Amazon GuardDuty

亚马逊GuardDuty用户指南



Amazon GuardDuty: 亚马逊GuardDuty用户指南

Copyright © 2023 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 拥有的其它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。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是 GuardDuty？ 1
的定价 GuardDuty 1
正在访问 GuardDuty 1
开始使用 2
开始前的准备工作 2
步骤 1：启用亚马逊 GuardDuty 3
步骤 2：生成样本发现并探索基本操作 4
步骤 3：配置将GuardDuty发现导出到 Amazon S3 存储桶 5
步骤 4：通过 SNS 设置GuardDuty查找提醒 6
后续步骤 8
概念和术语 9
GuardDuty 功能激活 11
功能激活 11
GuardDuty API 变更 11
与数据源相比，功能激活 11
了解功能激活的工作原理 12
合并功能激活变更 12
映射dataSources到features 12
基础数据来源 14
Amazon CloudTrail 事件日志 14
如何 GuardDuty 处理Amazon CloudTrail全球事件 14
Amazon CloudTrail管理活动 14
VPC 流日志 15
DNS 日志 15
GuardDutyEKS 保护 16
功能 16
Kubernetes 审计日志 16
运行时监控 16
EKS 审核日志监控 16
为独立账户配置 EKS 审计日志监控 17
在多账户环境中配置 EKS 审核日志监控 17
EKS 运行时监控 21
经过验证的平台 21
CPU 和内存限制 22
配置 EKS 运行时监控 22
手动管理GuardDuty代理 28
亚马逊 ECR 存储库托管代理 GuardDuty 31
评估覆盖范围 33
设置 CPU 和内存监控 37
运行时事件类型 37
EKS 附加代理发布历史记录 42
GuardDuty Lambda 保护 43
功能 43
Lambda 网络活动监控 43
配置 Lambda 保护 43
为独立账户配置 Lambda 保护 43
在多账户环境中配置 Lambda 保护 44
GuardDuty恶意软件防护 48
恶意软件防护中支持的容量 49
功能 49
弹性块存储 (EBS) 卷 49
GuardDuty服务账号 50
恶意软件防护中的自定义 51
常规设置 51

带有用户定义标签的扫描选项 52
全球GuardDutyExcluded标签 54
GuardDuty-启动恶意软件扫描 55
配置GuardDuty启动的恶意软件扫描 57
调用GuardDuty启动的恶意软件扫描的调查结果 62
按需恶意软件扫描 62
按需恶意软件扫描的工作原理 63
开始使用 63
监控恶意软件扫描状态和结果 65
恶意软件保护配额 66
GuardDutyRDS 防护 68
支持的数据库 68
RDS 保护如何使用 RDS 登录活动监控 68
为独立账户配置 RDS 保护 69
在多账户环境中配置 RDS 保护 69
为委派管理员配置 RDS 保护 69
为现有成员账户自动启用 RDS 保护 70
为新成员账户自动启用 RDS 保护 71
有选择地为成员账户启用或禁用 RDS 保护 72
..... 72
功能 72
RDS 登录活动监控 72
GuardDuty S3 保护 74
如何 GuardDuty 使用 S3 数据事件 74
为独立账户配置 S3 保护 17
启用或禁用 S3 保护 74
在多账户环境中配置 S3 保护 75
自动为组织成员账户启用 S3 保护 75
在成员账户中选择性地启用或禁用 S3 保护 75
自动为新 GuardDuty 账户禁用 S3 保护 76
功能 77
Amazon CloudTrailS3 的数据事件 77
了解调查结果 78
正在寻找细节 78
查找概述 78
资源 79
RDS 数据库 (DB) 用户详细信息 82
EKS 运行时监控运行时详细信息 82
EBS 卷扫描详细信息 83
恶意软件防护查找详情 84
操作 84
演员或目标 85
其他信息 86
证据 86
异常行为 86
GuardDuty 查找格式 88
威胁情报集 89
示例发现结果 90
通过 GuardDuty 控制台或 API 生成样本调查结果 90
自动生成常见 GuardDuty发现 91
GuardDuty调查结果的严重性级别 92
GuardDuty查找聚合 93
定位和分析GuardDuty调查结果 93
查找类型 94
EC2 查找类型 94
Backdoor:EC2/C&CActivity.B 95
Backdoor:EC2/C&CActivity.B!DNS 96

Backdoor:EC2/DenialOfService.Dns 96
Backdoor:EC2/DenialOfService.Tcp 97
Backdoor:EC2/DenialOfService.Udp 97
Backdoor:EC2/DenialOfService.UdpOnTcpPorts 97
Backdoor:EC2/DenialOfService.UnusualProtocol 98
Backdoor:EC2/Spambot 98
Behavior:EC2/NetworkPortUnusual 98
Behavior:EC2/TrafficVolumeUnusual 99
CryptoCurrency:EC2/BitcoinTool.B 99
CryptoCurrency:EC2/BitcoinTool.B!DNS 100
DefenseEvasion:EC2/UnusualDNSResolver 100
DefenseEvasion:EC2/UnusualDoHActivity 100
DefenseEvasion:EC2/UnusualDoTActivity 101
Impact:EC2/AbusedDomainRequest.Reputation 101
Impact:EC2/BitcoinDomainRequest.Reputation 101
Impact:EC2/MaliciousDomainRequest.Reputation 102
Impact:EC2/PortSweep 102
Impact:EC2/SuspiciousDomainRequest.Reputation 103
Impact:EC2/WinRMBruteForce 103
Recon:EC2/PortProbeEMRUnprotectedPort 103
Recon:EC2/PortProbeUnprotectedPort 104
Recon:EC2/Portscan 104
Trojan:EC2/BlackholeTraffic 105
Trojan:EC2/BlackholeTraffic!DNS 105
Trojan:EC2/DGADomainRequest.B 105
Trojan:EC2/DGADomainRequest.C!DNS 106
Trojan:EC2/DNSDataExfiltration 106
Trojan:EC2/DriveBySourceTraffic!DNS 107
Trojan:EC2/DropPoint 107
Trojan:EC2/DropPoint!DNS 107
Trojan:EC2/PhishingDomainRequest!DNS 108
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom 108
UnauthorizedAccess:EC2/MetadataDNSRebind 108
UnauthorizedAccess:EC2/RDPBruteForce 109
UnauthorizedAccess:EC2/SSHBruteForce 109
UnauthorizedAccess:EC2/TorClient 110
UnauthorizedAccess:EC2/TorRelay 110
EKS 运行时监控查找类型 111
CryptoCurrency:Runtime/BitcoinTool.B 112
Backdoor:Runtime/C&CActivity.B 112
UnauthorizedAccess:Runtime/TorRelay 113
UnauthorizedAccess:Runtime/TorClient 113
Trojan:Runtime/BlackholeTraffic 114
Trojan:Runtime/DropPoint 114
CryptoCurrency:Runtime/BitcoinTool.B!DNS 115
Backdoor:Runtime/C&CActivity.B!DNS 115
Trojan:Runtime/BlackholeTraffic!DNS 116
Trojan:Runtime/DropPoint!DNS 116
Trojan:Runtime/DGADomainRequest.C!DNS 116
Trojan:Runtime/DriveBySourceTraffic!DNS 117
Trojan:Runtime/PhishingDomainRequest!DNS 117
Impact:Runtime/AbusedDomainRequest.Reputation 118
Impact:Runtime/BitcoinDomainRequest.Reputation 118
Impact:Runtime/MaliciousDomainRequest.Reputation 119
Impact:Runtime/SuspiciousDomainRequest.Reputation 119
UnauthorizedAccess:Runtime/MetadataDNSRebind 120
Execution:Runtime/NewBinaryExecuted 120

PrivilegeEscalation:Runtime/DockerSocketAccessed 121
PrivilegeEscalation:Runtime/RuncContainerEscape 121
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified 122
DefenseEvasion:Runtime/ProcessInjection.Proc 122
DefenseEvasion:Runtime/ProcessInjection.Ptrace 123
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite 123
Execution:Runtime/ReverseShell 123
DefenseEvasion:Runtime/FilelessExecution 124
Impact:Runtime/CryptoMinerExecuted 124
Execution:Runtime/NewLibraryLoaded 124
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory 125
PrivilegeEscalation:Runtime/UserfaultfdUsage 125
AS3 结果类型 126
CredentialAccess:IAMUser/AnomalousBehavior 126
DefenseEvasion:IAMUser/AnomalousBehavior 127
Discovery:IAMUser/AnomalousBehavior 127
Exfiltration:IAMUser/AnomalousBehavior 128
Impact:IAMUser/AnomalousBehavior 128
InitialAccess:IAMUser/AnomalousBehavior 129
PenTest:IAMUser/KaliLinux 129
PenTest:IAMUser/ParrotLinux 129
PenTest:IAMUser/PentooLinux 130
Persistence:IAMUser/AnomalousBehavior 130
Policy:IAMUser/RootCredentialUsage 130
PrivilegeEscalation:IAMUser/AnomalousBehavior 131
Recon:IAMUser/MaliciousIPCaller 131
Recon:IAMUser/MaliciousIPCaller.Custom 132
Recon:IAMUser/TorIPCaller 132
Stealth:IAMUser/CloudTrailLoggingDisabled 132
Stealth:IAMUser/PasswordPolicyChange 133
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B 133
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 133
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS 134
UnauthorizedAccess:IAMUser/MaliciousIPCaller 135
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom 135
UnauthorizedAccess:IAMUser/TorIPCaller 135
Kubernetes 审计日志查找类型 136
CredentialAccess:Kubernetes/MaliciousIPCaller 137
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom 137
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess 138
CredentialAccess:Kubernetes/TorIPCaller 138
DefenseEvasion:Kubernetes/MaliciousIPCaller 138
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom 139
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess 139
DefenseEvasion:Kubernetes/TorIPCaller 140
Discovery:Kubernetes/MaliciousIPCaller 140
Discovery:Kubernetes/MaliciousIPCaller.Custom 140
Discovery:Kubernetes/SuccessfulAnonymousAccess 141
Discovery:Kubernetes/TorIPCaller 141
Execution:Kubernetes/ExecInKubeSystemPod 142
Impact:Kubernetes/MaliciousIPCaller 142
Impact:Kubernetes/MaliciousIPCaller.Custom 142
Impact:Kubernetes/SuccessfulAnonymousAccess 143
Impact:Kubernetes/TorIPCaller 143
Persistence:Kubernetes/ContainerWithSensitiveMount 143
Persistence:Kubernetes/MaliciousIPCaller 144
Persistence:Kubernetes/MaliciousIPCaller.Custom 144

Persistence:Kubernetes/SuccessfulAnonymousAccess 145
Persistence:Kubernetes/TorIPCaller 145
Policy:Kubernetes/AdminAccessToDefaultServiceAccount 145
Policy:Kubernetes/AnonymousAccessGranted 146
Policy:Kubernetes/ExposedDashboard 146
Policy:Kubernetes/KubeflowDashboardExposed 146
PrivilegeEscalation:Kubernetes/PrivilegedContainer 147
Lambda 保护查找类型 147
Backdoor:Lambda/C&CActivity.B 147
CryptoCurrency:Lambda/BitcoinTool.B 148
Trojan:Lambda/BlackholeTraffic 148
Trojan:Lambda/DropPoint 149
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom 149
UnauthorizedAccess:Lambda/TorClient 149
UnauthorizedAccess:Lambda/TorRelay 150
恶意软件防护查找类型 150
Execution:EC2/MaliciousFile 150
Execution:ECS/MaliciousFile 151
Execution:Kubernetes/MaliciousFile 151
Execution:Container/MaliciousFile 151
Execution:EC2/SuspiciousFile 151
Execution:ECS/SuspiciousFile 152
Execution:Kubernetes/SuspiciousFile 152
Execution:Container/SuspiciousFile 153
RDS 保护查找类型 153
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin 153
CredentialAccess:RDS/AnomalousBehavior.FailedLogin 154
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce 154
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin 155
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin 155
Discovery:RDS/MaliciousIPCaller 156
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin 156
CredentialAccess:RDS/TorIPCaller.FailedLogin 156
Discovery:RDS/TorIPCaller 157
S3 查找类型 157
Discovery:S3/AnomalousBehavior 158
Discovery:S3/MaliciousIPCaller 158
Discovery:S3/MaliciousIPCaller.Custom 159
Discovery:S3/TorIPCaller 159
Exfiltration:S3/AnomalousBehavior 159
Exfiltration:S3/MaliciousIPCaller 160
Impact:S3/AnomalousBehavior.Delete 160
Impact:S3/AnomalousBehavior.Permission 161
Impact:S3/AnomalousBehavior.Write 161
Impact:S3/MaliciousIPCaller 162
PenTest:S3/KaliLinux 162
PenTest:S3/ParrotLinux 162
PenTest:S3/PentooLinux 163
Policy:S3/AccountBlockPublicAccessDisabled 163
Policy:S3/BucketAnonymousAccessGranted 163
Policy:S3/BucketBlockPublicAccessDisabled 164
Policy:S3/BucketPublicAccessGranted 164
Stealth:S3/ServerAccessLoggingDisabled 165
UnauthorizedAccess:S3/MaliciousIPCaller.Custom 165
UnauthorizedAccess:S3/TorIPCaller 165
停用的S3 166
Exfiltration:S3/ObjectRead.Unusual 166

Impact:S3/PermissionsModification.Unusual 167
Impact:S3/ObjectDelete.Unusual 167
Discovery:S3/BucketEnumeration.Unusual 167
Persistence:IAMUser/NetworkPermissions 168
Persistence:IAMUser/ResourcePermissions 168
Persistence:IAMUser/UserPermissions 169
PrivilegeEscalation:IAMUser/AdministrativePermissions 169
Recon:IAMUser/NetworkPermissions 170
Recon:IAMUser/ResourcePermissions 170
Recon:IAMUser/UserPermissions 170
ResourceConsumption:IAMUser/ComputeResources 171
Stealth:IAMUser/LoggingConfigurationModified 171
UnauthorizedAccess:IAMUser/ConsoleLogin 172
UnauthorizedAccess:EC2/TorIPCaller 172
Backdoor:EC2/XORDDOS 172
Behavior:IAMUser/InstanceLaunchUnusual 173
CryptoCurrency:EC2/BitcoinTool.A 173
UnauthorizedAccess:IAMUser/UnusualASNCaller 173
按资源类型划分的调查结果 173
调查结果表 174
管理调查结果 183
筛选结果 183
在GuardDuty控制台中创建过滤器 183
过滤器属性 184
抑制规则 187
..... 187
抑制规则的常见用例和示例 188
在中创建抑制规则 GuardDuty 189
..... 190
可信和威胁 IP 列表 191
列表格式 192
上传可信 IP 列表和威胁列表所需的权限 194
对可信 IP 列表和威胁列表使用服务器端加密 194
上传可信 IP 列表和威胁列表 195
激活或停用可信 IP 列表和威胁列表 195
更新可信 IP 列表和威胁列表 196
导出调查结果 196
配置发现结果导出所需的权限 197
向 KMS 密钥授予 GuardDuty 权限 197
向存储桶授予 GuardDuty 权限 198
使用控制台将发现结果导出到存储桶 200
导出访问错误 202
导出更新频率 202
使用事件自动做出响应 CloudWatch 202
CloudWatch的事件通知频率 GuardDuty 203
CloudWatch的事件格式 GuardDuty 203
创建CloudWatch事件规则以通知您GuardDuty发现的情况（控制台） 204
为 GuardDuty (CLI) 创建CloudWatch事件规则和目标 208
CloudWatchGuardDuty多账户环境的事件 209
了解 CloudWatch 日志和跳过资源的原因 209
GuardDuty 恶意软件保护中的审计 CloudWatch 日志 209
GuardDuty 恶意软件防护日志保留 210
不原因 210
报告恶意软件保护中的误报 212
误报文件提交 212
修复调查结果 213
修复受感染的 EC2 实例 213

修复受感染的 S3 存储桶 213
修复受感染的 ECS 集群 215
修复被盗的凭证 Amazon 215
修复受感染的独立容器 216
修复 EKS 审核日志监控结果 216
配置问题 217
泄露用户所属 217
泄露用户组 219
泄露的容器映像 219
泄露节点 220
修复 EKS 运行时监控结果 220
修复受损的数据库 221
使用成功的登录事件修复可能受损的数据库 221
修复带有失败登录事件的潜在受损数据库 222
修复可能受损的凭证 222
限制网络访问 223
修复受损的 Lambda 函数 223
管理多个 账户 224
通过以下方式管理多个账户Amazon Organizations 224
通过邀请管理多个账户 224
GuardDuty 管理员和成员账户关系 224
使用以下方式管理账户 Amazon Organizations 225
GuardDuty委派管理员的重要注意事项 226
指定委派管理员所需的权限 226
指定GuardDuty委派管理员 227
将GuardDuty管理员帐户合并到单个组织委派管理员下 230
注销GuardDuty委派管理员 230
通过的成员账户 231
通过邀请指定管理员和成员账户（控制台） 231
通过邀请指定 GuardDuty 管理员和成员账户 (API) 232
同时 GuardDuty 在多个账户中启用 233
估算成本 236
了解使用成本是如何计算的 236
查看 GuardDuty 使用情况统计信息 236
安全性 238
数据保护 238
静态加密 239
传输中加密 239
选择不使用您的数据来改善服务 239
使用登录 CloudTrail 240
GuardDuty 中的信息 CloudTrail 240
GuardDuty 控制层事件 CloudTrail 240
GuardDuty 中的数据事件 CloudTrail 240
示例： GuardDuty 日志文件 241
Identity and Access Management 243
受众 243
使用身份进行身份验证 244
使用策略管理访问 245
亚马逊如何与 IAM 协同 GuardDuty 工作 246
基于身份的策略示例 251
使用服务相关角色 256
问题排查 264
Amazon 托管策略 265
合规性验证 269
故障恢复能力 269
基础设施安全性 269
GuardDuty 集成 270

与... 集 GuardDuty 成Amazon Security Hub 270
GuardDuty 与亚马逊Detective 集成 270
Security Hub 集成 270
亚马逊如何GuardDuty将调查结果发送给 Amazon Security Hub 271
在 Amazon Security Hub 中查看 GuardDuty 结果 271
启用和配置集成 280
停止向 Security Hub 发布结果 280
Detective 整合 280
启用集成 281
从 GuardDuty 发现转向亚马逊Detective 281
使用与 GuardDuty多账户环境的集成 281
暂停或禁用 282
GuardDuty公告 283
亚马逊 SNS 消息格式 285
配额 288
问题排查 290
我正在启动按需恶意软件扫描，但它导致缺少所需权限错误。 290
我在使用恶意软件防护时收到iam:GetRole错误。 290
我想管理多个账户，但没有所需的Amazon Organizations管理权限。 290
我是一名 GuardDuty 管理员，需要启用 GuardDuty启动的恶意软件扫描，但不使用Amazon托管策略 AmazonGuardDutyFullAccess 进行管理 GuardDuty。 291
其他排查中的排查中的 291
区域和终端节点 292
特定区域功能的可用性 292
文档历史记录 294
早期更新 304
Amazon词汇表 305
..... cccvi

什么是亚马逊 GuardDuty？

Amazon GuardDuty 是一项安全监控服务，用于分析和处理Amazon CloudTrail管理事件基础数据来源 (p. 14)、Amazon CloudTrail事件日志、VPC 流日志（来自 Amazon EC2 实例）和 DNS 日志。它还处理 Kubernetes 审计日志、RDS 登录活动、S3 日志、EBS 卷、运行时监控和 Lambda 网络活动日志等功能。它使用恶意 IP 地址和域列表以及机器学习来标识您的Amazon环境中意外的和未经授权的恶意活动。这包括特权升级、使用遭暴露的凭证或者与恶意 IP 地址、域通信或者您的 Amazon EC2 实例和容器工作负载中存在恶意软件等问题，或者在数据库中发现异常登录事件模式等问题。例如， GuardDuty 可以检测受感染的 EC2 实例和提供恶意软件或挖矿比特币的容器工作负载。它还监控Amazon账户访问行为是否存在入侵迹象，例如未经授权的基础设施部署，例如部署在以前未使用过的区域中的实例，或异常 API 调用，例如更改密码策略以降低密码强度。

GuardDuty 通过生成安全调查结果 (p. 78)，告知您Amazon环境的状态，您可在 GuardDuty 控制台或通过亚马逊查看 EventBridge。 GuardDuty 还支持您将发现结果导出到 Amazon Simple Storage Service (S3) 桶，并与 and Detective 等Amazon Security Hub其他服务集成。

的定价 GuardDuty

有关 GuardDuty 定价的信息，请参阅亚马逊 GuardDuty 定价。

正在访问 GuardDuty

您可以通过以下任何 GuardDuty 方式使用：

GuardDuty 控制台

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

此控制台是可用于访问和使用 GuardDuty 的基于浏览器的界面。 GuardDuty 控制台提供对您的 GuardDuty 账户、数据和资源的访问权限。

Amazon 命令行工具

可以使用Amazon命令行工具，在系统的命令行中发出命令来执行 GuardDuty 任务和Amazon任务。如果要构建执行任务的脚本，命令行工具会十分有用。

有关安装和使用的更多信息Amazon CLI，请参阅Amazon Command Line Interface用户指南。要查看的可用Amazon CLI命令 GuardDuty，请参阅 CLI 命令参考。

GuardDuty HTTPS AP

您可以使用 GuardDuty HTTPS API（可让您直接向服务发布 HTTPS 请求）以Amazon编程方式访问 GuardDuty 和。有关详细信息，请参阅 GuardDuty API 参考。

Amazon 软件开发工具包

Amazon 提供了包含各种编程语言和平台（Java、Python、Ruby、.NET、iOS、Android 等）的库和示例代码的软件开发工具包 (SDK)。这些开发工具包提供了一种简便方法，以使用编程方式访问 GuardDuty。有关 Amazon 开发工具包的信息（包括如何下载及安装），请参阅适用于 Amazon Web Services 的工具。

GuardDuty 入门

本教程提供了有关以下内容的实际操作介绍GuardDuty。步骤 1 中介绍了以独立帐户或GuardDuty管理员GuardDuty身份启用的最低要求。Amazon Organizations第 2 步至第 5 步涵盖使用推荐的其他功能，GuardDuty以充分利用您的发现。

主题

- 开始前的准备工作 (p. 2)
- 步骤 1：启用亚马逊 GuardDuty (p. 3)
- 步骤 2：生成样本发现并探索基本操作 (p. 4)
- 步骤 3：配置将GuardDuty发现导出到 Amazon S3 存储桶 (p. 5)
- 步骤 4：通过 SNS 设置GuardDuty查找提醒 (p. 6)
- 后续步骤 (p. 8)

开始前的准备工作

GuardDuty是一种威胁检测服务，用于监控基础数据来源 (p. 14)Amazon CloudTrail事件日志、Amazon CloudTrail管理事件、Amazon VPC 流日志和 DNS 日志。GuardDuty还会分析与其保护类型相关的功能，前提是您单独启用这些功能。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（如果已启用），为您的账户GuardDuty生成安全调查结果。

启用后GuardDuty，它将开始监视您的环境。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。

您无需基础数据来源 (p. 14)明确启用任何。亚马逊直接从这些服务中GuardDuty提取独立的数据流。对于新GuardDuty账户，默认情况下，中支持的所有可用保护类型Amazon Web Services 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项或全部。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Amazon Web Services 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，请考虑以下各项：

- GuardDuty是一项区域性服务，这意味着您在本页上遵循的任何配置步骤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Amazon区域GuardDuty中启用。这样，GuardDuty 就可以生成有关未授权或异常活动的结果，甚至在您未主动使用的区域中也是如此。这还可以GuardDuty监控 IAM 等全球Amazon服务Amazon CloudTrail的事件。如果未在所有支持的区域中启用 GuardDuty，则其检测涉及全球性服务的能力将会减弱。有关可用区域的完整列表，请参阅区域和终端节点 (p. 292)。GuardDuty
- 在Amazon账户中拥有管理员权限的任何用户都可以启用GuardDuty，但是，按照最低权限的安全最佳实践，建议您创建一个 IAM 角色、用户或群组来进行GuardDuty专门管理。有关启用所需权限的信息，GuardDuty请参阅启用 GuardDuty 所需的权限 (p. 252)。
- 默认情况下，当您在任Amazon Web Services 区域一区域中GuardDuty首次启用时，它还会启用该区域支持的所有可用保护类型，包括恶意软件防护。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，这些权限和信任策略GuardDuty允许直接使用和分析来自的事件基础数据来源 (p. 14)以生成安全调查结果。恶意软件防护会为您的帐户创建另一个与服务相关的角色，名

