](#)

2018 年 2 月 6 日

增加了对 GuardDuty 自动存档规则的支持	客户现在可以为调查发现抑制构建精细的自动存档规则。对于符合自动存档规则的搜索结果，GuardDuty 会自动将其标记为已存档。这使客户能够进一步调整 GuardDuty 以在当前调查结果表中仅保留相关的调查结果。 了解更多	2018 年 5 月 4 日
GuardDuty 已在欧洲 (巴黎) 区域上市	GuardDuty 现已在欧洲 (巴黎) 上市，允许您在该地区扩展持续的安全监控和威胁检测。 了解更多	2018 年 3 月 29 日
现在支持通过 AWS CloudFormation 创建 GuardDuty 管理员帐户和成员帐户。	有关更多信息，请参阅 AWS::GuardDuty::master 和 AWS::GuardDuty::member 。	2018 年 3 月 6 日
添加了九个 CloudTrail 基于新增的异常检测。	这些新的查找类型将在所有支持的区域 GuardDuty 中自动启用。 了解更多	2018 年 2 月 28 日
增加了三个新的威胁情报检测 (调查发现类型) 。	这些新的查找类型将在所有支持的区域 GuardDuty 中自动启用。 了解更多	2018 年 2 月 5 日
提高 GuardDuty 成员账户的限额。	在此版本中，您最多可以为每个 AWS 账户 (GuardDuty 管理员账户) 添加 1000 个 GuardDuty 成员账户。 了解更多	2018 年 1 月 25 日

[GuardDuty 管理员账户和成员账户的可信 IP 列表和威胁列表的上传和进一步管理发生了变化。](#)

在此版本中，管理员 GuardDuty 账户中的用户可以上传和管理可信 IP 列表和威胁列表。来自成员 GuardDuty 账户的用户无法上传和管理名单。管理员账户上传的可信 IP 列表和威胁列表会被强加到其成员账户的 GuardDuty 功能上。[了解更多](#)

2018 年 1 月 25 日

早期更新

更改	描述	日期
初次发布	《亚马逊 GuardDuty 用户指南》的首次发布。	2017 年 11 月 28 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。