为。AWSServiceRoleForAmazonGuardDutyMalwareProtection此角色包括允许恶意软件保护执行无代理扫描以检测您GuardDuty帐户中的恶意软件的权限和信任策略。它GuardDuty允许在您的账户中创建 EBS 卷快照，并与GuardDuty服务账户共享该快照。有关更多信息，请参阅的服务相关角色权限 GuardDuty (p. 256)：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Amazon账户将自动注册该区域的 30 天GuardDuty免费试用。

步骤 1：启用亚马逊 GuardDuty

使用的第一步GuardDuty是在您的帐户中启用它。启用后，GuardDuty将立即开始监视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帐户的搜索GuardDuty结果，则必须添加成员帐户并启用GuardDuty这些帐户。选择一个选项以了解如何GuardDuty为您的环境启用。

Standalone account environment

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机
2. 选择开始使用。
3. 请选择 EnableGuardDuty。

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位于同一个组织中，并且有权访问Amazon Organizations管理帐户，才能在组织GuardDuty内委派管理员。委派管理员可能需要其他权限，有关更多信息，请参阅指定委派管理员所需的权限 (p. 226)。

指定GuardDuty委派管理员

1. 使用管理账户在 https://console.aws.amazon.com/organizations/ 打开Amazon Organizations控制台。
2. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   是否已在您的账户中启用 GuardDuty？

   - 如果GuardDuty尚未启用，则可以选择 “开始使用”，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. 输入您要指定为组织GuardDuty委托管理员的帐户的十二位数Amazon帐户 ID，然后选择 Delegate。

   > Note
   >
   > 如果尚未启用 GuardDuty，则在指定委派管理员时，将在您当前的区域中为该账户启用GuardDuty。

添加成员账户

此过程包括通过将成员帐户添加到GuardDuty委托管理员帐户Amazon Organizations。还可以选择通过邀请添加成员。要详细了解在中关联成员的这两种方法GuardDuty，请参阅在亚马逊管理多个账户 GuardDuty (p. 224)。

1. 登录委托管理员账户
2. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
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. 通过选中账户 ID 旁边的复选框来选择要添加为成员的帐户。然后从 “操作” 菜单中选择 “添加成员”。

   Tip

   您可以通过开启自动启用功能自动将新帐户添加为成员；但是，这仅适用于启用该功能后加入组织的帐户。

步骤 2：生成样本发现并探索基本操作

当GuardDuty发现安全问题时，它会生成一个调查结果。GuardDuty发现是一个包含与该独特安全问题相关的详细信息的数据集。该发现的详细信息可用于帮助您调查问题。

GuardDuty支持使用占位符值生成样本调查结果，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回应。GuardDuty按照以下指南，为中提供的每种查找结果类型生成示例发现结果GuardDuty，有关生成示例发现的其他方法，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 (p. 90)。

创建和探索样本发现

1. 在导航窗格中，选择 Settings (设置)。
2. 在 Settings 页面上的 Sample findings 下，选择 Generate sample findings。
3. 在导航窗格中，选择 S u mmary 以查看有关Amazon环境中生成的发现的见解。有关摘要仪表板组件的更多信息，请参阅???。
4. 在导航窗格中，选择 Findings (结果)。样本发现结果显示在 “当前发现结果” 页面上，前缀为 [SAMPLE]。
5. 从列表中选择一个查找结果以显示该查找结果的详细信息。

   - 您可以查看查找详细信息窗格中可用的不同信息字段。不同类型的发现可能有不同的字段。有关所有查找类型中可用字段的更多信息，请参阅正在寻找细节 (p. 78)。在详细信息窗格中，您可以执行以下操作：

     - 在窗格顶部选择查找结果 ID 以打开该查找结果的完整 JSON 详细信息。也可以从此面板下载完整的 JSON 文件。JSON 包含控制台视图中未包含的一些附加信息，是其他工具和服务可以采集的格式。
     - 查看 “受影响的资源” 部分。实际上，此处的信息将帮助您确定账户中应进行调查的资源，并将包含相应Amazon Web Services Management Console的可操作资源的链接。
     - 选择 + 或-外观的玻璃图标，为该细节创建包容性或排他性滤镜。有关查找过滤器的更多信息，请参阅筛选结果 (p. 183)。
6. 存档所有样本发现

   a. 通过选中列表顶部的复选框来选择所有调查结果。
   b. 取消选择任何你想要保留的调查结果。
   c. 选择 “操作” 菜单，然后选择 “存档” 以隐藏样本调查结果。

      Note

      要查看存档的调查结果，请选择 “当前”，然后选择 “已存档” 以切换调查结果视图。

步骤 3：配置将GuardDuty发现导出到 Amazon S3 存储桶

GuardDuty建议将设置配置为导出搜索结果，因为它允许您将发现结果导出到 S3 存储桶，以便在 GuardDuty 90 天保留期之后无限期存储。这使您可以保留发现的记录或跟踪Amazon环境中随时间推移的问题。此处概述的过程将引导您设置新的 S3 存储桶并创建新的 KMS 密钥以加密控制台中的结果。有关这方面的更多信息，包括如何使用自己的现有存储桶或其他账户中的存储桶，请参阅导出调查结果 (p. 196)。

配置 S3 导出发现选项

1. 要对调查结果进行加密，您需要一个 KMS 密钥以及GuardDuty允许使用该密钥进行加密的策略。以下步骤将帮助您创建新的 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Amazon Web Services 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。但是，对于要从中导出发现的每个区域，您可以使用相同的存储桶和密钥对。

   a. 在 Amazon KMShttps://console.aws.amazon.com/kms 打开 控制台。
   b. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（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Amazon Key Management Service开发人员指南中的创建密钥。

   f. 为您的密钥提供别名，然后选择 Ne xt。
   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”创建密钥。
   i. 在客户管理的密钥页面上，选择您的密钥别名。
   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，授予对密钥的GuardDuty访问权限。此语句仅GuardDuty允许使用您向其添加此策略的密钥。编辑密钥策略时，确保 JSON 语法有效。如果在最后一条语句之前添加语句，则必须在右括号后添加逗号。

```
{
    "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"
        }
    }
}
```

将*## 1* 替换为 KMS 密钥的区域。将 *444455556666 ##### K* MS 密钥Amazon Web Services 账户的。将 *KMS KeyId* 替换为您选择进行加密的 KMS 密钥的密钥 ID。要识别所有这些值（区域和密钥 ID）Amazon Web Services 账户，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，将 *111122223333* 替换为账户的。Amazon Web Services 账户 GuardDuty将*## 2* 替换为GuardDuty账户的区域。将 *SourceDetectorID* 替换为 Region *2 GuardDuty* 账户的探测器 ID。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

l. 选择保存。

2. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
3. 在导航窗格中，选择 Settings (设置)。
4. 在 “查找结果导出选项” 下，选择 “立即配置”。
5. 选择 “新建存储桶”。为您的 S3 存储桶提供一个唯一的名称。
6. （可选）您可以通过生成示例发现来测试新的导出设置。在导航窗格中，选择 Settings (设置)。
7. 在 “样本调查结果” 部分下，选择 “生成样本调查结果”。新的样本发现将在最多五分钟后以条目形式显示GuardDuty在由创建的 S3 存储桶中。

步骤 4：通过 SNS 设置GuardDuty查找提醒

GuardDuty与亚马逊集成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。借EventBridge助，您可以将查找事件连接到Amazon Lambda函数、Amazon EC2 系统管理器自动化、亚马逊简单通知服务 (SNS) 等目标，使用GuardDuty发现结果启动对您的发现的自动响应。

在此示例中，您将创建一个 SNS 主题作为EventBridge规则的目标，然后您将EventBridge用于创建从中捕获发现数据的规则GuardDuty。生成的规则将发现的详细信息转发到电子邮件地址。要了解如何向 Slack 或 Amazon Chime 发送调查结果，以及如何修改发送警报的调查结果类型，请参阅。设置 Amazon SNS 主题和终端节点 (p. 204)

为您的发现警报创建 SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择 Create Topic。
4. 对于 “类型”，选择 “标准”。
5. 对于 Name（名称），请输入 **`GuardDuty`**。
6. 选择 Create Topic。您的新主题的主题详细信息将打开。
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 E ndpoint，输入要向其发送通知的电子邮件地址。
10. 选择 Create subscription（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，请转到您的电子邮件收件箱，然后在订阅消息中选择确认订阅。

    Note

    要检查电子邮件确认状态，请转到 SNS 控制台并选择订阅。

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

1. 通过 https://console.aws.amazon.com/events/ 打开EventBridge主机。

2. 在导航窗格中，选择 Rules (规则)。
3. 选择 Create rule (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 Event bus（事件总线），选择 default（默认）。
6. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。
7. 选择下一步。
8. 对于事件源，选择 Amazon 事件。
9. 对于事件模式，选择事件模式表单。
10. 对于 Event source（事件源），选择 Amazon services（服务）。
11. 对于 Amazon Service，选择 GuardDuty。
12. 对于 “事件类型”，选择 “GuardDuty查找”。
13. 选择 Next（下一步）。
14. 对于 Target types（目标类型），选择 Amazon service（服务）。
15. 对于选择目标，选择 SNS 主题，为主题选择您之前创建的 SNS 主题的名称。
16. 在 “其他设置” 部分中，为 “配置目标输入” 选择 “输入变压器”。

    添加输入转换器将从中发送的 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的输入路径中，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：

```
"You have 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>"
```

20. 选择 Confirm（确认）。
21. 选择 Next（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 Create rule（创建规则）。
25. （可选）使用步骤 2 中的流程生成样本调查结果，测试您的新规则。对于生成的每个样本调查结果，您都会收到一封电子邮件。

后续步骤

随着您继续使用GuardDuty，您将逐渐了解与您的环境相关的发现类型。每当收到新的发现时，您都可以找到信息，包括有关该发现的补救建议，方法是从查找结果详细信息窗格的查找结果描述中选择“了解更多”，或者在上搜索查找结果名称查找类型 (p. 94)。

以下功能将帮助您进行调整，GuardDuty使其能够为您的Amazon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 存储段名称等）轻松对发现结果进行排序，可以在其中创建和保存筛选条件GuardDuty。有关更多信息，请参阅筛选结果 (p. 183)：
- 如果您收到有关环境中预期行为的调查结果，则可以根据使用抑制规则 (p. 187)定义的标准自动存档调查结果。
- 为防止从可信 IP 的子集生成调查结果，或使GuardDuty监控 IP 超出其正常监控范围，可以设置可信 IP 和威胁列表 (p. 191)。

概念和术语

在您开始使用亚马逊时GuardDuty，您可以从了解其关键概念中受益。

账户

包含您的 Amazon 资源的标准 Amazon Web Services (Amazon) 账户。您可以使用账户登录到 Amazon 并启用 GuardDuty。

您还可以邀请其他账户启用 GuardDuty 并在 GuardDuty 中与您的 Amazon 账户关联。如果您的邀请被接受，您的帐户将被指定为管理员GuardDuty帐户，添加的帐户将成为您的成员帐户。然后您可以代表成员账户查看和管理这些账户的 GuardDuty 结果。

管理员帐户的用户可以配置GuardDuty、查看和管理自己的帐户及其所有成员帐户的搜索GuardDuty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在其自己的账户中配置 GuardDuty，并能查看和管理 GuardDuty 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。

一个Amazon账户不能同时是GuardDuty管理员和成员账户。一个 Amazon 账户只能接受一个成员资格邀请。接受成员资格邀请是可选的。

有关更多信息，请参阅在亚马逊管理多个账户 GuardDuty (p. 224)：

探测器

所有 GuardDuty 调查结果都与一个探测器关联，后者是表示 GuardDuty 服务的对象。探测器是一个区域实体，每个Amazon Web Services 区域GuardDuty运行机构都需要一个独特的探测器。当您在某个区域GuardDuty中启用时，将在该区域中生成一个具有唯一的 32 个字母数字 detectorID 的新检测器。detectorID 的格式为。`12abc34d567e8fa901bc2d34e56789f0`

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

Note

在多帐户环境中，成员帐户的所有发现结果都会汇总到管理员帐户的检测器中。

某些GuardDuty功能是通过检测器配置的，例如配置CloudWatch事件通知频率以及启用或禁用GuardDuty要处理的可选数据源。

数据源

一组数据的源或位置。检测Amazon环境中未经授权或意外的活动。GuardDuty分析和处理来自Amazon CloudTrail事件日志、Amazon CloudTrail管理事件、S3 Amazon CloudTrail 的数据事件、VPC 流日志、DNS 日志、EKS 审核日志、RDS 登录活动监控和 EBS 卷的数据。有关更多信息，请参阅基础数据来源 (p. 14)：

功能

为您的GuardDuty保护计划配置的功能对象有助于检测Amazon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以分析和处理数据。一些功能对象包括 EKS 审计日志、RDS 登录活动监控和 EBS 卷。有关更多信息，请参阅中的功能激活 GuardDuty (p. 11)：

结果

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 (p. 78)：

结果显示在 GuardDuty 控制台中，包含安全问题的详细说明。您也可以通过调用GetFindings和ListFindingsAPI 操作来检索生成的调查结果。

您还可以通过亚马逊CloudWatch活动查看您的GuardDuty发现。GuardDutyCloudWatch通过 HTTPS 协议将调查结果发送给亚马逊。有关更多信息，请参阅使用 Amazon Ev CloudWatch ents 创建对GuardDuty调查结果的自定义 (p. 202)：

扫描选项

启用GuardDuty恶意软件保护后，它允许您指定要扫描或跳过哪些 Amazon EC2 实例和 Amazon Elastic Block Store (EBS) 卷。此功能允许您将与 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。与您添加到包含标签列表的标签相关的资源会被扫描是否有恶意软件，而添加到排除标签列表的资源则不会被扫描。有关更多信息，请参阅带有用户定义标签的扫描选项 (p. 52)：

快照保留

启用GuardDuty恶意软件保护后，它会提供在您的Amazon账户中保留 EBS 卷快照的选项。GuardDuty 基于 EBS 卷的快照生成副本 EBS 卷。只有在恶意软件保护扫描在副本 EBS 卷中检测到恶意软件时，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，则无论快照保留设置如何，GuardDuty都会自动删除 EBS 卷的快照。有关更多信息，请参阅快照保留 (p. 51)：

禁止规则

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 筛选器定义一条规则，以便仅从特定 VPC 中的实例自动存档 `Recon:EC2/Portscan`，运行特定 AMI 或者使用特定的 EC2 标签。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 检测到执行其他恶意活动（例如，加密货币挖矿）的实例时发出警告。

GuardDuty管理员帐户中定义的禁止规则适用于GuardDuty成员帐户。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 (p. 187)：

可信 IP 列表

可信 IP 地址列表，用于与您的Amazon环境进行高度安全的通信。GuardDuty 不根据可信 IP 列表生成结果。有关更多信息，请参阅处理可信 IP 列表和威胁列表 (p. 191)：

威胁 IP 列表

已知恶意 IP 地址列表。除了因潜在的可疑活动而生成调查结果外，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 处理可信 IP 列表和威胁列表 (p. 191)。

中的功能激活 GuardDuty

当您首次启 GuardDuty 用 Amazon 或在其中启用保护类型时 GuardDuty， GuardDuty 开始在您的Amazon环境基础数据来源 (p. 14)中处理相应的内容。 GuardDuty 使用这些数据源处理事件流，例如 VPC 流日志、DNS 日志以及Amazon CloudTrail事件和管理日志。然后，它会分析这些事件以识别潜在的安全威胁并在您的帐户中生成调查结果。

除日志数据源外， GuardDuty 还可以使用来自Amazon环境中其他Amazon服务的额外数据来监控和分析潜在的安全威胁。

功能激活

当您添加其他 GuardDuty 保护（例如 S3 保护或 EKS 保护）时，您可以配置与保护类型对应的 GuardDuty 功能。从历史上看， GuardDuty 保护是在 APIdataSources 中调用的。但是，在 2023 年 3 月之后，新的 GuardDuty 保护类型现在配置为features和不配置dataSources。 GuardDuty 仍然支持配置 2023 年 3 月之前启动的保护类型，就像dataSources通过 API 一样，但新的保护类型仅可用于features。

如果您通过控制台管理 GuardDuty 配置和保护类型，则不会直接受到此更改的影响，也无需采取任何操作。功能激活会影响为启用 GuardDuty 或其中的保护类型而调用的 API 的行为 GuardDuty。有关更多信息，请参阅GuardDuty API 变更 (p. 11)：

GuardDuty 2023 年 3 月的 API 变更

GuardDuty API 配置了不属于列表的保护功能基础数据来源 (p. 14)。功能对象包含功能详细信息，例如功能名称和状态，并且可能包含某些功能的其他配置。此迁移会影响亚马逊 API 参考中的以下 GuardDuty API：

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

与数据源相比，功能激活

从历史上看，所有 GuardDuty 功能都是通过 API 中的dataSources对象传递的。从 2023 年 3 月起，features优先 GuardDuty 选择dataSources对象而不是 API 中的对象。所有早期的数据源都有相应的功能，但较新的功能可能没有相应的数据源。

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

- 该dataSources对象包含每种保护类型的对象及其状态。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 月开始，功能激活将是在您的Amazon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Amazon Web Services 区域的地方 GuardDuty 都是相同的。但是，可能并未在每个区域提供。因此，可用功能名称可能因地区而异。

了解功能激活的工作原理

GuardDuty API 将继续返回适用的dataSources对象，它们还将以不同的格式返回包含相同信息的features对象。 GuardDuty 2023 年 3 月之前推出的功能将通过dataSources对象和features对象提供。 GuardDuty 自 2023 年 3 月起推出的功能只能通过该features对象使用。您无法创建或更新检测器，也无法在同一 API 请求中Amazon Organizations使用两dataSources者和features对象符号来描述您的检测器。要启用 GuardDuty 保护类型，您需要使用现在也包含该features对象的 API 将现有数据源迁移到该features对象。

> **Note**
>
> GuardDuty 修改后不会添加新的数据源。

GuardDuty 已弃用数据源。但是，它仍然支持基础数据来源 (p. 14). 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。最佳做法还要求在为账户启用新的保护类型时使用功能激活。

合并功能激活变更

- 如果您通过 API、SDK 或Amazon CloudFormation模板管理 GuardDuty 配置，并希望启用潜在的新 GuardDuty 功能，则需要分别修改代码和模板。有关更多信息，请参阅亚马逊 API 参考中更新 GuardDuty 的 API。
- 对于在此升级之前配置的 GuardDuty 功能，您可以继续使用 API、SDK 或Amazon CloudFormation模板。但是，我们建议您切换到使用feature对象。

  所有数据源都有一个等效的要素对象。有关更多信息，请参阅映射dataSources到features (p. 12)：
- additionalConfiguration在features对象中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但功能的配置Status未设置为ENABLED，则 GuardDuty 不会更新AdditionalConfiguration。
  - 以下 API 会受到此影响：
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

映射dataSources到features

下表显示了保护类型、dataSources和的映射features。

GuardDuty 保护类型	**Data source name***	**Feature name**
VPC 流日志 (p. 15)	flowLogs（只读；无法修改）	FLOW_LOGS（只读；无法修改）
DNS 日志 (p. 15)	dnsLogs（只读；无法修改）	DNS_LOGS（只读；无法修改）

GuardDuty 保护类型	**Data source name***	**Feature name**
CloudTrail 事件 (p. 14)	cloudLogs（只读；无法修改）	CLOUD_LOGS（只读；无法修改）
S3 (p. 74)	s3Logs	S3_DATA_EVENTS
EKS 审核日志监控 (p. 16)	kubernetes.auditlogs	EKS_AUDIT_LOGS
恶意软件防护 (p. 48)	malwareProtection.scanEc2InstanceWithFindings.ebsVolumes	EBS_MALWARE_PROTECTION
RDS 登录事件 (p. 68)	GuardDuty 仅为这些保护类型提供功能激活支持。	RDS_LOGIN_EVENTS
EKS 运行时监控 (p. 21)		EKS_RUNTIME_MONITORING
EKS 运行时监控插件管理 (p. 21)		EKS_RUNTIME_MONITORING.additi
Lambda 保护 (p. 43)		LAMBDA_NETWORK_LOGS

*GetUsageStatistics 使用自己的dataSource名字。有关更多信息，请参阅 估算 GuardDuty 成本 (p. 236) 或 GetUsageStatistics。

基础数据来源

GuardDuty 使用基础数据源来检测与已知恶意域和 IP 地址的通信并识别异常行为。在从这些来源传输到的过程中 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分析和异常检测，然后丢弃这些日志。

下面介绍介绍如何 GuardDuty 使用每个支持的数据来源。启用后 GuardDuty Amazon Web Services 账户，将 GuardDuty 自动开始监视这些日志源。

主题

- Amazon CloudTrail 事件日志 (p. 14)
- Amazon CloudTrail管理活动 (p. 14)
- VPC 流日志 (p. 15)
- DNS 日志 (p. 15)

Amazon CloudTrail 事件日志

Amazon CloudTrail为您提供账户Amazon的 API 调用历史记录，包括使用、Amazon软件开发工具包Amazon Web Services Management Console、命令行工具和某些Amazon服务进行的 API 调用。CloudTrail 还可以帮助您确定哪些用户和账户调用了支持服务的Amazon API CloudTrail、调用调用的源 IP 地址以及调用调用的时间。有关更多信息，请参阅《Amazon CloudTrail用户指南》Amazon CloudTrail中的内容。 GuardDuty 还监视 CloudTrail 管理事件。

启用后 GuardDuty，它会立即开始分析您的 CloudTrail 事件日志。它 CloudTrail 通过独立和重复的事件流直接消耗 CloudTrail 管理资源。使用 CloudTrail活动无需额外 GuardDuty 付费。

GuardDuty 不会管理您的 CloudTrail 事件或以任何方式影响您的现有 CloudTrail 配置。要直接管理 CloudTrail 事件的访问和保留，您必须使用 CloudTrail 服务控制台或 API。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

如何 GuardDuty 处理Amazon CloudTrail全球事件

关于 GuardDuty 用 CloudTrail 作数据源的方式的另一个重要细节是 CloudTrail 全局事件的处理和处理。对于大多数服务，事件被记录在发生操作的区域。对于全球服务，例如 IAMAmazon Security Token Service、Amazon S3 CloudFront、Amazon 和 Route 53，事件将传送到包含全球服务的任何跟踪，事件将记录为在美国东部（弗吉尼亚北部）地区发生。有关更多信息，请参阅关于全球服务事件。

GuardDuty 处理进入一个区域的所有事件，包括 CloudTrail 发送到所有区域的全局事件。这 GuardDuty 允许维护每个区域的用户和角色配置文件，并使其能够准确检测跨区域恶意使用的证书。

我们强烈建议您在所有支持的Amazon区域 GuardDuty 中启用。这使您 GuardDuty 能够生成有关未经授权或异常活动的调查结果，即使在您不积极使用的区域也是如此。这也 GuardDuty 允许监视全球Amazon服务Amazon CloudTrail 的事件。如果 GuardDuty 未在所有支持的区域都启用，则其检测涉及全球服务的活动的能力就会降低。

Amazon CloudTrail管理活动

管理事件也称为控制平面事件。通过这些事件，可以了解对在您Amazon账户内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：

- 配置安全性（IAMAttachRolePolicy API 操作）
- 配置传送数据的规则（Amazon EC2CreateSubnet API 操作）
- 设置日志（Amazon CloudTrailCreateTrailAPI 操作）

VPC 流日志

Amazon VPC 的 VPC 流日志功能捕获有关在您Amazon环境内传入和传出与亚马逊Elastic Compute Cloud (Amazon EC2) 实例的网络接口的 IP 流量的信息。

启用后 GuardDuty，它会立即开始分析来自您账户内的 Amazon EC2 实例的 VPC 流日志。它通过独立和重复的流日志流直接从 VPC 流日志功能中消耗 VPC 流日志事件。此过程不会影响您的任何现有流日志配置。

GuardDuty Lambda 保护 (p. 43)

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的所有 Lambda 函数的 Amazon VPC 流日志，甚至包括那些不使用 VPC 网络的日志。为了保护您的 Lambda 函数免受潜在的安全威胁，您需要在您的 GuardDuty 账户中配置 Lambda 保护。有关更多信息，请参阅GuardDuty Lambda 保护 (p. 43)：

GuardDutyEKS 保护 (p. 16)

当您为账户启用 EKS 运行时监控时，会根据账户VPC 流日志 (p. 15)中的 EKS EC2 节点 GuardDuty 继续分析和生成安全调查结果。这 GuardDuty 有助于基于 VPC Flow Log 覆盖范围所特有的威胁检测功能继续提供安全覆盖范围。这还有 GuardDuty 助于在 EKS 运行时监控覆盖范围差距的情况下继续提供覆盖范围。但是，您无需为 EKS EC2 节点的 EKS 运行时监控和 VPC 流日志监控付费。

GuardDuty 如果从 EKS EC2 节点接收运行时事件，则无需为分析来自该实例的 VPC 流日志付费。或者， GuardDuty 如果未从 EKS EC2 节点接收运行时事件，则无需为分析来自实例的运行时事件付费。

GuardDuty 无法管理您的流日志或使其无法在您的账户中访问。要管理对流日志的访问和保留，您必须配置 VPC 流日志功能。

DNS 日志

如果您为 Amazon EC2 实例使用Amazon DNS 解析器（默认设置），则 GuardDuty 可以通过内部 DNS 解析器访问和处理您的请求和响应Amazon DNS 日志。如果您使用其他 DNS 解析器，例如 OpenDNS 或 GoogleDNS，或者如果您设置了自己的 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 DNS 日志。该数据流与通过 R oute 53 Resolver 查询记录功能提供的数据是分开的。此功能的配置不影响 GuardDuty分析。

亚马逊的 EKS 保护 GuardDuty

亚马逊的 EKS 保护GuardDuty提供威胁检测覆盖范围，帮助您保护Amazon环境中的 Amazon EKS 集群。EKS 保护包括 EKS 审核日志监控和 EKS 运行时系统监控。

EKS 审计日志监控

EKS 审计日志监控可帮助您检测亚马逊 Elastic Kubernetes 服务 (亚马逊 EKS) 内的 EKS 集群中可能存在的可疑活动。EKS 审计日志监控使用 Kubernetes 审核日志来捕获用户、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Kubernetes 审计日志 (p. 16)：

EKS 运行时监控

EKS 运行时监控使用操作系统级事件来帮助您检测 Amazon EKS 集群内的 Amazon EKS 节点和容器中的潜在威胁。有关更多信息，请参阅运行时监控 (p. 16)：

EKS 保护中的功能

Kubernetes 审计日志

Kubernetes 审核日志捕获您的 Amazon EKS 集群中的连续操作，包括来自用户、使用 Kubernetes API 的应用程序和控制平面的活动。审计日志是所有 Kubernetes 集群的组成部分。有关更多信息，请参阅 Kubernetes 文档中的审计。

亚马逊 EKS 允许通过 EKS 控制平面日志功能将 Kubernetes 审核CloudWatch日志作为亚马逊日志提取。GuardDuty如果您尚未为 Amazon EKS 启用 Kubernetes 审核日志，则不会管理您的亚马逊 EKS 控制层面日志，也不会在您的账户中允许访问 Kubernetes 审核日志。要管理您的 Kubernetes 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 审核日志监控的信息，请参阅EKS 审核日志监控 (p. 16)。

运行时监控

EKS 运行时监控使用新的 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安全代理可以接收这些 EKS 集群的运行时事件。考虑到您还为账户启用了 EKS 运行时监控，现在GuardDuty可以使用这些事件来增加各个 EKS 工作负载（例如文件访问、流程执行和网络连接）的运行时可见性。EKS 运行时监控通过分析 EKS 集群的运行时行为来帮助您检测潜在的安全威胁。

GuardDuty不会管理您的 EKS 集群的运行时事件，也不会让它们在您的账户中访问。

EKS 审核日志监控

EKS 审核日志监控可帮助您在Amazon Elastic Kubernetes Service 中的 EKS 集群中检测潜在的可疑活动。启用 EKS 审核日志监控后， GuardDuty 立即开始Kubernetes 审计日志 (p. 16)从您的 Amazon EKS 集群进行监控，并分析它们是否存在潜在的恶意和可疑活动。它通过独立和重复的流日志流直接从 Amazon EKS 控制层面日志记录功能使用 Kubernetes 审计日志事件。此过程不需要任何额外设置，也不影响您可能拥有的任何现有 Amazon EKS 控制平面日志配置。

当您禁用 EKS 审核日志监控时，会 GuardDuty 立即停止监控和分析您的 EKS 资源的 Kubernetes 审核日志。

EKS 审核日志监控可能并非在所有可用Amazon Web Services 区域的地方都可 GuardDuty 用。有关更多信息，请参阅特定区域功能的可用性 (p. 292)：

30 天免费试用期如何影响 GuardDuty 账户

- 当您首次启 GuardDuty 用（新 GuardDuty 账户）时，EKS Protection 中的 EKS 审核日志监控已启用，有 30 天的免费试用期。
- 现有 GuardDuty 账户可以首次启用 EKS 审核日志监控，试用期为 30 天。
- 如果您的现有 GuardDuty 账户在 EKS 运行时监控正式发布之前一直在使用 EKS 审核日志监控，并且该 GuardDuty 账户已经使用了定价模型，则无需采取任何措施即可继续使用 EKS Audit Log Monitoring。Amazon Web Services 区域

为独立账户配置 EKS 审计日志监控

选择以下访问方法之一，获取有关为独立账户启用或禁用 EKS 审核日志监控的说明。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Seting s 下，选择 EKS 保护。
3. 在“配置”选项卡下，您可以查看 EKS 审核日志监控的当前配置状态。
4. 要更新账户的配置，请选择编辑。
5. 选择“启用”以启用 EKS 保护功能以获得最佳保护。这将通过自动启用 EKS 审核日志监控和自动代理管理 GuardDuty。EKS 运行时监控 (p. 21)

   如果您的账户的 EKS Protection 配置中的现有保护范围已经包含其中一项功能，则选择“启用”将仅启用未包含在此保护范围内的功能。

   - 要启用或禁用 EKS 审核日志监控和 EKS 运行时监控，请在 E KS 保护下选择“启用”。
6. 要仅启用或禁用 EKS 审核日志监控，请分别选择或取消选择 EKS 审核日志监控。
7. 选择“保存”以确认您的选择。

API

1. 使用您自己的区域检测器 ID 调用 updateDetectorAPI 操作，`EKS_AUDIT_LOGS`并将`features`对象名称传递为`ENABLED`或`DISABLED`。
2. 您也可以启用或禁用运行 aAmazon CLI 命令的 EKS 审核日志监控。以下示例代码启用 GuardDuty EKS 审核日志监控。要将其禁用，请`ENABLED`替换为`DISABLED`。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

在多账户环境中配置 EKS 审核日志监控

在多账户环境中，只有 GuardDuty 委托管理员账户可以选择为其组织中的成员账户启用或禁用 EKS Audit Log Monitoring; 功能。 GuardDuty 成员账户无法从其账户修改此配置。委托管理员账户使用管理其成员账户Amazon Organizations。该委托管理员可以选择在所有新账户加入组织时为其自动启用 EKS 审核日志监控。有关多账户环境的更多信息，请参阅在 Amazon 中管理多个账户 GuardDuty。

为委派管理员配置 EKS 审核日志监控

选择要EKS_AUDIT_LOGS为委派管理员配置的访问方法之一。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用管理账户证书。
2. 在导航窗格中的 Seting s 下，选择 EKS 保护。
3. 在“配置”选项卡下，您可以查看委派管理员的 EKS 审核日志监控的当前配置状态。
4. 要更新委派管理员的配置，请在委派管理员窗格中选择编辑。
5. 要启用或禁用 EKS 审核日志监控和EKS 运行时监控 (p. 21)，请在 EKS 保护下分别选择启用或禁用。

   要仅启用或禁用 EKS 审核日志监控，请分别选择或取消选择 EKS 审核日志监控。选择“保存”以确认您的选择。

API

使用您自己的区域探测器 ID 调用 updateDetectorAPI 操作，并将`features`对象`name`和`status`作为`EKS_AUDIT_LOGS`和传递为`ENABLED`或`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

您可以通过运行以下Amazon CLI命令来启用或禁用 EKS 审核日志监控。确保使用委托管理员的有效*### # ID*。

> Note
>
> 以下示例代码启用 EKS 审核日志监控。要将其禁用，请`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
acountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

为现有成员账户自动启用 EKS 审核日志监控

> Note
>
> 此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

选择一种访问方法，为组织中的现有成员账户启用 EKS 审核日志监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托的管理员账户证书。
2. 在导航窗格中的 Seting s 下，选择 EKS 保护。
3. 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。

   要更新配置，请在“活跃成员帐户”窗格中选择“编辑”。

4. 要启用或禁用 EKS Audit Log Monitoring 和，请在 EKS 保护下分别为所有活跃成员帐户选择启用或为所有活跃成员帐户分别选择禁用。EKS 运行时监控 (p. 21)

   要为组织中的特定账户自定义 EKS 审核日志监控配置，请参阅有选择地启用或禁用成员账户的 EKS 审核日志监控 (p. 19)。

   要仅启用或禁用 EKS 审核日志监控，请分别为所有活跃成员账户选择或取消选择 EKS 审核日志监控。选择 “保存” 以确认您的选择。
5. 现在，您可以查看组织中启用了 EKS 审核日志监控的活跃成员账户的数量。

API

- 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*### ID* 调用 updateMemberDetectorsAPI 操作。
- 以下示例显示如何为单个成员账户启用 EKS 审计日志监控。要将其禁用，请ENABLED替换为DISABLED。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

  Note

  您也可以传递由空格分隔的账户 ID 列表。
- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

有选择地启用或禁用成员账户的 EKS 审核日志监控

Note

此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

选择一种访问方法，有选择地为组织中的成员账户启用或禁用 EKS 审核日志监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托的管理员账户证书。
2. 在导航窗格中的 Settings 下，选择 Accounts。

   在账户页面上，查看 EKS 审核日志监控列，了解您的成员账户状态。
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账户。您可以一次选择多个账户。在 “编辑保护计划” 下拉列表下，选择 EKS 审核日志监控，然后选择相应的选项。
4. 选择 “保存” 以确认您的选择。

API

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*### ID* 调用 updateMemberDetectorsAPI 操作。

以下示例显示如何为单个成员账户启用 EKS 审计日志监控。要将其禁用，请ENABLED替换为DISABLED。您也可以传递由空格分隔的账户 ID 列表。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

为新成员账户自动启用 EKS 审核日志监控

Note

此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

选择一种访问方法，为加入您的组织的新账户启用 EKS 审核日志监控。

Console

委托管理员可以使用 EKS 审核日志监控或账户页面，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 EKS 审核日志监控

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托的管理员账户证书。
2. 请执行下列操作之一：
   - 使用 E KS 保护页面：
     1. 在导航窗格中的 Seting s 下，选择 EKS 保护。
     2. 在 “配置” 选项卡下，您可以查看新账户的 EKS 审核日志监控的当前状态。
     3. 要更新 EKS 审核日志监控配置，请在 “新账户” 默认配置窗格中选择 “编辑”。
     4. 要启用或禁用 EKS 审核日志监控和EKS 运行时监控 (p. 21)，请在 EKS 保护下分别选择启用或禁用。

        要仅启用或禁用 EKS 审核日志监控，对于新账户，请分别选择或取消选择 EKS 审核日志监控。选择 “保存” 以确认您的选择。
   - 使用 “帐户” 页面：
     1. 在导航窗格中的 Settings 下，选择 Accounts。
     2. 在 “帐户” 页面上，选择 “自动启用” 首选项。
     3. 在 “自动启用 GuardDuty 和设置源首选项” 配置中，确保 GuardDuty 为添加到组织的所有帐户启用自动启用。
     4. 现在，您可以为新成员账户启用 EKS 审核日志监控。

API

- 要有选择地为您的新账户启用或禁用 EKS 审核日志监控，请使用您自己的### *ID* 调用 UpdateOrganizationConfigurationAPI 操作。
- 以下示例显示如何为单个成员账户启用 EKS 审计日志监控。要将其禁用，请ENABLED替换为DISABLED。您也可以传递由空格分隔的账户 ID 列表。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

EKS 运行时监控

EKS 运行时监控为您的环境中的亚马逊弹性 Kubernetes 服务 (Amazon EKS) 节点和容器提供运行时威胁检测范围。AmazonEKS 运行时监控使用新的GuardDuty安全代理（EKS 附加组件），它增加了对单个 EKS 工作负载的运行时可见性，例如文件访问、流程执行和网络连接。GuardDuty安全代理可帮助GuardDuty识别您的 EKS 集群中可能遭到入侵的特定容器。它还可以检测到有人企图将权限从单个容器升级到底层 EC2 主机以及更广泛的Amazon环境。有关更多信息，请参阅运行时监控 (p. 16)：

启用 EKS 运行时监控分为两个步骤：

- 启用 EKS 运行时监控后，GuardDuty可以开始监控 EKS 集群中的运行时事件。如果您的 EKS 集群没有通过自动GuardDuty或手动部署安全代理，则GuardDuty将无法接收 EKS 集群的运行时事件。
- GuardDuty要接收这些运行时事件，必须在 EKS 集群内的 EKS 节点上部署GuardDuty安全代理。您可以选择GuardDuty自动管理安全客户端，也可以手动管理安全客户端的部署和更新。

  自动管理代理

  如果您选择GuardDuty代表您管理安全代理，GuardDuty将完全自动部署 EKS 集群的安全代理并更新到安全代理。如果您通过管理多个帐户Amazon Organizations，则可以为您的组织配置 EKS 运行时监控。部署GuardDuty安全代理后，GuardDuty可以分析运行时事件中是否存在潜在威胁。

  手动管理代理

  如果您选择手动部署和更新GuardDuty安全代理，则需要在 EKS 集群内协调GuardDuty安全代理软件的部署，跨所有账户以及Amazon Web Services 区域此功能可用的部署。这也将要求您在部署新集群和工作负载时支持安全的数据流，同时监控和解决覆盖缺口。

  有关如何自动或手动配置GuardDuty安全客户端的信息，请参阅配置 EKS 运行时监控 (p. 22)。

  Note

  GuardDuty支持在亚马逊 EC2 实例上运行的 EKS 集群。它不支持在上运行的 EKS 集群Amazon Fargate。

30 天免费试用期对账户有何影响 GuardDuty

- 您可以通过 30 天免费试用期在 EKS 运行时监控中启用 EKS 运行时监控。GuardDuty首次启用时，默认情况下不启用 EKS 运行时监控。

  现有GuardDuty账户可以首次启用 EKS 审核日志监控，试用期为 30 天。
- 在上述两种情况下，GuardDuty账户都需要决定是要手动部署安全代理还是选择GuardDuty代表他们管理安全代理。

  30 天免费试用期与GuardDuty安全代理的部署无关。确保在启用 EKS 运行时监控时，还必须选择自动管理代理或手动部署和更新安全代理。

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。下表显示了部署GuardDuty代理和配置 EKS 运行时监控的经过验证的配置。

操作系统分发	内核版本	内核支持	CPU 架构		支持的 Kubernetes 版本
AL2	5.4	eBPF、追踪点、Kprobe	支持	支持	v1.21-1.27
	5.10				
Bottlerocket	5.10	eBPF、追踪点、Kprobe	支持	支持	v1.23-1.27
	5.15				

代理支持的 Kubernetes 版本 GuardDuty

以下列表显示了 EKS 附加GuardDuty安全代理支持的 EKS 集群的 Kubernetes 版本。有关`aws-guardduty-agent`发行版本的信息，请参见EKS 附加代理发布历史记录 (p. 42)。

Kubernetes 版本	亚马逊 EKS 附加GuardDuty代理版本		
–	v1.2.0	v1.1.0	v1.0.0
1.27	支持	不支持	不支持
1.26		支持	
1.25			支持
1.24			
1.23			
1.22			
1.21			

CPU 和内存限制

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

参数	最低限额	最大限额
CPU	200 米	1000 米
内存	256 Mi	1024 Mi

启用 EKS 运行时监控并评估覆盖范围以确保已部署 Amazon EKS 附加GuardDuty代理后，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 (p. 37)：

配置 EKS 运行时监控

重要概念

在配置 EKS 运行时监控之前，请考虑以下关键概念：

- EKS 运行时监控 — 通过监控GuardDuty安全代理捕获的 EKS 集群的运行时事件来GuardDuty检测潜在威胁。如果您选择 EKS 运行时监控，则必须自动或手动部署GuardDuty安全代理才能接收来自此代理的运行时事件。
  - 当您通过控制台启用 EKS 运行时监控时，GuardDuty可以开始监控和分析您的账户的所有现有 EKS 集群的运行时事件。GuardDuty要接收这些运行时事件以进行监控和分析，请确保代理也部署在 EKS 集群上。
  - 当您禁用 EKS 运行时监控时，它会对您的账户产生以下影响：
    - GuardDuty立即停止监视和分析所有现有 EKS 集群的运行时事件。
    - 如果您已通过配置自动代理管理GuardDuty，则此操作还会移除GuardDuty已部署的安全客户端。GuardDuty还会删除由创建的 VPC 终端节点，GuardDuty以便安全代理可以使用此 VPC 终端节点将 EKS 集群的运行时事件发送到GuardDuty。GuardDuty如果您手动部署了安全代理，则不会采取任何操作。
- 代理管理-如果您GuardDuty想为账户中的所有现有和新的 EKS 集群部署和更新所需的 EKS 附加代理，请选择自动管理代理。这还将创建一个 VPC 终端节点，安全代理通过该终端节点将运行时事件传送到该终端节点GuardDuty。EKS 运行时监控要求您的工作节点具有指向活动 `guardduty-data` VPC 终端节点的有效网络路径。对于自动管理代理用例，根据 IP 可用性GuardDuty选择子网来创建 VPC 终端节点。如果您使用高级网络拓扑，则必须验证连接是否可行。通过自动管理代理时GuardDuty，EKS 运行时监控不会创建共享 VPC。

  如果您想手动管理 EKS 附加代理，则需要协调GuardDuty安全代理软件在 EKS 集群中、所有账户和可用此功能的Amazon Web Services 区域位置的部署。这也将要求您在持续部署新集群和工作负载时支持安全的数据流，同时监控和解决覆盖缺口。手动管理 EKS 附加代理时，请务必为您的账户配置 EKS 运行时监控。如果您未配置 EKS 运行时监控，则GuardDuty安全代理可能无法按预期运行。有关手动部署安全代理的更多信息，请参阅手动管理GuardDuty代理 (p. 28)。

  Note

  安全代理将运行时事件传送到GuardDuty。GuardDuty要监控有关 EKS 工作负载的运行时事件，请确保部署了安全代理并且还为您的账户启用了 EKS 运行时监控。

  - 如果您已配置GuardDuty为自动管理代理，则禁用 EKS 运行时监控也会删除 EKS 附加代理。GuardDuty将停止接收现有和新的 EKS 集群的运行时事件。删除 EKS 附加代理不会自动从 EKS 集群中删除`amazon-guardduty`命名空间。如果要删除`amazon-guardduty`命名空间，请参阅删除命名空间。

    要继续接收 EKS 集群的运行时事件，您需要再次启用 EKS 运行时监控并确保部署安全代理（自动或手动）。
  - 如果您手动部署了 EKS 附加代理，则禁用 EKS 运行时监控将导致GuardDuty无法接收现有和新 EKS 集群的运行时事件。GuardDuty不会采取任何操作从您的 EKS 集群中删除代理。
  - 如果您已手动部署了 EKS 附加代理，现在想要自动管理安全客户端的部署和更新，则在GuardDuty未删除手动创建的安全代理时不要部署新的安全代理。此外，GuardDuty将根据需要更新现有的安全代理。GuardDuty无法验证您是否已配置与此GuardDuty安全代理关联的 Amazon VPC 终端节点。如果您想GuardDuty继续使用手动部署的GuardDuty代理，请确保不要删除关联的 Amazon VPC 终端节点。
  - 如果您已配置GuardDuty为自动管理代理，但现在取消选择了此选项，则GuardDuty不会删除GuardDuty安全客户端。要继续接收 EKS 集群的运行时事件，请务必手动部署安全代理。有关更多信息，请参阅手动管理GuardDuty代理 (p. 28)：

了解为什么GuardDuty选择亚马逊 VPC 终端节点

GuardDutyGuardDuty由于以下原因，选择将与您的 Amazon EKS 集群运行时事件类型 (p. 37)关联的亚马逊 VPC 终端节点从 Amazon EKS 附加代理发送到：

- 亚马逊 VPC（接口）终端节点由提供支持PrivateLink。这GuardDuty允许使用专用网络路径发送运行时事件。

- 某些Amazon服务可以选择将与其服务相关的接口 VPC 终端节点的费用包含在服务成本中。只要您已启用 EKS 运行时监控并在您的 EKS 集群上运行GuardDuty代理，就无需支付向其发送安全遥测数据 (运行时事件类型 (p. 37)) 的网络费用。GuardDuty
- Amazon EKS 工作节点实例可以在非公共子网中运行。GuardDuty如果不使用 Amazon VPC 终端节点，在这些节点上运行的GuardDuty代理将无法访问的公共终端节点。

为独立账户配置 EKS 运行时监控

有关与之关联的账户 Amazon Organizations，请参阅为多账户环境配置 EKS 运行时监控 (p. 25)。

Console

为独立账户启用或禁用 EKS 运行时监控

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “设置” 下，选择 EKS 保护。
3. 在 “配置” 选项卡下，您可以选择 “编辑” 来更新您的账户的现有配置。
4. 在编辑配置页面上，选择以下选项之一：

   - 选择 “启用” 以启用 EKS 保护功能以获得最佳保护。这将自动启用 EKS 审核日志监控 (p. 16) EKS 运行时监控和自动代理管理GuardDuty。

     如果您账户的 EKS Protection 配置中的现有保护范围已经包含其中一项功能，则选择 “启用” 将仅启用此保护范围中未包含的功能。
   - 展开 Advanced options (高级选项)。在 “选择保护范围” 下，您可以选择 EKS 审核日志监控或 EKS 运行时监控，或者同时选择两者。

     如果您选择 EKS 运行时监控，请确保手动或自动部署安全代理以接收运行时事件。如果您GuardDuty想管理账户中所有现有和新的 EKS 集群的安全代理的部署和更新，请选择自动管理代理；否则，请参阅手动管理GuardDuty代理 (p. 28)。
5. 选择保存。
6. 在 “保存配置” 对话框中，选择 “保存”。

API

1. 使用您自己的区域探测器 ID 调用 updateDetectorAPI 操作，并将`features`对象名称传递为或`EKS_RUNTIME_MONITORING`并将状态传递为`ENABLED`或`DISABLED`。
2. 如果将`EKS_RUNTIME_MONITORING`和都设置`Status`ENABLED为`EKS_ADDON_MANAGEMENT`，则GuardDuty允许手动管理安全客户端。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。

   如果设置`Status`为 f ENABLED o EKS_RUNTIME_MONITORING r 但 f EKS_ADDON_MANAGEMENT or 设置`Status`为`DISABLED`或未设置全部，则必须手动管理GuardDuty安全客户端。有关更多信息，请参阅手动管理GuardDuty代理。
3. 您也可以启用或禁用运行 a Amazon CLI 命令的 EKS 运行时监控。以下示例代码启用 EKS 运行时监控。要禁用它，请将其`ENABLED`替换为`DISABLED`。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

为多账户环境配置 EKS 运行时监控

在多账户环境中，只有GuardDuty委托管理员账户可以选择为其组织中的成员账户启用或禁用 EKS 运行时监控功能。GuardDuty成员账户无法从其账户修改此配置。委托管理员帐户使用以下方式管理其成员帐户Amazon Organizations。该委托管理员可以选择在所有新账户加入组织时自动为他们启用 EKS 运行时监控。有关多账户环境的更多信息，请参阅 Amazon GuardDuty 用户指南中的管理多个账户。

为委派管理员配置 EKS 运行时监控

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “设置” 下，选择 EKS 保护。
3. 在 “配置” 选项卡下的 “委派管理员” 部分，选择 “编辑” 以更新此帐户的现有配置。
4. 在编辑配置页面上，选择以下选项之一：
   - 选择 “启用” 以启用 EKS 保护功能以获得最佳保护。这将自动启用 EKS 审核日志监控 (p. 16) EKS 运行时监控和自动代理管理GuardDuty。
   - 展开 Advanced options (高级选项)。在 “选择保护范围” 下，您可以选择 EKS 审核日志监控或 EKS 运行时监控，或者同时选择两者。

     如果您选择 EKS 运行时监控，请确保手动或自动部署安全代理以接收运行时事件。如果您GuardDuty想管理账户中所有现有和新的 EKS 集群的安全代理的部署和更新，请选择自动管理代理；否则，请参阅手动管理GuardDuty代理 (p. 28)。
5. 选择保存。
6. 在 “保存配置” 对话框中，选择 “保存”。

API

使用您自己的区域探测器 ID 调用 updateDetectorAPI 操作，`EKS_RUNTIME_MONITORING`并将`features`对象`name`和`status`作为`ENABLED`或传递`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

您可以通过运行以下Amazon CLI命令来启用或禁用 EKS 运行时监控。确保使用委托管理员的有效*### ID*。

> **Note**
>
> 以下示例代码启用 EKS 运行时监控。要禁用它，请将其`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --acount-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" :
 "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" :
 "ENABLED"}] ]'
```

为活跃成员账户配置 EKS 运行时监控

> **Note**
>
> 此功能仅适用于通过以下方式管理成员的GuardDuty委托管理员Amazon Organizations。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户凭证。
2. 在导航窗格中的 “设置” 下，选择 EKS 保护。
3. 在 “配置” 选项卡下的 “活跃成员帐户” 部分，选择 “编辑” 以更新所有活跃成员帐户的现有配置。
4. 在编辑配置页面上，选择以下选项之一：

   - 为所有活跃成员帐户选择 “启用” 以启用 EKS 运行时监控功能以获得最佳保护。这将通过以下方式自动启用 EKS 审核日志监控、EKS 运行时监控和自动代理管理GuardDuty。
   - 展开 Advanced options (高级选项)。在 “选择保护范围” 下，您可以选择 EKS 审核日志监控或 EKS 运行时监控，或者同时选择两者。

     如果您选择 EKS 运行时监控，则必须自动或手动部署GuardDuty安全代理才能接收运行时事件。如果您GuardDuty想管理账户中所有现有和新的 EKS 集群的部署和更新安全代理，请选择自动管理代理；否则，请参阅手动管理GuardDuty代理 (p. 28)。

   此步骤还将GuardDuty为加入您的组织的新账户自动启用，并设置相同的 EKS 运行时监控配置。
5. 选择保存。
6. 在 “保存配置” 对话框中，选择 “保存”。

API

- 要有选择地为您的成员账户启用或禁用 EKS 运行时监控，请使用您自己的*### ID* 调用 updateMemberDetectorsAPI 操作。
- 如果将EKS_RUNTIME_MONITORING和都设置StatusENABLED为EKS_ADDON_MANAGEMENT，则GuardDuty允许手动管理安全客户端。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。

  如果设置Status为 f ENABLED o EKS_RUNTIME_MONITORING r 但 f EKS_ADDON_MANAGEMENT or 设置Status为DISABLED或未设置全部，则必须手动管理GuardDuty安全客户端。有关更多信息，请参阅手动管理GuardDuty代理。
- 以下示例说明如何为单个成员账户启用 EKS 运行时监控。要禁用它，请将其ENABLED替换为DISABLED。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
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"}] ]'
```

  Note

  您也可以传递以空格分隔的账户 ID 列表。
- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

为新成员自动启用 EKS 运行时监控

Note

此功能仅适用于通过以下方式管理成员的GuardDuty委托管理员Amazon Organizations。

GuardDuty委托管理员可以为加入您的组织的新账户启用 EKS 运行时监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户凭证。
2. 在导航窗格中的 “设置” 下，选择 EKS 运行时监控。
3. 在 “配置” 选项卡下的 “新帐户默认配置” 部分中，选择编辑以更新加入组织的新帐户的现有配置。
4. 在编辑配置页面上，选择以下选项之一：

   - 选择 “启用” 以启用 EKS 运行时监控功能以获得最佳保护。这将通过以下方式自动启用 EKS 审核日志监控、EKS 运行时监控和自动代理管理GuardDuty。
   - 展开 Advanced options (高级选项)。在 “选择保护范围” 下，您可以选择 EKS 审核日志监控或 EKS 运行时监控，或者同时选择两者。

     如果您选择 EKS 运行时监控，则必须自动或手动部署GuardDuty安全代理才能接收运行时事件。如果您GuardDuty想管理账户中所有现有和新的 EKS 集群的部署和更新安全代理，请选择自动管理代理；否则，请参阅手动管理GuardDuty代理 (p. 28)。

   此步骤还将GuardDuty为加入您的组织的新账户自动启用，并设置相同的 EKS 运行时监控配置。
5. 选择保存。
6. 在 “保存配置” 对话框中，选择 “保存”。

API

- 要有选择地为您的新账户启用或禁用 EKS 运行时监控，请使用您自己的*### ID* 调用 UpdateOrganizationConfigurationAPI 操作。
- 如果将EKS_RUNTIME_MONITORING和都设置StatusENABLED为EKS_ADDON_MANAGEMENT，则GuardDuty允许手动管理安全客户端。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。

  如果设置Status为 f ENABLED o EKS_RUNTIME_MONITORING r 但 f EKS_ADDON_MANAGEMENT or 设置Status为DISABLED或未设置全部，则必须手动管理GuardDuty安全客户端。有关更多信息，请参阅手动管理GuardDuty代理。
- 以下示例说明如何为单个成员账户启用 EKS 运行时监控。要禁用它，请将其ENABLED替换为DISABLED。您也可以传递以空格分隔的账户 ID 列表。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable  --features '[{"Name" :
 "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" :
 [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'
```

有选择地为活跃成员账户启用或禁用 EKS 运行时监控

Note

此功能仅适用于通过以下方式管理成员的GuardDuty委托管理员Amazon Organizations。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户凭证。
2. 在导航窗格中的 Settings 下，选择 Accounts。
3. 在“帐户”页面上，查看 EKS 运行时监控和自动管理代理的列。这些列中的值表示账户的 EKS 运行时监控和自动管理代理是启用还是未启用。
4. 选择要为 EKS 运行时监控或自动管理代理配置的帐户。这包括配置 EKS 运行时监控和自动管理代理。

   您可以一次选择多个账户。
5. 从操作下拉菜单中，您可以选择启用 EKS 运行时监控。

   必须自动或手动部署GuardDuty安全代理才能接收运行时事件。如果您GuardDuty想管理所选账户中所有现有和新 EKS 集群的安全代理的部署和更新，请选择自动管理代理；否则，请参阅手动管理GuardDuty代理 (p. 28)。

API

要有选择地为您的成员账户启用或禁用 EKS 运行时监控，请使用您自己的*### ID* 调用 updateMemberDetectorsAPI 操作。

以下示例说明如何为单个成员账户启用 EKS 运行时监控。要禁用它，请将其ENABLED替换为DISABLED。您也可以传递以空格分隔的账户 ID 列表。

如果将EKS_RUNTIME_MONITORING和都设置StatusENABLED为EKS_ADDON_MANAGEMENT，则GuardDuty允许手动管理安全客户端。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。

如果设置Status为 f ENABLED o EKS_RUNTIME_MONITORING r 但 f EKS_ADDON_MANAGEMENT or 设置Status为DISABLED或未设置全部，则必须手动管理GuardDuty安全客户端。有关更多信息，请参阅手动管理GuardDuty代理。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --acount-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" :
 "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" :
 "ENABLED"}] ]'
```

手动管理GuardDuty代理

本节介绍在启用 EKS 运行时监控后如何管理您的 Amazon EKS 附加GuardDuty代理（代理）。要使用 EKS 运行时监控，必须启用 EKS 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无助于GuardDuty检测潜在威胁或得出调查结果。

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，请确保您已经为您的账户配置了 EKS 运行时监控。如果您不配置 EKS 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，请参阅配置 EKS 运行时监控 (p. 22)：完成以下步骤后，请参阅部署GuardDuty安全代理 (p. 30)。

选择以下访问方法之一来创建 Amazon VPC 终端节点。

Console

创建 VPC 端点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中的虚拟私有云下，选择终端节点。
3. 选择 Create Endpoint（创建端点）。
4. 在创建终端节点页面上，对于 “服务” 类别，选择 “其他终端节点服务”。
5. 在服务名称中，输入**`com.amazonaws.`*`us-east-1`*`.guardduty-data`**。

   确保将 *us-east-1* 替换为正确的区域。此区域必须与属于您的 Amazon Web Services 账户 ID 的 EKS 集群处于同一区域。
6. 选择 “验证服务”。
7. 成功验证服务名称后，选择您的集群所在的 VPC。添加以下策略以限制 VPC 终端节点仅限于指定账户。使用本政策下方`Condition`提供的组织，您可以更新以下策略以限制对终端节点的访问。要为组织中的特定账户 ID 提供 VPC 终端节点支持，请参阅Organization condition to restrict access to your endpoint (p. 29)。

```
{
 "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 终端节点的账户相匹配。以下列表显示了如何与其他 Amazon Web Services 账户 ID 共享 VPC 终端节点：

限制访问您的终端节点的组织条件

- 要指定多个账户来访问 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"
```

- 要限制对组织 ID 的资源访问，请将您的ResourceOrgID资源添加到策略中。

  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，选择您的集群所在的子网。
10. 在安全组下，选择一个从您的 VPC（或 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，请创建一个安全组。

    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

- 调用CreateVpcEndpoint。
- 为参数使用以下值：
  - 在服务名称中，输入**com.amazonaws.*us-east-1*.guardduty-data**。

    确保将 *us-east-1* 替换为正确的区域。此区域必须与属于您的 Amazon Web Services 账户 ID 的 EKS 集群处于同一区域。
  - 对于 DNSOpti ons，通过将其设置为来启用私有 DNS 选项。true
- 有关Amazon Command Line Interface，请参见创建 vpc-端点。

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，请确保您已经设置了先决条件并为您的账户启用了 EKS 运行时监控。如果您不启用 EKS 运行时监控，则GuardDuty安全代理（EKS 附加组件）将无法运行。

选择以下访问方法之一首次部署GuardDuty安全代理。

Console

1. 从以下位置打开 Amazon EKS 控制台：https://console.aws.amazon.com/eks/home#/clusters。
2. 选择您的集群名称。
3. 选择 Add-ons（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 EKS 运行时监控。
6. 在“配置选定的附加组件设置”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 EKS 运行时监控。

7. 为账户配置 EKS 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”。选择下一步。
8. 在 “查看并创建” 页面上，验证所有详细信息，然后选择 “创建”。
9. 导航回集群详细信息并选择资源选项卡。
10. 您可以查看带有前缀的新容器aws-guardduty-agent。

API

您可以使用以下任一选项配置 Amazon EKS 附加代理 (`aws-guardduty-agent`)：

- CreateAddon为您的账户调用。
- 使用以下值作为请求参数：
  - 对于 `addonName`，输入 `aws-guardduty-agent`。
  - 有关支持的信息`addonVersion`，请参阅代理支持的 Kubernetes 版本 GuardDuty (p. 22)。
- 请参阅 create-addon。Amazon Command Line Interface

更新GuardDuty安全代理

在每个版本中，GuardDuty提供EKS 附加代理发布历史记录 (p. 42)。在更新 Amazon EKS 附加版本之前，请参阅代理支持的 Kubernetes 版本 GuardDuty (p. 22)。

要更新您的 Amazon EKS 集群GuardDuty的安全代理，请参阅更新附加组件。

清除资源

在以下情况下，您可能需要移除您的 Amazon EKS 附加代理 (`aws-guardduty-agent`) 并删除 Amazon VPC 终端节点：

- 您想从手动管理代理切换到自动管理代理GuardDuty。
- 你想在 EKS 保护中禁用 EKS 运行时监控。

在这两种情况下，都GuardDuty不会采取任何操作来移除 EKS 附加代理或与您的账户的 EKS 运行时监控配置关联的 Amazon VPC 终端节点。有关更多信息，请参阅重要概念 (p. 22)：

移除亚马逊 EKS 附加代理

要删除手动部署的 Amazon EKS 插件代理 (`aws-guardduty-agent`)，请参阅删除附加组件。

删除 EKS 附加代理不会从 EKS 集群中删除`amazon-guardduty`命名空间。要删除`amazon-guardduty`命名空间，请参阅删除命名空间。

删除亚马逊 VPC 端点

要删除作为`aws-guardduty-agent`部署先决条件创建的 Amazon VPC 终端节点，请参阅删除接口终端节点。

亚马逊 ECR 存储库托管代理 GuardDuty

以下 Amazon ECR 存储库列表用于托管 GuardDuty (`aws-guardduty-agent`) 的 Amazon EKS 附加代理。

Amazon Web Services 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（阿联酋）	601769779514.dkr.ecr.me-central-1.amazonaws.com
欧洲地区（伦敦）	109118265657.dkr.ecr.eu-west-2.amazonaws.com
欧洲地区（爱尔兰）	373421517865.dkr.ecr.us-west-1.amazonaws.com
美国东部（弗吉尼亚州北部）	031903291036.dkr.ecr.us-east-1.amazonaws.com
美国东部（俄亥俄州）	591382732059.dkr.ecr.us-east-2.amazonaws.com
欧洲地区（爱尔兰）	673884943994.dkr.ecr.eu-west-1.amazonaws.com
南美洲（圣保罗）	941219317354.dkr.ecr.sa-east-1.amazonaws.com
欧洲地区（斯德哥尔摩）	366771026645.dkr.ecr.eu-north-1.amazonaws.com
欧洲地区（法兰克福）	409493279830.dkr.ecr.eu-central-1.amazonaws.com
欧洲（苏黎世）	718440343717.dkr.ecr.eu-central-2.amazonaws.com
亚太地区（新加坡）	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
亚太地区（悉尼）	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
亚太地区（雅加达）	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
亚太地区（东京）	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com

Amazon Web Services 区域	亚马逊 ECR 存储库 URI
亚太地区 (首尔)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
亚太地区（大阪）	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
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

评估 EKS 运行时监控的覆盖范围

EKS 运行时监控中的覆盖范围可帮助您确定 EKS 运行时监控、Amazon VPC 终端节点和GuardDuty安全代理的组合状态。如果您在GuardDuty账户中启用了 EKS 运行时监控，确保配置了 VPC 终端节点，并在 EKS 集群中的所有 Amazon Elastic Kubernetes 服务 (Amazon EKS) 节点上运行GuardDuty安全代理，则您的 EKS 集群可能会表明覆盖状态为。`Healthy`如果发现与这些配置中的任何一个相关的问题，则您的 EKS 集群会指示覆盖状态为`Unhealthy`。例如，未配置 VPC 终端节点或部分配置了GuardDuty安全代理的 EKS 集群不在 EKS 运行时监控威胁检测范围内。

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所选账户中运行正常的 EKS 集群占所有 EKS 集群的百分比Amazon Web Services 区域。以下等式将其表示为：

（健康集群/所有集群）*100

如果您是独立账户或成员账户，则可以查看与您的账户关联的所有 EKS 集群的覆盖率统计信息。如果您是GuardDuty管理员，则可以查看与您的成员账户关联的所有 EKS 集群的覆盖率统计信息。

选择一种访问方法来查看您的账户的覆盖范围统计信息。

Console

- 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
- 在“设置”下，选择 EKS 保护。
- 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下可用的覆盖状态汇总的覆盖率统计信息。
  - 您可以按以下列筛选群集列表：
    - `EKS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ACCOUNT_ID`
    - `ADDON_VERSION`

- 您可以按表中任何可用的列对群集列表进行排序。
- 如果您的任何 EKS 集群的覆盖状态为 “不健康”，则 “问题” 列可能包含有关不健康覆盖原因的其他信息。

  有关这些问题的更多信息，请参阅疑难解答覆盖范围问题 (p. 35)。

API/CLI

- 使用您自己的有效探测器 ID、区域和服务终端节点调用 ListCoverageAPI。您可以使用此 API 对集群列表进行筛选和排序。
  - 您可以`filter-criteria`使用以下选项之一更改示例`CriterionKey`：
    - `EKS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `RESOURCE_TYPE`
    - `ACCOUNT_ID`
    - `ADDON_VERSION`
  - 您可以使用以下选项更改示例`AttributeName`：`sort-criteria`
    - `EKS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `ACCOUNT_ID`
    - `ADDON_VERSION`
    - `UPDATED_AT`
  - 您可以更改*####*（最多 50 个）。
  - 你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws --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
```

- 调用GetCoverageStatistics以检索基于的覆盖率聚合统计数据`statisticsType`。
  - 您可以将示例更改`statisticsType`为以下选项之一：
    - `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Amazon资源类型汇总的覆盖范围统计数据。
    - 您可以更改命令`filter-criteria`中的示例。您可以将以下选项用于`CriterionKey`：
      - `EKS_CLUSTER_NAME`
      - `COVERAGE_STATUS`
      - `RESOURCE_TYPE`
      - `ACCOUNT_ID`
      - `ADDON_VERSION`
  - 你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws --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"}}] }'
```

疑难解答覆盖范围问题

如果您的 EKS 集群的覆盖状态为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。

保险问题的结构是Issue type:Extra information。通常，问题将包含可选的额外信息，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，下表提供了解决覆盖范围问题的推荐步骤。

问题类型（前缀）	额外信息	推荐的故障排除步骤
插件创建失败	插件aws-guardduty-agent与集群的当前集群版本不兼容。*ClusterName*不支持指定的插件。	确保你使用的是支持部署 EKS 插件的 Kubernetes 版本之一。aws-guardduty-agent有关更多信息，请参阅代理支持的 Kubernetes 版本 GuardDuty (p. 22)：有关更新 Kubernetes 版本的信息，请参阅更新亚马逊 EKS 集群 Kubernetes 版本。
VPC 端点创建失败	共享 VPC vpcID 不支持创建 *V* PC 终端节点	不可采取行动 目前，EKS 运行时监控不支持共享 VPC。
	#### DNS ### vpcID ### DNS enableDnsSupport # enableDnsHostnames VPC ##########Ec2### ###400######a1b2c3d4-5678-90ab-cdef-example11111##true	确保将以下 VPC 属性设置为true-enableDnsSupport和enableDnsHostnames。有关更多信息，请参阅 VPC 中的 DNS 属性。 如果您使用位于 https://console.aws.amazon.com/vpc/ 的亚马逊 VPC 控制台来创建亚马逊 VPC，请务必同时选择 “启用 DNS 主机名” 和 “启用 DNS 解析”。有关更多信息，请参阅 VPC 配置选项。
本地 EKS 集群	本地前哨集群不支持 EKS 插件。	不可采取行动。 有关更多信息，请参阅Amazon前哨基地上的 Amazon EKS。
未授予 EKS 运行时监控启用权限	*（可选）	1. 如果有关于此问题的额外信息，请修复根本原因并执行下一步。 2. 切换 EKS 运行时监控将其关闭，然后再次打开。确保GuardDuty代理也已部署，无论是自动部署GuardDuty还是手动部署。
EKS 运行时监控启用资源配置正在进行中	*（可选）	不可采取行动。

问题类型（前缀）	额外信息	推荐的故障排除步骤
		启用 EKS 运行时监控后，覆盖状态可能会Unhealthy一直保持到资源配置步骤完成。覆盖状态会定期受到监控和更新。
插件创建失败 插件更新失败 插件状态不正常	EKS 插件问题-AddonIssueCode: AddonIssueMessage	使用问题消息，您可以找出并修复根本原因，然后再次执行该过程。有关插件问题代码的列表，请参见AddonIssue。
任何问题类型	由于授权失败而导致的错误。	切换 EKS 运行时监控将其关闭，然后再次打开。确保GuardDuty代理也已通过自动部署GuardDuty或手动部署。

保险状态变更事件

默认情况下，当 EKS 集群的状态从更改Healthy为Unhealthy或其他状态时，会在您的账户的 Amazon EventBridge 总线中GuardDuty发布此信息。您还可以创建EventBridge规则，以便在任何 Amazon EKS 集群的覆盖状态发生变化时收到通知。有关更多信息，请参阅创建规则。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。此外，您可以使用以下示例通知架构创建自定义事件模式。请务必替换您账户的值。要在您的 EKS 集群的覆盖状态从变Unhealthy为时收到通知Healthy，detail-type应为GuardDuty Runtime Protection Healthy；否则，detail-type应为GuardDuty Runtime Protection Unhealthy。

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Healthy",
  "source": "aws.guardduty",
  "account": "Amazon Web Services ## ID",
  "time": "event timestamp (string)",
  "region": "Amazon Web Services ##",
  "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"
  }
}
```

设置 CPU 和内存监控

启用 EKS 运行时监控并评估覆盖范围以确保已部署 Amazon EKS 附加GuardDuty代理后，您可以设置和查看容器洞察指标。

以下步骤可以帮助您评估已部署的代理与代理的CPU 和内存限制 (p. 22)对比情况GuardDuty：

1. 在亚马逊 EKS 和 Kubernetes 上设置容器见解
2. 亚马逊 EKS 和 Kubernetes 容器洞察指标

使用的运行时事件类型 GuardDuty

GuardDuty安全代理收集以下事件类型并将其发送到GuardDuty后端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了 EKS 运行时监控结果，则可以查看相应的发现细节。

处理事件

字段名称	描述
Process name	观察到的进程的名称。
流程路径	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	辅助 PID 命名空间中进程的进程 ID，主机级 PID 命名空间除外。对于容器内的进程，它是容器内部观察到的进程 ID。
处理用户 ID	执行流程的用户的唯一 ID。
进程 UUID	分配给进程的唯一 ID GuardDuty。
进程 GID	流程组的进程 ID。
进程 EGID	流程组的有效组 ID。
处理 EUID	该进程的有效用户 ID。
流程用户名	执行该流程的用户名。
流程开始时间	创建流程的时间。此字段采用 UTC 日期字符串格式 (`2023-03-22T19:37:20.168Z`)。
流程可执行文件 SHA-256	进程可执行文件的`SHA256`哈希值。
流程脚本路径	已执行的脚本文件的路径。
流程环境变量	可供进程使用的环境变量。只有`LD_PRELOAD`然后`LD_LIBRARY_PATH`才能被收集。
进程当前工作目录 (PWD)	显示该进程的工作目录。
家长流程	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。

容器事件

字段名称	描述
容器名称	容器的名称。
容器用户界面	容器运行时分配的容器的唯一 ID。
容器运行时间	用于运行容器的容器运行时间（例如`docker`或`containerd`）。
容器映像 ID	容器镜像的 ID。
容器镜像名称	容器镜像的名称。

Kubernetes pod 事件

字段名称	描述
Pod ID	Kubernetes 容器的 ID。
容器名称	Kubernetes 容器的名称。
容器命名空间	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
插座类型	表示通信语义的套接字类型。例如，`SOCK_RAW`。
地址家庭	代表与地址相关的通信协议。例如，地址系列用`AF_INET`于 IP v4 协议。
方向标识	连接方向的 ID。
协议号	第 4 层协议号，例如 UDP 的 17 和适用于 TCP 的 6。
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 本地终端节点 IP	连接的本地 IP。
DNS 本地端点端口	连接的端口号。
DNS 负载	包含 DNS 查询和响应的 DNS 数据包的有效负载。

公开活动

字段名称	描述
文件路径	在此事件中打开的文件的路径。
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。

装载事件

字段名称	描述
装载目标	装载源的路径。
装载源	在装载目标处装载的主机路径。
文件系统类型	表示已安装文件系统的类型。
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	硬链接指向的文件的路径。

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的路径。

Dup 活动

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	一个新的文件描述符，它是旧文件描述符的副本。旧文件描述符和新文件描述符都代表相同的打开文件对象。
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。仅在旧文件描述符代表网络套接字时适用。
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。仅在旧文件描述符代表网络套接字时适用。
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。仅在旧文件描述符代表网络套接字时适用。
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。仅在旧文件描述符代表网络套接字时适用。

内存地图事件

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
地址家族	代表与地址相关的通信协议。例如，地址系列用AF_INET于 IP 版本的 4 协议。
插座类型	表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。地址族中通常只有一个协议。例如，地址系列AF_INET只有 IP 协议。

连接活动

字段名称	描述
地址家族	代表与地址相关的通信协议。例如，地址系列用AF_INET于 IP v4 协议。
插座类型	表示通信语义的套接字类型。例如，SOCK_RAW。
协议号	指定地址系列中的特定协议。地址族中通常只有一个协议。例如，地址系列AF_INET只有 IP 协议。
文件路径	如果地址族是，则为套接字文件的路径AF_UNIX。
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。
本地端点端口	连接的端口号。

处理 VM 读取事件

字段名称	描述
Flags	表示控制此事件行为的选项。
目标 PID	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。

处理 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	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 活动

字段名称	描述
目标 PID	目标进程的进程 ID。

字段名称	描述
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。
Flags	表示控制此事件行为的选项。

EKS 附加代理发布历史记录

下表显示了 Amazon EKS 附加GuardDuty代理的发布版本历史记录。

代理版本	容器映像	发布说明	上市日期
v1.2.0	x86_64 (AMD64)：sha256:d610413d662ec0420[illegible]d7f2c08e9f5a077ea307ffdb5d3 Graviton (ARM64)：sha256:174d7ab28b2f95e53[illegible]ad26f602dfe72c2b351a0ef9297a	除了基于 AMD64 的实例外，现在还支持基于 Arm64 的实例。添加并验证了对 Bottlerocket 的支持 支持 Kubernetes 版本 1.27 一般性能增强和稳定性改进。	2023 年 6 月 16 日
v1.1.0	sha256:b19ba3a3c1a508d153263ae2f[illegible]1829303281c	此代理支持的 Kubernetes 版本 GuardDuty (p. 22)，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 8 日
v1.0.0	sha256:e38bdd2b1323e89113f1a31bd[illegible]06b1e4411e	亚马逊 EKS 附加代理的初始版本。	2023 年 3 月 30 日

亚马逊的 Lambda 保护 GuardDuty

在您的Amazon环境中调用Amazon Lambda函数时，Lambda Protection 可帮助您识别潜在的安全威胁。启用 Lambda Protection 后， GuardDuty 开始监控 Lambda 网络活动日志，VPC 流日志 (p. 15)从账户的所有 Lambda 函数开始，包括那些不使用 VPC 网络的日志，并在调用 Lambda 函数时生成。如果 GuardDuty 识别出可疑的网络流量，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。

您可以随时为任何账户或可用Amazon Web Services 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 天试用期内。有关使用情况统计信息的信息，请参阅估算成本 (p. 236)。

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的所有 Lambda 函数的 Amazon VPC 流日志，包括那些不使用 VPC 网络的日志，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 Prot GuardDuty ection 处理的数据量。这将直接影响 Lambda 保护的使用成本。每当 GuardDuty 开始监控额外的网络活动日志时，它都会在发布前至少 30 天向开启了 Lambda Protection 的账户发出通知。

Lambda 保护中的功能

Lambda 网络活动监控

当您启用 Lambda 保护时，会 GuardDuty 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 网络的日志。对于配置为使用 VPC 网络的 Lambda 函数，您无需为 Lambda 创建的弹性网络接口 (ENI) 启用 VPC 流日志 GuardDuty。 GuardDuty 仅对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和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 无法管理您的 Lambda 网络活动日志（包括 VPC 和非 VPC 流日志），也无法在您的账户中访问这些日志。

配置 Lambda 保护

为独立账户配置 Lambda 保护

对于与之关联的账户Amazon Organizations，您可以通过 GuardDuty控制台或 API 指令自动执行此流程，如下一节所述。

选择您的访问方法，为独立账户启用或禁用 Lambda 保护。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中，在设置下选择 Lambda 保护。

3. Lambda 保护页面显示您的账户的当前状态。您可以随时通过选择 “启用” 或 “禁用” 来启用或禁用该功能，然后选择 “确认”。

API

使用您自己的区域探测器 ID 运行 updateDetectorAPI 操作，并将`features`对象`name`和`status`作为`LAMBDA_NETWORK_LOGS`和传递为`ENABLED`或`DISABLED`。

您也可以通过运行以下Amazon CLI命令来启用或禁用 Lambda 网络活动监控。确保使用您自己的有效*### ID*。

Note

以下示例代码启用 Lambda 网络活动监控。要将其禁用，请`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

```
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 GuardDuty 委托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 成员账户无法从其账户修改此配置。委托管理员账户使用管理成员账户Amazon Organizations。委托管理员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 中管理多个账户 GuardDuty。

为委托管理员配置 Lambda 保护

选择一种访问方法来为委托管理员启用或禁用 Lambda 网络活动监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用管理账户证书。
2. 在导航窗格中，在设置下选择 Lambda 保护。
3. 在 Lambda 保护页面上，选择 “启用” 或 “禁用”，然后选择 “确认您的选择”。

API

使用您自己的区域探测器 ID 运行 updateDetectorAPI 操作，并将`features`对象`name`和`status`作为`LAMBDA_NETWORK_LOGS`和传递为`ENABLED`或`DISABLED`。

您可以通过运行以下Amazon CLI命令来启用或禁用 Lambda 网络活动监控。确保使用委托管理员的有效*### ID*。

Note

以下示例代码启用 Lambda 网络活动监控。要将其禁用，请`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --acountids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

为现有成员账户自动启用 Lambda 网络活动监控

Note

此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

作为委托管理员，您可以为组织中的现有成员账户启用 Lambda 网络活动监控。

选择一种访问方法，为组织中的现有成员账户启用 Lambda 网络活动监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托管理员账户证书。
2. 在导航窗格中，在设置下选择 Lambda 保护。
3. 在 Lambda 保护页面上，选择全部启用，为所有成员账户启用 Lambda 网络活动监控。

   默认情况下，此操作会自动打开“自动启用新成员账户 GuardDuty 和 Lambda 网络活动监控”选项。

   如果您无法使用“全部启用”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 (p. 46)。
4. 确认您的选择。现在，您可以查看组织中启用了 Lambda 网络活动监控的活跃成员账户的数量。

API

- 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*### ID* 调用 updateMemberDetectorsAPI 操作。
- 以下示例说明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ENABLED替换为DISABLED。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

  您也可以传递由空格分隔的账户 ID 列表。
- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

为新成员账户自动启用 Lambda 网络活动监控

Note

此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

选择一种访问方法，为加入您的组织的新账户启用 Lambda 网络活动监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托管理员账户证书。
2. 委托管理员可以使用 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。

   请执行下列操作之一：
   - 使用 L ambda 保护页面：
     1. 在导航窗格中，在设置下选择 Lambda 保护。
     2. 在 Lambda 保护页面上，在新成员账户加入您的组织时为其开启自动启用 Lambda 网络活动监控。
   - 使用“帐户”页面：
     1. 在导航窗格中的 Settings 下，选择 Accounts。
     2. 在“帐户”页面上，选择“自动启用首选项”。
     3. 在自动启用 GuardDuty 和设置源首选项配置中，为新成员账户开启自动启用 Lambda 网络活动监控。

API

- 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*### ID* 调用 UpdateOrganizationConfigurationAPI 操作。
- 以下示例说明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 (p. 46)。如果您不想为加入组织的所有新账户启用该功能，请将其设置AutoEnable为NONE。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

  您也可以传递由空格分隔的账户 ID 列表。
- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

有选择地为成员账户启用或禁用 Lambda 网络活动监控

Note

此功能仅适用于通过以下方式管理成员的 GuardDuty 委托管理员Amazon Organizations。

选择您的访问方法，有选择地为组织中的成员账户启用或禁用 Lambda 网络活动监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用委托管理员账户证书。
2. 在导航窗格中的 Settings 下，选择 Accounts。

   在账户页面上，查看 Lambda 网络活动监控列。它指示 Lambda 网络活动监控是否已启用。

3. 选择要为其配置 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

使用您自己的*### ID* 调用 updateMemberDetectorsAPI。

以下示例说明如何为单个成员账户启用 Lambda 网络活动监控。要将其禁用，请ENABLED替换为DISABLED。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

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

您也可以传递由空格分隔的账户 ID 列表。

成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

亚马逊的恶意软件防护 GuardDuty

恶意软件保护通过扫描连接到亚马逊弹性计算云 (Amazon EC2) 实例和容器工作负载的亚马逊弹性区块存储 (Amazon EBS) 卷来帮助您检测恶意软件的潜在存在。恶意软件保护提供扫描选项，您可以在扫描时决定是否要包含或排除特定的 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账户中保留连接到 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恶意软件保护结果时，才会保留快照。

恶意软件保护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。下表显示了两种扫描类型之间的比较。

Factor	GuardDuty-启动恶意软件扫描	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生成表明 Amazon EC2 实例或容器工作负载中可能存在恶意软件的发现时，都会GuardDuty自动对连接到您的可能受影响资源的 Amazon EBS 卷启动无代理恶意软件扫描。有关更多信息，请参阅GuardDuty-启动恶意软件扫描 (p. 55)：	您可以通过提供与您的 Amazon EC2 实例或容器工作负载关联的亚马逊资源名称 (ARN) 来启动按需恶意软件扫描。即使没有为您的资源生成任何GuardDuty搜索结果，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 (p. 62)：
需要配置	要使用GuardDuty启动的恶意软件扫描，必须为您的帐户启用该扫描。有关更多信息，请参阅配置GuardDuty启动的恶意软件扫描 (p. 57)：	要使用按需恶意软件扫描，您的帐户必须已GuardDuty启用。无需进一步配置即可启动按需恶意软件扫描。
等待启动新扫描的时间	每当GuardDuty生成其中一个时调用GuardDuty启动的恶意软件扫描的调查结果 (p. 62)，就会每 24 小时启动一次自动恶意软件扫描。	自上次扫描开始时间起 1 小时后，您可以对同一资源启动按需恶意软件扫描。
30 天免费试用版的可用性	如果您在账户中首次启用了GuardDuty启动的恶意软件扫描，则可以使用 30 天免费试用期*。	对新帐户或现有GuardDuty帐户进行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，恶意软件保护还可以帮助您选择要扫描或跳过的资源。恶意软件防护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`GuardDutyExcluded`标记。它不支持带有用户定义标签的扫描选项。有关更多信息，请参阅带有用户定义标签的扫描选项 (p. 52)：

*创建 EBS 卷快照和保留快照将产生使用成本。有关更多信息，请参阅快照保留 (p. 51)：

恶意软件保护是一项可选的增强功能，其设计方式不会影响您的资源性能。GuardDuty有关恶意软件防护在其中工作原理的信息GuardDuty，请参见恶意软件防护中的功能 (p. 49)。有关不同版本的恶意软件保护可用性的信息Amazon Web Services 区域，请参见区域和终端节点 (p. 292)。

Note

GuardDuty恶意软件防护不支持 ECS Fargate。

恶意软件防护中支持的容量

以下列表描述了恶意软件保护中哪些未加密和加密的 Amazon EBS 卷支持扫描：

- GuardDuty支持未加密和使用客户管理的密钥加密的卷。如果您的 Amazon EBS 卷使用客户管理的密钥加密，则GuardDuty使用相同的密钥对副本 EBS 卷进行加密。
- 对于未加密的 EBS 卷，GuardDuty使用自己的密钥对副本 EBS 卷进行加密。恶意软件保护支持扫描连接到您的 Amazon EC2 实例的 EBS 卷和位于您Amazon账户中的容器工作负载。
- 恶意软件防护不支持扫描使用 EBS 默认Amazon 托管式密钥加密的 E BS 卷。

  它也不支持使用 as 扫描 Amazon EC2 实`productCode`例`marketplace`。如果对这样的 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 (p. 210) 中的 `UNSUPPORTED_PRODUCT_CODE_TYPE`。

默认情况下，如果在加密设置为`true`但未指定 KMS 密钥 ID 的情况下调用 CreateVolumeAPI，则创建的卷将使用 EBS 加密的默认Amazon KMS密钥进行加密。但是，如果未明确提供加密密钥，则可以调用ModifyEbsDefaultKmsKeyId来修改默认密钥。

通过使用以下方法之一，您可以更新 EBS 默认密钥 ID，该密钥 ID 将由选择通过不指定关联的 KMS 密钥 ID 进行加密的新创建的 EBS 卷使用。要修改 EBS 默认密钥 ID，请向您的 IAM 策略添加以下必要权限-`ec2:modifyEbsDefaultKmsKeyId`。

修改亚马逊 EBS 卷的默认 KMS 密钥 ID

请执行下列操作之一：

- 使用 API-您可以使用该 ModifyEbsDefaultKmsKeyIdAPI。有关如何查看卷加密状态的更多信息，请参阅创建 Amazon EBS 卷。
- 使用Amazon CLI命令 — 以下示例修改了默认 KMS 密钥 ID，如果您不提供 KMS 密钥 ID，该密钥 ID 将加密 Amazon EBS 卷。确保将区域替换为您Amazon Web Services 区域的 KM 密钥 ID。

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

上面的命令将生成类似于以下输出的输出：

```
{
  "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。

恶意软件防护中的功能

弹性块存储 (EBS) 卷

本节介绍恶意软件防护（包括GuardDuty启动的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相关的 Amazon EBS 卷。在继续操作之前，请考虑以下自定义：

- 扫描选项 — 恶意软件保护提供指定标签的功能，以便在扫描过程中包括或排除 Amazon EC2 实例和 Amazon EBS 卷。只有GuardDuty启动的恶意软件扫描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，请参阅带有用户定义标签的扫描选项 (p. 52)：

- 快照保留 — 恶意软件保护提供了在您的Amazon账户中保留您的 Amazon EBS 卷快照的选项。默认情况下，此选项处于关闭状态。对于GuardDuty已启动的和按需的恶意软件扫描，您可以选择保留快照。有关更多信息，请参阅快照保留 (p. 51)：

如果GuardDuty生成的发现表明 Amazon EC2 实例或容器工作负载中可能存在恶意软件，并且您已在 GuardDuty Malware Protection 中启用了启动的扫描类型，则可以根据您的扫描选项调用启动的恶意软件扫描。GuardDuty

要对与 Amazon EC2 实例关联的 Amazon EBS 卷启动按需恶意软件扫描，请提供 Amazon 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GuardDuty启动的恶意软件扫描的响应，GuardDuty创建连接到可能受影响资源的相关 EBS 卷的快照，并与共享这些快照。GuardDuty服务账号 (p. 50)接下来，恶意软件保护在服务帐户中根据这些快照创建加密副本 EBS 卷。

扫描完成后，GuardDuty删除加密副本 EBS 卷和 EBS 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 EBS 卷的快照不会被删除并自动保留在您的Amazon账户中。如果未发现恶意软件，则无论快照保留设置如何，都不会保留您的 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期的信息，请参阅 Amazon EBS 定价。

GuardDuty将最多保留其扫描的每个副本 EBS 卷 55 个小时，除非副本 EBS 卷及其恶意软件扫描出现服务中断或故障，届时GuardDuty将保留这样的 EBS 卷不超过七天。延长卷保留期是为了对中断或故障进行分类和解决。GuardDuty恶意软件保护将在解决中断或故障后或延长保留期到期后删除副本 EBS 卷。

GuardDuty服务账户由 Amazon Web Services 区域

创建快照并与GuardDuty服务帐号共享时，将在您的CloudTrail日志中创建一个新事件。此事件指定相应的`snapshotId`和`userId`（该的GuardDuty服务帐户Amazon Web Services 区域）。有关更多信息，请参阅恶意软件防护中的功能 (p. 49)：

以下示例是CloudTrail事件的片段，该代码段显示了请求的请求正文：`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服务帐户。`userId`是GuardDuty服务帐户，取决于所选区域。

Amazon Web Services 区域	区域代码	GuardDuty服务账户 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	178123968615
美国西部（北加利福尼亚）	us-west-1	669213148797
美国西部（俄勒冈州）	us-west-2	447226417196

Amazon Web Services 区域	区域代码	GuardDuty服务账户 ID (**`userId`**)
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
亚太地区（东京）	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
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
欧洲（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	957664736811
亚太地区（雅加达）（选择加入）	ap-southeast-3	452118225523
中东（阿联酋）（选择加入）	me-central-1	828603743433

恶意软件防护中的自定义

本节介绍当恶意软件扫描被调用（按需启动或通过启动）时，如何为 Amazon EC2 实例或容器工作负载自定义扫描选项GuardDuty。

常规设置

快照保留

GuardDuty为您提供在Amazon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。只有在启动扫描之前开启了此设置，快照才会被保留。

扫描开始时，根据您的 EBS 卷的快照GuardDuty生成副本 EBS 卷。扫描完成且账户中的快照保留设置已开启后，只有在发现并生成恶意软件时，EBS 卷的快照才会被保留。恶意软件防护查找类型 (p. 150)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 卷快照时，此步骤会产生使用成本。如果您为账户开启快照保留设置，则当发现恶意软件并保留快照时，您将为此承担使用成本。有关快照成本及其保留期的信息，请参阅 Amazon EBS 定价。

选择以下访问方法之一来开启快照保留设置。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “防护计划” 下，选择 “恶意软件防护”。
3. 在控制台底部选择常规设置。要保留快照，请开启快照保留。

API

1. 运行以下Amazon CLI命令以在GuardDuty恶意软件防护生成发现结果时自动保留快照。

   确保将*###ID##########ID*。`detectorId`
2. 你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

3. 如果要关闭快照保留，请`RETENTION_WITH_FINDING`替换为`NO_RETENTION`。

带有用户定义标签的扫描选项

通过使用GuardDuty启动的恶意软件扫描，您还可以指定标签，在扫描和威胁检测过程中包括或排除 Amazon EC2 实例和 Amazon 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次GuardDuty启动的恶意软件扫描。每个列表最多可以包含 50 个标签。

如果您还没有与您的 EC2 资源关联的用户定义标签，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中标记您的 Amazon EC2 资源或在 Windows 实例的 Amazon EC2 用户指南中标记您的 A mazon EC2 资源。

> 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。它支持全球`GuardDutyExcluded`标签 (p. 54)。

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 Amazon EC2 实例或 Amazon EBS 卷，则可以将任何 Amazon EC2 实例或 Amazon EBS 卷的`GuardDutyExcluded`标签设置为，并且GuardDuty不会对其进行扫描。`true`有关`GuardDutyExcluded`标签的更多信息，请参阅恶意软件保护的服务相关角色权限 (p. 259)。您也可以将 Amazon EC2 实例标签添加到排除列表中。如果您向排除标签列表中添加多个标签，则至少包含其中一个标签的任何 Amazon EC2 实例都将被排除在恶意软件扫描过程之外。

选择一种访问方法，将与 Amazon EC2 实例关联的标签添加到排除列表中。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “防护计划” 下，选择 “恶意软件防护”。
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**配对。提供是可选的**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《适用于 Linux 实例的 Amazon EC2 用户指南》中的标签限制或《适用于 Windows 实例的亚马逊 EC2 用户指南》中的标签限制。

   如果未提供密钥值，且 EC2 实例使用指定密钥进行标记，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

- 更新恶意软件扫描设置，将 EC2 实例或容器工作负载排除在扫描过程之外。

  以下Amazon CLI示例命令将新标签添加到排除标签列表中。确保将示例 d *etector-id ######### ID*。`detectorId`

  `MapEquals`是`Key/Value`对的列表。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --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《适用于 Linux 实例的 Amazon EC2 用户指南》中的标签限制或《适用于 Windows 实例的亚马逊 EC2 用户指南》中的标签限制。

将 EC2 实例包含在恶意软件扫描中

如果您想扫描 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 实例将跳过恶意软件扫描。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一个包含这些标签的 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 (p. 210)：

选择以下访问方法之一，将与 EC2 实例关联的标签添加到包含列表中。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “防护计划” 下，选择 “恶意软件防护”。
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 “包含标记”，然后指定要包含在扫描中的标签**Key**和**Value**配对。提供是可选的**Value**。添加所有包含标签后，选择保存。

Important

标签键和值区分大小写。有关更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的标签限制或《适用于 Windows 实例的亚马逊 EC2 用户指南》中的标签限制。

如果未提供密钥的值，则 EC2 实例使用指定密钥进行标记，则无论标签的分配值如何，EC2 实例都将包含在恶意软件保护扫描过程中。

6. 选择 “添加新的包含标签”，然后指定要包含的标签**Key**和**Value**配对。提供是可选的**Value**。

Important

标签键和值区分大小写。有关更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的标签限制或《适用于 Windows 实例的亚马逊 EC2 用户指南》中的标签限制。

如果未提供密钥值，则 EC2 实例使用指定密钥进行标记，则无论标签的分配值如何，EC2 实例都将包含在恶意软件保护扫描过程中。

API

- 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Amazon CLI示例命令将新标签添加到包含标签列表中。确保将示例 d *etector-id ####### #### ID*。detectorId将示例*TestKey*和替换为*TestValue*Key与您的 EC2 资源关联的标签的和Value对。

  MapEquals是Key/Value对的列表。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --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《适用于 Linux 实例的 Amazon EC2 用户指南》中的标签限制或《适用于 Windows 实例的亚马逊 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。此操作会清除您当前的所有标签。

全球GuardDutyExcluded标签

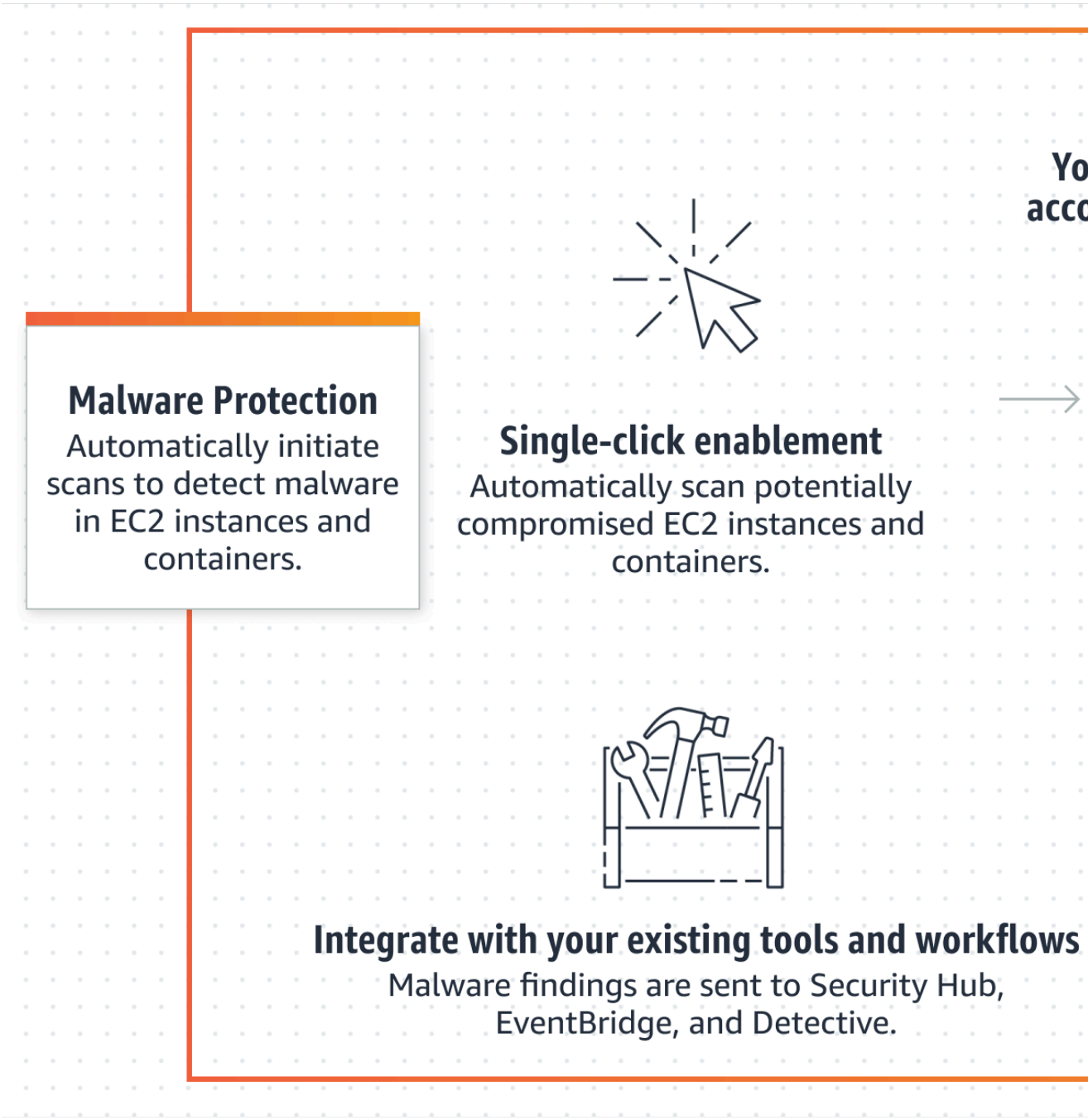
默认情况下，使用GuardDutyScanId标签创建 EBS 卷的快照。请勿删除此标签，因为这样做会GuardDuty阻止访问快照。两种恶意软件防护扫描类型均不扫描GuardDutyExcluded标签设置为的 Amazon EC2 实例或 Amazon EBS 卷。true如果您对此类资源启动任何恶意软件防护扫描，则会生成扫描 ID，但EXCLUDED_BY_SCAN_SETTINGS由于原因会跳过扫描。有关更多信息，请参阅恶意软件扫描期间跳过资源的原因 (p. 210)：

GuardDuty-启动恶意软件扫描

启用GuardDuty启动恶意软件扫描后，只要GuardDuty检测到表明您的 Amazon EC2 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调查结果 (p. 62)，就会GuardDuty自动对连接到可能受影响的 Amazon EC2 实例或容器工作负载的 Amazon Elastic Block Store (Amazon EBS) 卷启动无代理扫描，以检测是否存在恶意软件。使用扫描选项，您可以添加与要扫描的资源关联的包含标记，或者添加与要跳过扫描过程的资源关联的排除标记。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，以便仅在恶意软件保护检测到恶意软件存在时保留 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 (p. 51)：

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 小时会调用一次自动GuardDuty启动的恶意软件扫描。有关如何扫描连接到您的 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 (p. 49)。

下图描述了GuardDuty启动的恶意软件扫描的工作原理。



当发现恶意软件时，GuardDuty生成恶意软件防护查找类型 (p. 150)。如果GuardDuty未在同一资源上生成恶意软件的检测结果，则不会调用GuardDuty启动的恶意软件扫描。您还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 (p. 62)：

30 天免费试用期对账户有何影响 GuardDuty

您可以随时选择为任何帐户或可用Amazon Web Services 区域帐户开启或关闭GuardDuty启动的恶意软件扫描功能。

- GuardDuty首次激活（新GuardDuty帐户）时，GuardDuty启动的恶意软件扫描已开启，并包含在 30 天免费试用期内。
- 现有GuardDuty账户可以首次开启GuardDuty发起的恶意软件扫描，免费试用期为30天。
- 如果您的现有GuardDuty帐户在按需恶意软件扫描正式推出之前一直在使用恶意软件保护，并且该GuardDuty帐户已经使用了定价模式，则无需执行任何操作即可继续使用GuardDuty启动的恶意软件扫描。Amazon Web Services 区域

  Note

  如果您有 30 天的免费试用期，则创建 Amazon EBS 卷快照的使用成本及其保留期仍然适用。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，请参见配置GuardDuty启动的恶意软件扫描 (p. 57)。

配置GuardDuty启动的恶意软件扫描

为独立GuardDuty帐户配置启动的恶意软件扫描

对于与关联的账户Amazon Organizations，您可以通过控制台设置自动执行此流程，如下一节所述。

启用或禁用GuardDuty启动的恶意软件扫描

在下面选择您的访问方式，获取有关为独立帐户启用和禁用GuardDuty启动的恶意软件扫描的说明。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的“防护计划”下，选择“恶意软件防护”。
3. 恶意软件保护窗格列出了您的帐户GuardDuty启动的恶意软件扫描的当前状态。您可以随时启用或禁用它，方法是分别选择“启用”或“禁用”，然后确认您的选择。

API

- 使用您自己的区域探测器 ID 运行 updateDetectorAPI 操作，并将`dataSources`对象`EbsVolumes`设置为`true`或`false`。

  您还可以通过运行以下AmazonAmazon CLI命令使用命令行工具启用或禁用GuardDuty启动的恶意软件扫描。确保使用您自己的有效*### ID*。

  Note

  以下示例代码启用GuardDuty了启动的恶意软件扫描。要禁用它，请将其`true`替换为`false`。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到当前区域的detectorID，也可以使用 API。ListDetectors

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

在多GuardDuty账户环境中配置启动的恶意软件扫描

在多帐户环境中，只有GuardDuty管理员帐户可以配置GuardDuty启动的恶意软件扫描。GuardDuty管理员帐户可以为其成员帐户启用或禁GuardDuty用启动的恶意软件扫描。管理员为成员帐户配置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设置，无法通过控制台修改这些设置。GuardDuty在Amazon 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，请参阅使用以下GuardDuty方式管理账户 Amazon Organizations (p. 225)：

建立可信访问权限以启用GuardDuty启动的恶意软件扫描

如果GuardDuty委派管理员与组织中的管理帐户不同，则管理帐户必须为其组织启用GuardDuty启动的恶意软件扫描。这样，委托管理员就可以创建通过其恶意软件保护的服务相关角色权限 (p. 259)进行管理的内部成员帐户Amazon Organizations。

Note

在指定GuardDuty委派管理员之前，请参阅GuardDuty委派管理员的重要注意事项 (p. 226)。

选择以下访问方法之一，以允许GuardDuty委托管理员为成员帐户启用恶意软件防护。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   要登录，请使用您所在Amazon Organizations组织的管理帐户。
2. 在导航窗格中，选择保护计划。
3. a. 如果您尚未指定委派管理员，则：

      在 “设置” 页面的授权管理员下，输入您要指定用于管理组织中的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管理账户不同的委托管理员，那么：

         在 “设置” 页面的 “委派管理员” 下，打开 “权限” 设置。此操作将允许委托管理员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帐户相同的委托管理员，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，请参阅自动为所有组织成员帐户启用GuardDuty启动的恶意软件扫描 (p. 59)：

         Tip

         如果委派管理员与您的管理帐户不同，则必须向委派管理员提供权限，以允许对成员帐户启用GuardDuty启动的恶意软件扫描。
4. 如果您想允许委派管理员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Amazon Web Services 区域，然后重复上述步骤。

API

1. 使用您的管理账户证书，运行以下命令：

   ```
   aws organizations enable-aws-service-access --service-principal malware-
   protection.guardduty.amazonaws.com
   ```
2. （可选）要为非委派管理员的管理帐户启用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保护的服务相关角色权限 (p. 259)明确创建，然后启用委托管理员GuardDuty发起的恶意软件扫描，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管理员Amazon Web Services 区域。如果您已将某个账户指定为某个区域的委派管理员，则该账户必须是您在所有其他区域的委派管理员。对所有其他区域重复上述步骤。

自动为所有组织成员帐户启用GuardDuty启动的恶意软件扫描

Note

此功能仅适用于通过管理成员的GuardDuty委托管理员Amazon Organizations。

您可以为组织中的所有成员帐户启用GuardDuty启动的恶意软件扫描。

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的 “防护计划” 下，选择 “恶意软件防护”。

   恶意软件保护页面列出了管理员帐户和成员帐户GuardDuty启动的恶意软件扫描的当前状态。
3. 选择 “启用” 以GuardDuty启用管理员帐户启动的恶意软件扫描。
4. 选择 “全部启用”，只需单击一下即可对所有成员帐户启用GuardDuty启动的恶意软件扫描，然后确认您的选择。然后，控制台将显示成功启用的成员帐户的数量。

   启用后，您可以从左侧导航窗格中的 “帐户” 中管理成员帐户。

   Note

   此操作还启用 “自动启用” 功能，可自动为组织内未来的成员帐户启用GuardDuty启动的恶意软件扫描。

有选择地启用或禁用对成员GuardDuty帐户发起的恶意软件扫描

Note

此功能仅适用于通过管理成员的管理GuardDuty员Amazon Organizations。

在下方选择您的访问方式，获取有关有选择地为成员帐户启用和禁用GuardDuty发起的恶意软件扫描的说明。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中，选择 Accounts (账户)。

   Note

   在 “帐户” 表中，查看 “恶意软件防护” 列。绿色勾号图标表示恶意软件防护已启用，蓝色的短划线图标表示已禁用。如果此列为空，则该帐户没有资格获得恶意软件防护。您也可以按 “启用” 或 “已禁用” 进行筛选。
3. 选择要为其配置GuardDuty启动的恶意软件扫描的帐户。从 “操作” 菜单中选择 “启用恶意软件防护” 或 “禁用恶意软件防护”，然后确认您的选择以更改所选帐户的设置。该表格将自动更新以显示您的更改。

API

要有选择地启用或禁用对您的成员帐户GuardDuty发起的恶意软件扫描，请使用您自己的### ID 调用 updateMemberDetectorsAPI 操作。

以下示例显示如何为单个成员帐户启用GuardDuty启动的恶意软件扫描。要禁用它，请将其ENABLED替换为DISABLED。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

Note

您也可以传递以空格分隔的账户 ID 列表。

成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

要有选择地启用或禁用对您的成员帐户GuardDuty发起的恶意软件扫描，请使用您自己的### ID 运行 updateMemberDetectorsAPI 操作。以下示例显示如何为单个成员帐户启用GuardDuty启动的恶意软件扫描。要禁用它，请将其true替换为false。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

Note

您也可以传递以空格分隔的账户 ID 列表。

成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

为GuardDuty组织中新添加的帐户配置启动的恶意软件扫描

新添加的成员帐户必须先启用，GuardDuty然后才能选择 “启用” 或 “禁用GuardDuty启动的恶意软件扫描”。有关更多信息，请参阅步骤 3 – 接受邀请 (p. 232)：

受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。在下方选择您的访问方式，获取有关如何查看您的账户GuardDuty发起的恶意软件扫描的当前状态的说明。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中，选择 Accounts (账户)。
3. 选择自动启用并查看GuardDuty启动的恶意软件扫描的状态。
4. 您可以为新成员帐户启用或禁GuardDuty用启动的恶意软件扫描。
5. 选择 “更新设置” 以确认您的选择。

API

Important

默认情况下，新检测器会自动启用GuardDuty启动的恶意软件扫描。

如果您是首次在新帐户上启用启动GuardDuty的恶意软件扫描的GuardDuty管理员，并且不希望默认启用GuardDuty启动的恶意软件扫描，则可以通过使用可选dataSources对象修改 createDetectorAPI 操

作来将其禁用。以下示例使用启用新GuardDuty检测器Amazon CLI，但禁用GuardDuty了启动的恶意软件扫描。

```
aws guardduty create-detector --enable --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "AutoEnable": "NEW"}]'
```

- 要有选择地为您的新成员帐户启用或禁用GuardDuty启动的恶意软件扫描，请使用您自己的### ID 调用 UpdateOrganizationConfigurationAPI 操作。
- 以下示例显示如何为单个成员帐户启用GuardDuty启动的恶意软件扫描。要禁用它，请将其ENABLED替换为DISABLED。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

  Note

  您也可以传递以空格分隔的账户 ID 列表。
- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

对通过GuardDuty邀请管理的组织中的现有帐户启用启动的恶意软件扫描

必须在成员GuardDuty帐户中创建恶意软件保护服务相关角色 (SLR)。管理员无法在不受管理GuardDuty的成员帐户中启用启动的恶意软件扫描功能。Amazon Organizations

目前，您可以通过GuardDuty控制台 https://console.aws.amazon.com/guardduty/ 执行以下步骤，为现有成员账户启用GuardDuty启动的恶意软件扫描。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在您的管理员帐户中，选择导航窗格中的帐户。
3. 选择想要启用GuardDuty启动的恶意软件扫描的成员帐户，然后选择操作。
4. 选择 “取消关联成员”。
5. 在您的会员帐户中，在导航窗格的 “保护计划” 下选择 “恶意软件防护”。
6. 选择 “启用恶意软件防护”。GuardDuty将为成员帐户创建 SLR。有关 SLR 的更多信息，请参阅恶意软件保护的服务相关角色权限 (p. 259)。
7. 在您的管理员帐户中，选择导航窗格上的帐户。
8. 选择需要重新添加到组织的成员账户。
9. 选择操作，然后选择添加成员。

API

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上运行 DisassociateMembersAPI。
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。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --data-
sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

3. 使用管理员帐户运行 CreateMembersAPI 以将成员重新添加到组织中。

调用GuardDuty启动的恶意软件扫描的调查结果

当GuardDuty检测到 Amazon EC2 实例或容器工作负载上存在恶意软件的可疑行为时，将调用GuardDuty启动的恶意软件扫描。在以下搜索GuardDuty结果列表中，某些发现结果仅在出站时才能启动扫描。

- Backdoor:EC2/C&CActivity.B (p. 95)
- Backdoor:EC2/C&CActivity.B!DNS (p. 96)
- Backdoor:EC2/DenialOfService.Dns (p. 96)
- Backdoor:EC2/DenialOfService.Tcp (p. 97)
- Backdoor:EC2/DenialOfService.Udp (p. 97)
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts (p. 97)
- Backdoor:EC2/DenialOfService.UnusualProtocol (p. 98)
- Backdoor:EC2/Spambot (p. 98)
- CryptoCurrency:EC2/BitcoinTool.B (p. 99)
- CryptoCurrency:EC2/BitcoinTool.B!DNS (p. 100)
- Impact:EC2/AbusedDomainRequest.Reputation (p. 101)
- Impact:EC2/BitcoinDomainRequest.Reputation (p. 101)
- Impact:EC2/MaliciousDomainRequest.Reputation (p. 102)
- Impact:EC2/PortSweep (p. 102)
- Impact:EC2/SuspiciousDomainRequest.Reputation (p. 103)
- Impact:EC2/WinRMBruteForce (p. 103)（仅限出境）
- Recon:EC2/Portscan (p. 104)
- Trojan:EC2/BlackholeTraffic (p. 105)
- Trojan:EC2/BlackholeTraffic!DNS (p. 105)
- Trojan:EC2/DGADomainRequest.B (p. 105)
- Trojan:EC2/DGADomainRequest.C!DNS (p. 106)
- Trojan:EC2/DNSDataExfiltration (p. 106)
- Trojan:EC2/DriveBySourceTraffic!DNS (p. 107)
- Trojan:EC2/DropPoint (p. 107)
- Trojan:EC2/DropPoint!DNS (p. 107)
- Trojan:EC2/PhishingDomainRequest!DNS (p. 108)
- UnauthorizedAccess:EC2/RDPBruteForce (p. 109)（仅限出境）
- UnauthorizedAccess:EC2/SSHBruteForce (p. 109)（仅限出境）
- UnauthorizedAccess:EC2/TorClient (p. 110)
- UnauthorizedAccess:EC2/TorRelay (p. 110)

按需恶意软件扫描

按需恶意软件扫描可帮助您检测连接到 Amazon EC2 实例的亚马逊弹性区块存储 (Amazon EBS) 卷上是否存在恶意软件。无需配置，您可以通过提供要扫描的 Amazon 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 API 启动按需恶意软件扫描。在启动按需恶意软件扫描之

前，您可以设置首选快照保留 (p. 51)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。按照生成的恶意软件保护查找类型的建议补救措施后，如果要对同一资源启动扫描，则可以在距离上一次扫描开始时间过去 1 小时后启动按需恶意软件扫描。

  按需恶意软件扫描不要求自上次恶意软件扫描启动之日起已过 24 小时。在对同一资源启动按需恶意软件扫描之前，应该已经过去了一个小时。为避免在同一 EC2 实例上重复恶意软件扫描，请参阅重新扫描同一个亚马逊 EC2 实例 (p. 64)。

  Note

  按需恶意软件扫描不包含在 30 天免费试用GuardDuty期内。使用费用适用于每次恶意软件扫描时扫描的 Amazon EBS 总容量。有关更多信息，请参阅亚马逊GuardDuty定价。有关创建 Amazon EBS 卷快照的成本及其保留期的信息，请参阅 Amazon EBS 定价。

按需恶意软件扫描的工作原理

启动按需恶意软件扫描后，GuardDuty创建连接到您的 Amazon EC2 实例的 Amazon EBS 卷的快照，该实例已为扫描提供了亚马逊资源名称 (ARN)，并将这些快照与共享。GuardDuty服务账号 (p. 50)GuardDuty根据GuardDuty服务帐户中的快照创建加密副本 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 (p. 49)。

如果发现恶意软件并且您启用了快照保留设置，则您的 EBS 卷的快照将自动保留在您的Amazon Web Services 账户中。按需恶意软件扫描会生成恶意软件防护查找类型 (p. 150). 如果未找到恶意软件，无论快照保留设置如何，您的 EBS 卷的快照都会被删除。

默认情况下，使用`GuardDutyScanId`标签创建 EBS 卷的快照。请勿删除此标签，因为这样做会GuardDuty阻止访问快照。两种恶意软件防护扫描类型均不扫描`GuardDutyExcluded`标签设置为的 Amazon EC2 实例或 Amazon EBS 卷。`true`如果您对此类资源启动任何恶意软件防护扫描，则会生成扫描 ID，但`EXCLUDED_BY_SCAN_SETTINGS`由于原因会跳过扫描。有关更多信息，请参阅恶意软件扫描期间跳过资源的原因 (p. 210)：

Amazon Organizations服务控制策略-拒绝访问

使用中的Amazon Organizations服务控制策略 (SCP)，委托管理员可以限制权限并拒绝诸如对您的账户拥有的 Amazon EC2 实例启动按需恶意软件扫描之类的操作。

作为GuardDuty成员账户，当您启动 Amazon EC2 实例的按需恶意软件扫描时，您可能会收到错误。您可以连接管理账户，了解为何为您的成员账户设置了 SCP。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，您可以代表在账户中设置了以下先决条件的活跃成员帐户启动按需恶意软件扫描。中的独立账户和活跃成员账户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Amazon Web Services 区域位置启用。
- 确保已连接到 IAM 用户或 IAM 角色。Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)您将需要与 IAM 用户或 IAM 角色关联的访问密钥和私有密钥。
- 作为委托管理员，您可以选择代表活跃成员帐户启动按需恶意软件扫描。
- 如果您是成员账户且恶意软件保护的服务相关角色权限 (p. 259)不存在，则启动对属于您账户的 Amazon EC2 实例的按需恶意软件扫描，将自动创建 SLR 用于恶意软件保护。

Important

确保在恶意软件扫描（无论是GuardDuty启动扫描还是按需扫描）仍在进行时，没有人删除恶意软件保护的 SLR 权限。这样做会阻止扫描成功完成并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 小时内未对同一资源启动任何扫描；否则，将对其进行重复数据消除。有关更多信息，请参阅重新扫描相同的资源 (p. 64)：

启动按需恶意软件扫描

选择以下访问方法之一启动按需恶意软件扫描。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   使用以下两个选项之一启动扫描：

   a. 使用 “恶意软件防护” 页面：

      i. 在导航窗格中的 “防护计划” 下，选择 “恶意软件防护”。
      ii. 在恶意软件保护页面上，提供要启动扫描的 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 A mazon 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”。

2. 使用任一方法成功启动扫描后，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GuardDuty恶意软件防护中的扫描状态和结果 (p. 65)：

API

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`返回`scanId`。调用 DescribeMalwareScansmonitor 启动的扫描进度。

[1] 有关您的亚马逊 EC2 实例 ARN 格式的信息，请参阅亚马逊资源名称 (ARN)。对于 Amazon EC2 实例，您可以使用以下示例 ARN 格式，替换分区、区域、Amazon Web Services 账户 ID 和 Amazon EC2 实例 ID 的值。有关您的实例 ID 长度的信息，请参阅资源 ID。

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

重新扫描同一个亚马逊 EC2 实例

无论是GuardDuty启动扫描还是按需扫描，您都可以在上一次恶意软件扫描开始时间后 1 小时后在同一 EC2 实例上启动新的按需恶意软件扫描。如果新的恶意软件扫描在上一次恶意软件扫描启动后的 1 小时内启动，则您的请求将导致以下错误，并且不会为此请求生成任何扫描 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 (p. 64)。

要跟踪恶意软件扫描的状态，请参见监控GuardDuty恶意软件防护中的扫描状态和结果 (p. 65)。

监控GuardDuty恶意软件防护中的扫描状态和结果

您可以监视每次GuardDuty恶意软件防护扫描的扫描状态。扫描状态的可能值为`CompletedRunningSkipped`、和`Failed`。

扫描完成后，将为状态为的扫描填充扫描结果`Completed`。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`GuardDuty initiated`或`On demand`。

每次恶意软件扫描的扫描结果的保留期为 90 天。选择以下访问方法之一来跟踪恶意软件扫描的状态。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中，选择恶意软件扫描。
3. 您可以按筛选条件中提供的以下属性筛选恶意软件扫描。

   - 扫描 ID
   - 账号 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，请参见正在寻找细节 (p. 78)。

API

- 恶意软件扫描获得扫描结果后，您可以根据、`EC2_INSTANCE_ARN`、、`SCAN_IDACCOUNT_IDSCAN_TYPEGUARDDUTY_FINDING_IDSCAN_STATUS`、和筛选恶意软件扫描`SCAN_START_TIME`。

  `GUARDDUTY_FINDING_ID`筛选条件在GuardDuty启动时`SCAN_TYPE`可用。有关任何筛选条件的信息，请参见正在寻找细节 (p. 78)。
- 您可以在下面的命令中更改*`######`*。目前，您可以逐`CriterionKey`一进行筛选。的选项`CriterionKey`有`EC2_INSTANCE_ARNSCAN_ID`、`ACCOUNT_ID`、`SCAN_TYPEGUARDDUTY_FINDING_IDSCAN`和`SCAN_START_TIME`。

  如果您使用与以下`CriterionKey`相同的内容，请确保将示例`EqualsValue`替换为您自己的有效Amazon*`##ID`*。

  用你自己的有效示例`detector-id`替换这个例子*`detector-id`*。*`############ 50 ###### ##`*`AttributeName`是强制性的，必须是`scanStartTime`。

```
aws guardduty describe-malware-scans --detector-id 60b87779336485625554d637e0e4bb3b2
 --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发现的详细信息（如果`Infected`）。

Note

对恶意软件扫描进行筛选`Scan type = GuardDuty initiated`将仅生成在引入该`Scan type`字段之后启动的扫描GuardDuty。目前，该过滤器的结果将返回`null`。

恶意软件保护配额

恶意软件保护具有该功能使用的各种资源的默认可用性如下。

范围	默认值	注释
提取和分析压缩或存档文件中的数据	5	存档文件中允许的最大嵌套层数。
威胁数量	32	您可以在发现面板中查看的最大威胁数。GuardDuty恶意软件防护可能已检测到更多威胁名称。如果检测到的威胁名称数量大于默认值，则可以通过在GuardDuty控制台的详细信息面板中选择查找名称下方的查找 ID 来查看 JSON 详细信息。
每个实例每次扫描的 EBS 容量	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，GuardDuty恶意软件保护会`deviceName`按字母顺序排序，然后选择前 11 个 EBS 卷。
支持的加密类型	未加密并使用客户管理的密钥加密。	恶意软件保护支持未加密和使用客户托管密钥加密的 EBS 卷。恶意软件防护不支持使用 EBS 托管密钥加密的 EBS 卷。
EBS 卷大小	1024 GB	GuardDuty恶意软件防护可以在每个区域扫描的最大 EBS 卷大小（以 GB 为单位）。
支持的文件系统类型	GuardDuty恶意软件防护可以扫描以下文件系统类型： • 新技术文件系统 (NTFS) • X 文件系统 (XFS) • 二次扩展 (ext2) 文件系统 • 第四个扩展 (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	您可以添加的最大资源标签数，用于自定义恶意软件扫描选项设置。有关更多信息，请参阅带有用户定义标签的扫描选项 (p. 52)：

范围	默认值	注释
调查结果保留期	90	GuardDuty保留调查结果的最大天数。有关最新信息，请参见亚马逊的配额 GuardDuty (p. 288)。
恶意软件扫描保留期	90	GuardDuty恶意软件防护保留扫描历史记录的最大天数。有关查看近期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 (p. 65)。
按需恶意软件扫描的每秒交易量 (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发限制	1	每个区域每秒可以启动的并发恶意软件按需扫描请求的数量。

GuardDutyRDS 防护

亚马逊的 RDS Protection GuardDuty 会分析和分析 RDS 登录活动，以确定您的亚马逊 Aurora 数据库是否存在潜在的访问威胁（亚马逊 Aurora MySQL 兼容版和 Aurora PostgreSQL 兼容版）。此功能允许您识别潜在的可疑登录行为。RDS Protection 不需要额外的基础设施；它的设计旨在不影响数据库实例的性能。

当 RDS Protection 检测到表明您的数据库受到威胁的潜在可疑或异常登录尝试时，GuardDuty会生成一个新的调查结果，其中包含有关可能受感染的数据库的详细信息。

您可以随时在亚马逊GuardDuty提供该功能的任何账户启用或禁用 RDS 保护功能。Amazon Web Services 区域现有GuardDuty账户可以启用 RDS 保护，试用期为 30 天。对于新GuardDuty账户，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 (p. 236)：

> Note
>
> 未启用 RDS 保护功能时，GuardDuty既不会提取 RDS 登录活动，也不会检测异常或可疑的登录行为。

有关尚GuardDuty不支持 RDS 保护的Amazon Web Services 区域位置的信息，请参阅特定区域功能的可用性 (p. 292)。

支持的亚马逊 Aurora 数据库

下表显示了支持的 Aurora 数据库版本。

Amazon Aurora 数据库引擎	支持的引擎版本
Aurora MySQL	• 2.10.2 或更高版本 • 3.2.1 或更高版本
Aurora PostgreSQL	• 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

RDS 保护如何使用 RDS 登录活动监控

亚马逊的 RDS 保护GuardDuty可帮助您保护账户中支持的亚马逊 Aurora (Aurora) 数据库。启用 RDS 保护功能后，GuardDuty立即开始监控来自您账户中的 Aurora 数据库的 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，以前看不见的外部参与者未经授权访问您账户中的 Aurora 数据库。当您首次启用 RDS Protection 或新创建的数据库实例时，需要一段学习时间才能为正常行为建立基准。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相关的异常登录信息。有关更多信息，请参阅RDS 登录活动监控 (p. 72)：

当 RDS Protection 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会生成一个新的发现，其中包含有关可能受感染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 (p. 153)：如果您禁用 RDS 保护，将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不管理您的支持的数据库 (p. 68)或 RDS 登录活动，也不会向您提供 RDS 登录活动。

为独立账户配置 RDS 保护

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 在导航窗格中的设置下，选择 RDS 保护。
3. R DS 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” 来启用或禁用该功能。确认您的选择。

API

使用您自己的区域探测器 ID 运行 updateDetectorAPI 操作，并将`features`对象`name`作为`RDS_LOGIN_EVENTS`和`status`传递`ENABLED`或`DISABLED`。

您也可以通过运行以下Amazon CLI命令来启用或禁用 RDS 保护。确保使用您自己的有效*### ID*。

Note

以下示例代码启用 RDS 保护。要禁用它，请将其`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

在多账户环境中配置 RDS 保护

在多账户环境中，只有GuardDuty委托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成员账户无法从其账户修改此配置。委托管理员帐户使用以下方式管理其成员帐户Amazon Organizations。该委托管理员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

为委派管理员配置 RDS 保护

选择一种访问方法为委派管理员配置 RDS 登录活动监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用管理账户证书。
2. 在导航窗格中，选择 RDS 保护。

3. 在 RDS 保护页面上，选择启用或禁用以启用或禁用 RDS 登录活动监控。

   确认您的选择。

API

使用您自己的区域探测器 ID 运行 updateDetectorAPI 操作，并将`features`对象`name`和`status`作为`RDS_LOGIN_EVENTS`和`ENABLED`或传递`DISABLED`。

您可以通过运行以下Amazon CLI命令来启用或禁用 RDS 保护。确保使用委托管理员的有效*### ID*。

Note

以下示例代码启用 RDS 保护。要禁用它，请将其`ENABLED`替换为`DISABLED`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
acountids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

为现有成员账户自动启用 RDS 保护

Note

此功能仅适用于通过管理成员的GuardDuty委托管理员Amazon Organizations。

选择一种访问方法，为组织中的现有成员账户启用 RDS 保护功能。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户证书。
2. 在导航窗格中的设置下，选择 RDS 保护。
3. 在 RDS 保护页面上，选择全部启用以为所有成员账户启用 RDS 登录活动监控。

   默认情况下，此操作会自动启用 “自动启用GuardDuty新成员账户的 RDS 登录活动监控” 选项。

   如果您无法使用 “全部启用” 选项，请参阅有选择地为成员账户启用或禁用 RDS 保护 (p. 72)。
4. 确认您的选择。现在，您可以查看组织中启用 RDS 登录活动监控的活跃成员账户的数量。

API

- 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*### ID* 调用 updateMemberDetectorsAPI 操作。
- 以下示例显示如何为单个成员账户启用 RDS 保护。要禁用它，请将其`ENABLED`替换为`DISABLED`。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"name": "RDS_LOGIN_EVENTS", "status":
 "ENABLED"}]'
```

Note

您也可以传递以空格分隔的账户 ID 列表。

- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

为新成员账户自动启用 RDS 保护

Note

此功能仅适用于通过管理成员的GuardDuty委托管理员Amazon Organizations。

选择一种访问方法，为加入组织的新账户启用 RDS 登录活动。

Console

委托管理员可以使用 RDS Prot ection 或 Accounts 页面，通过控制台在组织中启用新成员账户。

为新成员账户自动启用 RDS 保护

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户证书。
2. 请执行下列操作之一：
   - 使用 R DS 保护页面：
     1. 在导航窗格中的设置下，选择 RDS 保护。
     2. 在 RDS 保护页面上，为新成员账户开启自动启用 RDS 登录活动监控。
     3. 在确认对话框中选择确认。
   - 使用“帐户”页面：
     1. 在导航窗格中的 Settings 下，选择 Accounts。
     2. 在“帐户”页面上，选择“自动启用”首选项。
     3. 在自动启用GuardDuty和设置源首选项配置中，为新成员账户开启自动启用 RDS 登录活动监控。

API

- 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*### ID* 调用 UpdateOrganizationConfigurationAPI 操作。
- 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，请参见有选择地为成员账户启用或禁用 RDS 保护 (p. 72)。如果您不想为所有加入组织的新账户启用此功能，autoEnable请将其设置为NONE。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的“设置”页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

Note

您也可以传递以空格分隔的账户 ID 列表。

- 成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

有选择地为成员账户启用或禁用 RDS 保护

Note

此功能仅适用于通过管理成员的GuardDuty委托管理员Amazon Organizations。

选择一种访问方法，有选择地启用或禁用对组织中成员账户的 RDS 登录活动的监控。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   确保使用委派管理员账户证书。
2. 在导航窗格中的 Settings 下，选择 Accounts。

   在账户页面上，查看 RDS 登录活动列以了解您的成员账户的状态。
3. 启用或禁用 RDS 登录活动

   选择要为 RDS 保护配置的账户。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 RDS 登录活动，然后选择相应的选项。

API

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*### ID* 调用 updateMemberDetectorsAPI 操作。

以下示例显示如何为单个成员账户启用 RDS 保护。要禁用它，请将其ENABLED替换为DISABLED。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

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

Note

您也可以传递以空格分隔的账户 ID 列表。

成功执行代码后，它会返回一个空列表UnprocessedAccounts。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 以及问题摘要。

RDS 保护中的功能

RDS 登录活动监控

RDS 登录活动记录了支持的亚马逊 Aurora 数据库 (p. 68)在您的Amazon环境中成功和失败的登录尝试。为了帮助您保护数据库，GuardDutyRDS Protection 会持续监控登录活动，以防出现潜在的可疑登录尝试。例如，对手可能试图通过猜测数据库的密码来暴力访问 Amazon Aurora 数据库。

启用 RDS 保护功能后，GuardDuty会自动开始直接从 Aurora 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生成调查结果，其中包含有关可能受感染的数据库的详细信息。当您首次启用 RDS Protection 或新创建的数据库实例时，需要一段学习时间才能为正常行为建立基准。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相关的异常登录信息。

RDS 保护功能不需要任何额外设置；它不会影响任何现有的 Amazon Aurora 数据库配置。GuardDuty不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账户加入您的组织时为其自动启用 RDS 保护功能，则此操作会自动GuardDuty为这些新成员账户启用。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GuardDutyRDS 防护 (p. 68)。

亚马逊的Amazon S3 保护 GuardDuty

S3 保护Amazon GuardDuty允许监控对象级 API 操作，以识别 S3 存储桶中数据的潜在安全风险。

GuardDuty 通过分析Amazon CloudTrail管理事件和 S3 数据事件来监控针对，并监控针对，并监控针 CloudTrail 对 Amazon S3 资源的威胁。这些数据源监控不同类型的活动，例如，S3 的 CloudTrail 管理事件包括列出或配置 S3 存储桶的操作`ListBuckets`，例如`DeleteBuckets`、和`PutBucketReplication`。S3 的数据事件示例包括对象级 API 操作，例如`GetObject`、`ListObjects`、`DeleteObject`、和`PutObject`。

GuardDuty 默认情况下，所有已启用且不可配置的帐户的 CloudTrail 管理事件监控处于启用状态 GuardDuty 。 CloudTrail S3 数据事件日志是中的可配置数据来源 GuardDuty。默认情况下，为新检测器启用 S3 保护，对于在添加 S3 保护之前创建的帐户，必须手动启用此数据源。本主题涵盖了启用或禁用 S3 数据事件监控的过程。

强烈建议您启用 S3 保护 GuardDuty。如果禁用该功能， GuardDuty 则无法全面监控或生成发现结果，以发现对存储在 S3 存储桶中的数据的可疑访问。

如何 GuardDuty 使用 S3 数据事件

中的 S3 保护功能 GuardDuty 指是否将 S3 数据事件作为数据来源启用 GuardDuty。启用 S3 数据事件监控后， GuardDuty 立即开始分析来自您的所有 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Amazon CloudTrailS3 的数据事件 (p. 77)：

GuardDuty 不处理对您已公开访问的对象的请求，但会在存储段公开访问时提醒您。当基于 S3 数据事件监控 GuardDuty 检测到威胁时，它会生成安全发现。有关 GuardDuty 可以为 Amazon S3 生成的发现类型的信息，请参阅GuardDuty S3 查找类型 (p. 157)。

如果您禁用 S3 保护，则 GuardDuty 立即停止使用此数据源并停止监控对存储在 S3 存储桶中的数据的访问。

为独立账户配置 S3 保护

对于关联的帐户Amazon Organizations，可以通过控制台设置自动执行此过程，如下一节所述。

在添加 S3 保护 GuardDuty 之前使用的账户可以通过控制台或`UpdateDetector` API 操作 GuardDuty 进行配置来启用新数据源。

要将 Amazon S3 数据事件配置为账户的数据源，请参阅以下配置选项。

启用或禁用 S3 保护

在下面选择您的访问方法，获取有关为独立账户启用或禁用 S3 保护的说明。

Console

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中，在设置下选择 S3 保护。
3. S 3 保护窗格列出了您的账户的 S3 保护的当前状态。您可以随时启用或禁用它，分别选择 “启用” 或 “禁用”，然后确认您的选择。

API

- 使用您自己的区域检测器 ID 运行 updateDetectorAPI 操作，并将"S3 Logs":"enable"设置为 true 或 false 的dataSources对象传递。

  您也可以通过运行以下Amazon CLIAmazon 命令使用命令行工具启用或禁用 S3 保护。务必使用您自己的有效探测器 ID。

  Note

  以下示例代码启用 S3 保护。要将其禁用，请true替换为false。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
data-sources '{"S3Logs":{"Enable":true}}'
```

在多账户环境中配置 S3 保护

在多账户环境中，只有 GuardDuty 管理员帐户才能配置 S3 保护。 GuardDuty 管理员账户可以为其成员账户启用或禁用 S3 保护。 GuardDuty 成员账户无法启用或禁用此数据源。

GuardDuty 在Amazon Organizations支持下管理其成员账户的管理员账户可以选择在组织中的所有新账户上自动启用 S3 保护。有关更多信息，请参阅使用以下GuardDuty方式管理账户 Amazon Organizations (p. 225)：

自动为组织成员账户启用 S3 保护

Note

此功能仅适用于通过注册的 GuardDuty 成员的管理员Amazon Organizations。

1. 使用您的管理员帐户执行此步骤。

   通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Settings 下，选择 Accounts。
3. 确保 “的自动启 GuardDuty 用” 已开启。如果已关闭，则可以通过从标题中选择 “启用” 或选择 “自动启用为关闭” 来启用。此功能将自动 GuardDuty 为组织内的新成员账户启用，必须启用该功能才能自动启用 S3 保护。
4. 开启自动启用后，除了 GuardDuty 通过选择 S3 保护切换图标启用外，您还可以为新成员启用 S3 保护。 GuardDuty 选择 “更新设置” 进行确认。

在成员账户中选择性地启用或禁用 S3 保护

在下面选择您的访问方法，获取有关为成员账户启用或禁用 S3 保护的说明。

Console

为所有账户启用 S3 保护

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 如果您想同时为所有账户启用 S3 保护，请从导航窗格中选择 S3 保护。

3. 您将看到一条声明，该声明反映了您管理的启用了 S3 保护的账户数量。选择 “全部启用” 可为所有账户启用 S3 保护。

   Note

   如果您在组织内管理帐户，则此操作还会启用自动启用功能，以自动为组织内的future 成员账户启用 S3 保护。

在成员账户中选择性地启用或禁用 S3 保护

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Settings 下，选择 Accounts。

   Note

   在账户表中，查看 S 3 保护列。绿色勾号图标表示 S3 保护已启用，蓝色短划线图标表示已禁用。如果此列为空，则该账户没有资格获得 S3 保护。您也可以按 “启用” 或 “禁用” 进行筛选。
3. 选择您要为其配置 S3 保护的账户。从 “操作” 菜单中选择 “启用 S3 保护” 或 “禁用 S3 保护”，然后确认您的选择以更改所选账户的设置。表格将自动更新以显示您的更改。

API

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 updateMemberDetectorsAPI 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`true`替换为`false`。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI 来找到。

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 123456789012 --data-sources '{"S3Logs":{"Enable":true}}'
```

Note

您也可以传递由空格分隔的账户 ID 列表。

成功执行代码后，它会返回一个空列表`UnprocessedAccounts`。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 以及问题摘要。

Note

如果您使用脚本加入新账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 createDetectorAPI 操作。

自动为新 GuardDuty 账户禁用 S3 保护

Important

默认情况下，S3 保护自动为新探测器启用。

如果您是首次在新账户上启 GuardDuty 用 S3 保护的 GuardDuty 管理员，并且您不希望在默认情况下启用 S3 保护，则可以通过修改带有可选`dataSources`对象的 createDetectorAPI 操作来将其禁用。以下示例使用在禁Amazon CLI用 S3 保护的情况下启用新的 GuardDuty 检测器。

```
aws guardduty create-detector --enable --data-sources '{"S3Logs":{"Enable":false}}'
```

S3 保护中的功能

Amazon CloudTrailS3 的数据事件

数据事件，也称为数据平面操作，用于深入了解对资源执行的资源操作。它们通常是高容量的活动。

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

- `GetObject` API 操作
- `PutObject` API 操作
- `ListObjects` API 操作
- `DeleteObject` API 操作

默认情况下，新账户启用 S3 数据事件监控。但是，此数据源是可选的，可以随时为任何账户或地区启用或禁用。有关将 Amazon S3 配置为数据源的更多信息，请参阅亚马逊的Amazon S3 保护 GuardDuty (p. 74)。

了解亚马逊的GuardDuty调查结果

GuardDuty发现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Amazon环境中检测到意外和潜在的恶意活动时，就会生成调查结果。

您可以在GuardDuty控制台的 “GuardDuty发现” 页面上查看和管理您的调查结果，也可以使用Amazon CLI或API 操作来查看和管理您的调查结果。有关管理发现结果的方法的概述，请参阅管理亚马逊的GuardDuty调查结果 (p. 183)。

话题：

正在寻找细节 (p. 78)

了解GuardDuty调查结果中可用的数据类型。

示例发现结果 (p. 90)

了解如何生成示例调查结果以测试或更好地理解 GuardDuty。

GuardDuty 查找格式 (p. 88)

了解 GuardDuty 调查结果类型的格式以及 GuardDuty 跟踪的各种威胁目的。

查找类型 (p. 94)

按类型查看和搜索所有可用的 GuardDuty 调查结果。每个发现类型条目都包含对该发现的解释以及补救提示和建议。

正在寻找细节

在亚马逊GuardDuty控制台中，您可以在结果摘要部分查看查找详情。查找详细信息因查找类型而异。

有两个主要细节决定了哪种信息可用于任何发现。第一个是资源类型，可以是`Instance`、`AccessKey`、`S3BucketKubernetes cluster`、`ECS cluster`、`ContainerRDSDBInstance`、或`Lambda`。决定查找信息的第二个细节是资源角色。资源角色可以`Target`用于访问密钥，这意味着该资源是可疑活动的目标。例如，对于类型发现，资源角色也可以是`Actor`，这意味着您的资源是执行可疑活动的参与者。本主题介绍一些常见的发现细节。

查找概述

调查结果的概述部分包含该发现的最基本的识别特征，包括以下信息：

- 账户 ID — 活动发生时提示生成此发现GuardDuty的Amazon账户的 ID。
- 计数 — 汇总符合此模式的活动与该发现 ID 的次GuardDuty数。
- 创建于-首次创建此发现的时间和日期。如果此值与 Up dated at 不同，则表示该活动已发生多次，并且是一个持续存在的问题。

  Note

  GuardDuty控制台中查找结果的时间戳显示在本地时区，而 JSON 导出和 CLI 输出以 UTC 显示时间戳。
- 查找结果 ID-此查找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。
- 查找类型-表示触发查找结果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 (p. 88)：

- 区域-生成调查结果的Amazon区域。有关支持的区域的更多信息，请参阅区域和终端节点 (p. 292)。
- 资源 ID — 活动所针对的Amazon资源的 ID，该资源GuardDuty提示生成此调查结果。
- 扫描 ID — 适用于启用GuardDuty恶意软件保护时的发现，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。有关更多信息，请参阅恶意软件防护查找详情 (p. 84)：
- 严重性-为发现分配的严重性级别为 “高”、“中” 或 “低”。有关更多信息，请参阅GuardDuty调查结果的严重性级别 (p. 92)：
- 更新于-上次更新此发现时，新活动与提示GuardDuty生成此发现的模式相匹配.

资源

受影响的资源提供了有关启动活动所针对的Amazon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-启动查找的Amazon资源的角色。此值可以是 TA RGET 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参与者。

资源类型-受影响资源的类型。如果涉及多个资源，则调查结果可能包括多种资源类型。资源类型包括实例、S3Bucket AccessKey、ecs Cluster、Container KubernetesCluster、r dsdbinStan ce 和 L am bda。根据资源类型的不同，可用的发现细节也不同。选择资源选项卡以了解该资源的可用详细信息。

Instance

实例详情：

> **Note**
>
> 如果实例已经停止，或者在进行跨区域 API 调用时，底层 API 调用源自不同区域的 EC2 实例，则可能会丢失一些实例的详细信息。

- 实例 ID — 参与提示GuardDuty生成调查结果的活动的 EC2 实例的 ID。
- 实例类型-调查中涉及的 EC2 实例的类型。
- 启动时间-启动实例的时间和日期。
- 前哨 ARN — 的亚马逊资源名称 (ARN)。Amazon Outposts仅适用于实Amazon Outposts例。有关更多信息，请参阅什么是 Amazon Outposts？
- 安全组名称-附加到相关实例的安全组的名称。
- 安全组 ID — 关联到相关实例的安全组的 ID。
- 实例状态-目标实例的当前状态。
- 可用区-相关实例所在的Amazon区域可用区。
- 映像 ID — 用于构建活动所涉及的实例的亚马逊机器映像的 ID。
- 图片描述 — 描述用于构建活动所涉及的实例的亚马逊系统映像 ID。
- 标签 — 附加到此资源的标签列表，以`key:`的格式列出`value`。

AccessKey

访问密钥详情：

- 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。
- 主体 ID — 参与提示GuardDuty生成调查结果的活动的用户的主要 ID。
- 用户类型-参与提示GuardDuty生成调查结果的活动的用户类型。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

亚马逊 S3 存储桶详情：

- 名称-调查结果所涉及的存储桶的名称。
- ARN-调查结果所涉及的存储桶的 ARN。
- 所有者 — 拥有调查结果所涉存储段的用户的权威用户 ID。有关权威用户 ID 的更多信息，请参阅Amazon账户标识符。
- 类型-存储段查找的类型，可以是目标或来源。
- 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`:的格式列出`value`。
- 有效权限-对存储桶上所有有效权限和策略的评估，以表明所涉及的存储桶是否已公开公开。值可以是公开的，也可以是非公开的。

EKSCluster

Kubernetes 集群详细信息：

- 名称 — Kubernetes 集群的名称。
- ARN-用于识别集群的 ARN。
- 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显示在本地时区，而 JSON 导出和 CLI 输出以 UTC 显示时间戳。
- VPC ID — 与您的集群关联的 VPC 的 ID。
- 状态-群集的当前状态。
- 标签-应用于集群的元数据，可帮助您对集群进行分类和组织。每个标签由一个密钥和一个可选值组成，列出的格式为`key：value`。你可以同时定义键和值。

  集群标签不会传播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、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-创建此工作负载的时间和日期。
- 标签 — 附加到 Kubernetes 工作负载的键值对。
- 容器 — 作为 Kubernetes 工作负载的一部分运行的容器的详细信息。
- 命名空间-工作负载属于此 Kubernetes 命名空间。
- 容量 — Kubernetes 工作负载使用的容量。
  - 主机路径 — 表示卷映射到的主机上预先存在的文件或目录。
  - 名称-卷的名称。
- 容器安全上下文 — 定义容器中所有容器的权限和访问控制设置。
- 主机网络 — `true` 如果容器包含在 Kubernetes 工作负载中，则设置为。

Kubernetes 用户详细信息：

- 群组 — 参与生成调查结果的活动的用户的 Kubernetes RBAC（基于角色访问的控制）群组。

- ID — Kubernetes 用户的唯一 ID。
- 用户名 — 参与生成调查结果的活动的 Kubernetes 用户的姓名。
- 会话名称 — 扮演具有 Kubernetes RBAC 权限的 IAM 角色的实体。

ECSCluster

ECS 集群详细信息：

- ARN-用于识别集群的 ARN。
- 名称-群集的名称。
- 状态-群集的当前状态。
- 活动服务计数-在集群上运行的处于某种ACTIVE状态的服务数量。您可以使用以下方式查看这些服务ListServices
- 注册的容器实例数-注册到集群的容器实例的数量。这包括ACTIVE和DRAINING状态中的容器实例。
- 正在运行的任务数-集群中RUNNING处于状态的任务数量。
- 标签-应用于集群的元数据，可帮助您对集群进行分类和组织。每个标签由一个密钥和一个可选值组成，列出的格式为key：value。你可以同时定义键和值。
- 任务详细信息-集群中任务的详细信息。

Container

集装箱详情：

- 容器运行时间-用于运行容器的容器运行时间（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。
- 图像-容器实例的图像。
- 容量装载量 — 集装箱容量列表。容器可以在其文件系统下装入一个卷。
- 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。
- 流程详细信息-描述与调查结果相关的流程的详细信息。

RDSDBInstance

rdsdbInstance 详细信息：

> **Note**
>
> 此资源可在与数据库实例相关的 RDS 保护调查结果中找到。

- 数据库实例 ID — 与GuardDuty调查结果所涉及的数据库实例相关的标识符。
- 引擎-调查所涉及的数据库实例的数据库引擎名称。可能的值是兼容 Aurora mySQL 或兼容 Aurora PostgreSQL。
- 引擎版本-GuardDuty 调查中涉及的数据库引擎的版本。
- 数据库集群 ID — 数据库集群的标识符，其中包含GuardDuty调查结果所涉及的数据库实例 ID。
- 数据库实例 ARN — 用于识别GuardDuty调查中涉及的数据库实例的 ARN。

Lambda

Lambda 函数详细信息

- 函数名称-调查结果中涉及的 Lambda 函数的名称。

- 函数版本-调查结果中涉及的 Lambda 函数的版本。
- 函数描述-对调查结果所涉及的 Lambda 函数的描述。
- 函数 ARN — 调查结果所涉的 Lambda 函数的亚马逊资源名称 (ARN)。
- 修订版 ID — Lambda 函数版本的修订版 ID。
- 角色-调查结果中涉及的 Lambda 函数的执行角色。
- VPC 配置 — 亚马逊 VPC 配置，包括与您的 Lambda 函数关联的 VPC ID、安全组和子网 ID。
- VPC ID — 与调查结果中涉及的 Lambda 函数关联的亚马逊 VPC 的 ID。
- 子网 ID-与您的 Lambda 函数关联的子网的 ID。
- 安全组-连接到相关的 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:valuepair` 的格式列出。

RDS 数据库 (DB) 用户详细信息

Note

本部分适用于您在中启用 RDS 保护功能时的发现GuardDuty。有关更多信息，请参阅GuardDutyRDS 防护 (p. 68)：

该GuardDuty发现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-异常登录尝试中涉及的数据库实例的名称。
- SSL — 用于网络的安全套接字层 (SSL) 版本。
- 身份验证方法-参与调查的用户使用的身份验证方法。

EKS 运行时监控运行时详细信息

Note

这些详细信息仅在GuardDuty生成其中一个时才可用EKS 运行时监控查找类型 (p. 111)。

本部分包含运行时详细信息，例如流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。

流程详情

- 名称-进程的名称。
- 可执行路径-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 P ID — 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，它是容器内部观察到的进程 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。
- StartT ime — 进程启动的时间。这是 UTC 日期字符串格式 (`2023-03-22T19:37:20.168Z`)。
- UUID — 分配给进程的GuardDuty唯一 ID。
- 父进程 UUID — 父进程的唯一 ID。此 ID 由分配给父进程GuardDuty。
- 用户 — 执行流程的用户。

- 用户 ID — 执行流程的用户的 ID。
- 有效用户 ID — 事件发生时进程的有效用户 ID。
- 世系-有关该过程祖先的信息。
  - 进程 ID — 操作系统分配给进程的 ID。
  - UUID — 分配给进程的GuardDuty唯一 ID。
  - 可执行路径-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 P ID — 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，它是容器内部观察到的进程 ID。
  - 用户 ID — 执行流程的用户的用户 ID。
  - 名称-进程的名称。

运行时上下文

在以下字段中，生成的查找结果可能仅包含与查找结果类型相关的字段。

- 装载源 — 容器在主机上安装的路径。
- 装载目标 — 容器中映射到主机目录的路径。
- 文件系统类型 — 表示已安装文件系统的类型。
- 标志-表示控制此发现所涉及事件行为的选项。
- 修改进程-有关运行时在容器内创建或修改二进制、脚本或库的进程的信息。
- 修改于 — 运行时进程在容器内创建或修改二进制、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-访问的 Docker 套接字的路径。
- Runc 二进制路径-`runc` 二进制路径。
- 发布代理路径-`cgroup` 发布代理文件的路径。

EBS 卷扫描详细信息

> **Note**
>
> 本部分适用于在您打开GuardDuty启动的恶意软件扫描时发现的GuardDuty恶意软件防护 (p. 48)结果。

EBS 卷扫描提供了有关连接到可能受感染的 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。
- 扫描开始于-恶意软件扫描开始的日期和时间。
- 扫描完成时间-恶意软件扫描完成的日期和时间。
- 触发器查找 ID — 启动此恶意软件扫描的GuardDuty发现的发现 ID。
- 来源-可能的值为`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。
  - 已扫描的项目数量-已扫描文件的总数。它提供诸如`totalGbfiles`、和之类的详细信息`volumes`。
  - 检测到的威胁项目数-扫描期间`files`检测到的恶意软件总数。

- 最高严重性威胁详细信息-扫描期间检测到的最严重威胁的详细信息以及恶意文件数量。它提供诸如severitythreatName、和之类的详细信息count。
- 按名称检测到的威胁-容器元素对所有严重级别的威胁进行分组。它提供诸如itemCount、uniqueThreatNameCountshortened、和之类的详细信息threatNames。

恶意软件防护查找详情

Note

本部分适用于在您打开GuardDuty启动的恶意软件扫描时发现的GuardDuty恶意软件防护 (p. 48)结果。

当恶意软件保护扫描检测到恶意软件时，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来查看扫描详细信息。您的恶意软件保护发现的严重程度取决于GuardDuty发现的严重程度。

Note

该GuardDutyFindingDetected标签指定快照包含恶意软件。

以下信息可在详细信息面板的 “检测到的威胁” 部分下找到。

- 名称-威胁的名称，通过检测对文件进行分组而获得。
- 严重性-检测到的威胁的严重程度。
- 哈希 — 文件的 SHA-256。
- 文件路径 — 恶意文件在 EBS 卷中的位置。
- 文件名 — 检测到威胁的文件的名称。
- 卷 ARN-已扫描的 EBS 卷的 ARN。

以下信息位于详细信息面板的恶意软件扫描详细信息部分下。

- 扫描 ID-恶意软件扫描的扫描 ID。
- 扫描开始于-扫描开始的日期和时间。
- 扫描完成时间-扫描完成的日期和时间。
- 扫描的文件-扫描的文件和目录的总数。
- 扫描的总GB-在此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。
- 以下信息可在详细信息面板的音量详细信息部分下找到。
  - 卷 ARN — 卷的亚马逊资源名称 (ARN)。
  - SnapshotARN — EBS 卷快照的 ARN。
  - 状态-卷的扫描状态，例如RunningSkipped、和Completed。
  - 加密类型-用于加密卷的加密类型。例如，CMCMK。
  - 设备名称-设备的名称。例如，/dev/xvda。

操作

调查结果的操作提供了有关触发该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-查找活动类型。此值可以是 NETWORK_CONNECTION、PORT_PROBE、DNS_REQUEST、AWS_API_ CALL 或 RDS_LOGIN_TREM 可用信息因操作类型而异：

- NETWORK_ CONNECTION — 表示已在识别的 EC2 实例和远程主机之间交换了网络流量。此操作类型包含以下附加信息：
  - 连接方向-在提示GuardDuty生成调查结果的活动中观察到的网络连接方向。它可以是以下值之一：
    - IN BOUND — 表示远程主机启动了与您账户中已识别的 EC2 实例上的本地端口的连接。
    - 出站 — 表示已识别的 EC2 实例启动了与远程主机的连接。
    - 未知-表示GuardDuty无法确定连接方向。
  - 协议 — 在活动中观察到的提示GuardDuty生成调查结果的网络连接协议。
  - 本地 IP — 触发查找结果的流量的原始源 IP 地址。此信息可用于区分流量流经的中间层的 IP 地址与触发调查结果的流量的原始源 IP 地址。例如，EKS pod 的 IP 地址与运行 EKS pod 的实例的 IP 地址。
  - 已阻止-表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。此操作类型包含以下附加信息：
  - 本地 IP — 触发查找结果的流量的原始源 IP 地址。此信息可用于区分流量流经的中间层的 IP 地址与触发调查结果的流量的原始源 IP 地址。例如，EKS pod 的 IP 地址与运行 EKS pod 的实例的 IP 地址。
  - 已阻止-表示目标端口是否被阻止。
- DNS_RE QUEST — 表示已识别的 EC2 实例查询了域名。此操作类型包含以下附加信息：
  - 协议 — 在活动中观察到的提示GuardDuty生成调查结果的网络连接协议。
  - 已阻止-表示目标端口是否被阻止。
- AWS_API_CALL — 表示调用了 API。Amazon此操作类型包含以下附加信息：
  - API — 调用并因此提示生成此发现的 API 操作GuardDuty的名称。

    Note

    这些操作还可能包括由Amazon CloudTrail捕获的非 API 事件。有关更多信息，请参阅捕获的非 API 事件。CloudTrail
  - 用户代理 — 发出 API 请求的用户代理。此值告诉您该调用是从Amazon Web Services Management Console、Amazon服务、S Amazon DK 还Amazon CLI是。
  - 错误代码 — 如果发现是由失败的 API 调用触发的，则会显示该调用的错误代码。
  - 服务名称-尝试进行触发调查结果的 API 调用的服务的 DNS 名称。
- RDS_LOGIN_T REMY — 表示有人尝试从远程 IP 地址登录可能受感染的数据库。
  - IP 地址-用于进行潜在可疑登录尝试的远程 IP 地址。

演员或目标

如果资源角色是，则搜索结果中会有一个 “参与者” 部分TARGET。这表明您的资源已成为可疑活动的目标，Acto r 部分包含有关以您的资源为目标的实体的详细信息。

如果资源角色是，则搜索结果会有一个 “目标” 部分ACTOR。这表示您的资源参与了针对远程主机的可疑活动，此部分包含有关您的资源所针对的 IP 或域的信息。

“参与者” 或 “目标” 部分中提供的信息可能包括以下内容：

- 关联-有关远程 API 调用者的Amazon帐户是否与您的GuardDuty环境相关的详细信息。如果此值为`true`，则 API 调用者以某种方式关联到您的账户；如果是`false`，则 API 调用者来自您的环境之外。
- 远程账户 ID — 拥有用于访问最终网络资源的出口 IP 地址的账户 ID。
- IP 地址-提示GuardDuty生成调查结果的活动所涉及的 IP 地址。
- 位置 — 提示GuardDuty生成调查结果的活动所涉的 IP 地址的位置信息。
- 组织 — 提示GuardDuty生成调查结果的活动所涉的 IP 地址的 ISP 组织信息。
- 端口 — 提示GuardDuty生成调查结果的活动中涉及的端口号。
- 域 — 提示生成调查结果的活动GuardDuty所涉及的域。

其他信息

所有发现都有一个附加信息部分，其中可以包含以下信息：

- 威胁列表名称-威胁列表的名称，包括提示GuardDuty生成调查结果的活动所涉及的 IP 地址或域名。
- 样本-表示这是否是样本发现的真值或假值。
- 已存档-一个真值或假值，表示该发现是否已存档。
- 不寻常-历史上未观察到的活动细节。这些可能包括异常（以前未被观察到）的用户、位置、时间、时段、登录行为或 ASN Org。
- 不寻常的协议-提示GuardDuty生成调查结果的活动中涉及的网络连接协议。
- 代理详细信息-有关当前在您的 EKS 集群上部署的安全代理的详细信息Amazon Web Services 账户。这仅适用于 EKS 运行时监控查找类型。
  - 代理版本-GuardDuty 安全代理的版本。
  - 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结果有 “证据” 部分，其中包含以下信息：

- 威胁情报详细信息-识别`Threat name`出的威胁列表的名称。
- 威胁名称-与威胁相关的恶意软件系列或其他标识符的名称。

异常行为

以结尾的发现类型AnomalousBehavior表示该发现是由GuardDuty异常检测机器学习 (ML) 模型生成的。机器学习模型会评估向您的账户发出的所有 API 请求，并识别与对手使用的战术相关的异常事件。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、发出请求的地点以及请求的具体 API。

有关API请求的哪些因素对于调用请求的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。身份由 CloudTrailUserIdentity 元素定义，可能的值为：`RootIAMUser`、`AssumedRole`、`FederatedUserAWSAccount`、或`AWSService`。

除了与 API 活动相关的所有GuardDuty发现的可用详细信息外，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，也可以在调查结果的 JSON 中找到。

- 异常 API — 用户身份在与调查结果相关的主 API 请求附近调用的 API 请求列表。此窗格通过以下方式进一步分解 API 事件的详细信息。
  - 列出的第一个 API 是主 API，即与观察到的最高风险活动相关的 API 请求。这是触发发现的 API，与查找类型的攻击阶段相关。这也是控制台的 “操作” 部分和调查结果的 JSON 中详细介绍的 API。
  - 列出的任何其他 API 都是在主 API 附近观察到的来自所列用户身份的其他异常 API。如果列表中只有一个 API，则 ML 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。
  - API 列表根据 API 是否成功调用，或者是否调用 API 失败（表示已收到错误响应）进行划分。收到的错误响应类型列在每个未成功调用的 API 的上方。可能的错误响应类型为：`access deniedaccess denied exceptionauth failure`、`instance limit exceeded`、`invalid permission - duplicate`、`invalid permission - not found`、和`operation not permitted`。
  - API 按其关联服务进行分类。

    Note

    如需了解更多背景信息，请选择 Historial API 以查看有关顶级 API 的详细信息，最多可查看 20 个，通常同时显示用户身份和账户内所有用户。API 被标记为稀有（每月少于一次）、不频繁（每月几次）或频繁（每天到每周），具体取决于它们在您的账户中的使用频率。

- 异常行为（账户）— 本部分提供有关您账户中被分析行为的更多详细信息。此面板中跟踪的信息包括：
  - ASN 组织 — 进行异常 API 调用的 ASN 组织。
  - 用户名-进行异常 API 调用的用户的姓名。
  - 用户代理 — 用于进行异常 API 调用的用户代理。用户代理是用于进行呼叫的方法，例如`aws-cli`或`Botocore`。
  - 用户类型-进行异常 API 调用的用户类型。可能的值为`AWS_SERVICEASSUMED_ROLE`、`IAM_USER`、或`ROLE`。
  - 存储桶-正在访问的 S3 存储桶的名称。
- 异常行为（用户身份）— 本节提供有关调查结果所涉及的用户身份分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 模型以前从未见过该用户身份在训练期间以这种方式进行此 API 调用。以下有关用户身份的其他详细信息可用：
  - ASN 组织 — 异常 API 调用的 ASN 组织。
  - 用户代理 — 用于进行异常 API 调用的用户代理。用户代理是用于进行呼叫的方法，例如`aws-cli`或`Botocore`。
  - 存储桶-正在访问的 S3 存储桶的名称。
- 异常行为（存储桶）— 本部分提供了有关与发现相关的 S3 存储桶的已分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。本节中跟踪的信息包括：
  - ASN 组织 — 异常 API 调用的 ASN 组织。
  - 用户名-进行异常 API 调用的用户的姓名。
  - 用户代理 — 用于进行异常 API 调用的用户代理。用户代理是用于进行呼叫的方法，例如`aws-cli`或`Botocore`。
  - 用户类型-进行异常 API 调用的用户类型。可能的值为`AWS_SERVICEASSUMED_ROLE`、`IAM_USER`、或`ROLE`。

    Note

    要了解有关历史行为的更多背景信息，请在“异常行为（帐户）”、“用户 ID”或“存储桶”部分中选择历史行为，以查看您的账户中以下每个类别的预期行为的详细信息：罕见（每月少于一次）、罕见（每月几次）或频繁（每天到每周），具体取决于您的账户中使用它们的频率。
- 异常行为（数据库）-本节提供有关与发现相关的数据库实例的已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 模型在训练期间从未见过以这种方式登录此数据库实例的尝试。在查找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-异常登录尝试中涉及的数据库实例的名称。

    Note

    历史行为部分提供了有关先前观察到的相关数据库的用户名、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。

基于卷的 S3 异常

本节详细介绍基于卷的 S3 异常的上下文信息。基于容量的 finding (Exfiltration:S3/AnomalousBehavior (p. 159)) 可监控用户对 S3 存储桶进行的 S3 API 调用次数异常，这表明存在潜在的数据泄露现象。对以下 S3 API 调用进行监控，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 存储桶时通常行为的基准。为了检测数据泄露，基于容量的异常检测发现会根据通常的行为基线评估所有活动。在“异常行为（用户身份）”、“观测量（用户身份）”和“观测容量（存储桶）”部分中选择历史行为，分别查看以下指标。

- 在过去 24 小时内，与受影响的 S3 存储桶相关的 IAM 用户或 IAM 角色（取决于发出了哪个）调用的 `s3-api-name` API 调用次数。
- 在过去 24 小时内，与所有 S3 存储桶关联的 IAM 用户或 IAM 角色（取决于发出了哪个）调用的 `s3-api-name` API 调用次数。
- 过去 24 小时内与受影响 S3 存储桶关联的所有 IAM 用户或 IAM 角色（取决于发出的角色）的 `s3-api-name` API 调用次数。

基于 RDS 登录活动的异常

本节详细介绍了不寻常的参与者执行的登录尝试次数，并按登录尝试的结果分组。通过监视登录事件中是否有`successfulLoginCount`、`failedLoginCount`和的异常模式来RDS 保护查找类型 (p. 153)识别异常行为。`incompleteConnectionCount`

- successfulLoginCount— 此计数器表示异常操作者与数据库实例成功建立的连接（登录属性的正确组合）的总和。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。这表示登录组合的一个或多个属性（例如用户名、密码或数据库名）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关闭。例如，端口扫描，其中连接了数据库端口，但没有向数据库发送任何信息，或者连接在成功或失败的尝试中止了登录。

GuardDuty 查找格式

当在您的Amazon环境中 GuardDuty 检测到可疑或意外行为时，它会生成调查结果。调查结果是一种通知，其中包含有关发现 GuardDuty 的潜在安全问题的详细信息。调查结果的详细 (p. 93)信息包括有关所发生的事情、可疑活动涉及哪些Amazon资源、该活动何时发生的信息以及其他信息。

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，recon GuardDuty: ec2/PortProbeUnprotectedPort 查找类型会迅速通知您，在您的Amazon环境中的某个地方，EC2 实例有一个未受保护的端口，潜在的攻击者正在探测该端口。

GuardDuty 使用以下格式命名其生成的各种类型的发现：

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName。 DetectionMechanism！ Artifact

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-描述威胁的主要目的、攻击类型或潜在攻击的阶段。有关 GuardDuty 威胁目的的完整列表，请参阅以下部分。
- ResourceTypeAffected-描述在本调查结果中将哪种Amazon资源类型确定为对手的潜在目标。目前，GuardDuty 可以为 EC2、S3、IAM 和 EKS 资源生成调查结果。
- ThreatFamilyName-描述 GuardDuty 正在检测到的总体威胁或潜在的恶意活动。例如，值NetworkPortUnusual表示在调查结果中识别的 EC2 实例在 GuardDuty 调查结果中也发现的特定远程端口上没有通信历史记录。
- DetectionMechanism-描述 GuardDuty 检测发现的方法。这可以用来表示常见发现类型的变异或 GuardDuty 使用特定机制进行检测的发现。例如，b ackdoor: ec2/DenialOfService .Tcp 表示检测到通过 TCP 的拒绝服务 (DoS)。UDP 变体是后门:ec2/DenialOfService .Udp。

值为 .Custom 表示根据您的自定义威胁列表 GuardDuty 检测到发现结果，而. Reputority 表示使用域名信誉评分模型 GuardDuty 检测到该发现结果。

- Ar@@ ti fact-描述恶意活动中使用的工具所拥有的特定资源。例如，查找结果中的 DNS 类型:ec2/CryptoCurrency.BBitcoinTool! DNS 表示 EC2 实例正在与已知的比特币相关域进行通信。

威胁情报集

GuardDuty 在威胁中，目的描述威胁的主要目的、攻击类型或潜在攻击的阶段。例如，某些威胁目的（例如 Backdoor）表示攻击的类型。但是，某些威胁目的，例如Impac t，与 MITRE ATT&CK 战术一致。MITRE ATT&CK 战术表明对手攻击周期的不同阶段。在当前版本中 GuardDuty， ThreatPurpose 可以具有以下值：

后门

此值表示对手入侵了Amazon资源并更改了资源，因此它能够联系其主命令和控制 (C&C) 服务器以接收有关恶意活动的进一步指令。

行为

该值表示 GuardDuty 检测到的活动或活动模式与所涉Amazon资源的既定基准不同。

CredentialAccess

该值表示 GuardDuty 已检测到攻击者可能利用这些活动模式从您的环境中窃取账户 ID 或密码等证书。这种威胁目的基于 MITRE ATT&CK 战术

加密货币

该值表示 GuardDuty 已检测到您环境中的某个Amazon资源正在托管与加密货币（例如比特币）相关的软件。

DefenseEvasion

该值表示 GuardDuty 已检测到活动或活动模式，对手在渗透您的环境时可能使用这些活动或活动模式来逃避侦测。这种威胁目的基于 MITRE ATT&CK 战术

发现

该值表示 GuardDuty 已检测到活动或活动模式，对手可能利用这些活动或活动模式来扩展他们对您的系统和内部网络的了解。这种威胁目的基于 MITRE ATT&CK 战术。

处决

该值表示 GuardDuty 已检测到对手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&CK 战术。

渗透

该值表示 GuardDuty 已检测到对手在尝试从您的网络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&CK 战术。

影响

该值表示 GuardDuty 已检测到活动或活动模式，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

InitialAccess

这种威胁目的基于 MITRE ATT&CK 战术

Pentest

有时，Amazon资源所有者或其授权代表会故意对Amazon应用程序进行测试以发现漏洞，例如开放的安全组或过于宽松的访问密钥。这些笔试是为了在对手发现易受攻击的资源之前识别和锁定这些资源。但是，授权的笔试人员使用的某些工具是免费提供的，因此未经授权的用户或对手可以用来运行探测测

试。尽管 GuardDuty 无法确定此类活动背后的真正目的，但 Pentest 值表示 GuardDuty 正在检测此类活动，它与已知笔试用工具生成的活动类似，并且可能表示正在对您的网络进行恶意探测。

持久性

该值表示 GuardDuty 已检测到活动或活动模式，即使对手的初始访问路径被切断，他们也可能使用这些活动或活动模式来尝试保持对您的系统的访问权限。例如，这可能包括在通过现有用户的泄露证书获得访问权限后创建一个新的 IAM 用户。删除现有用户的凭证后，对手将保留对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&CK 战术。

策略

此值表明您的Amazon Web Services 账户行为违反了推荐的安全最佳实践。

PrivilegeEscalation

此值告诉您，您的Amazon环境中涉及的主体正在表现出对手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&CK 战术。

Recon

该值表示 GuardDuty 已检测到对手在对您的网络进行侦测时可能使用的活动或活动模式，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Amazon环境中的漏洞范围。

Stealth

该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，这使得评估活动的真实性质变得极其困难。

木马

此值表示攻击使用的是默默执行恶意活动的特洛伊木马程序。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

该值表示 GuardDuty 正在检测未授权个人的可疑活动或可疑活动模式。

在中生成样本发现 GuardDuty

您可以使用亚马逊生成样本调查结果 GuardDuty ，以帮助您可视化和了解 GuardDuty 可以生成的各种发现类型。在生成示例调查结果时， GuardDuty 会填充当前调查结果列表，每个支持的调查结果类型对应一个示例调查结果。

生成的样本是用占位符值填充的近似值。这些示例可能看起来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 CloudWatch 事件或过滤器。表中列出了查找类型的可用值查找类型 (p. 94)列表。

要根据环境中的模拟活动生成一些常见的调查结果，请参阅下面的自动生成常见 GuardDuty发现 (p. 91)。

通过 GuardDuty 控制台或 API 生成样本调查结果

选择一种访问方法，学习如何通过该方法生成样本发现。

Note

控制台方法生成每种查找类型中的一个。单个样本发现只能通过 API 生成。

Console

使用以下过程来生成示例调查结果。此过程为每种查找结果类型生成一个样本 GuardDuty 发现。

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中，选择 Settings (设置)。
3. 在 Settings 页面上的 Sample findings 下，选择 Generate sample findings。
4. 在导航窗格中，选择 Findings (结果)。样本发现显示在当前发现结果页面上，前缀为 [SAMPLE]。

API

您可以通过 CreateSampleFindingsAPI 生成与任何查找结果类型匹配的单个样本 GuardDuty 查找结果，查找类型 (p. 94)表中列出了查找结果类型的可用值。

这对于测试 CloudWatch 事件规则或基于发现的自动化很有用。以下示例说明如何使用生成该`Backdoor:EC2/DenialOfService.Tcp`类型的单个样本查找Amazon CLI。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
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。在查找结果 JSON 详细信息的 “additionalInfo” 部分`"sample": true`中，样本发现的值为。

自动生成常见 GuardDuty发现

您可以使用以下脚本自动生成多个常见 GuardDuty 发现。gu ardduty-tester.t emplate 用于Amazon CloudFormation 创建一个隔离环境，其中包含堡垒主机、一个可以通过 SSH 访问的测试器 Amazon EC2 实例和两个目标 EC2 实例。然后，您可以运行 guardduty_tester.sh 在测试人员 EC2 实例、目标 Windows EC2 实例和目标 Linux EC2 实例之间开始交互，模拟五种常见攻击，这些攻击 GuardDuty 可以检测并通过生成的发现通知您。

1. 作为先决条件，你必须在要运行 gu ardduty-tester.template 和 guardduty_tester.sh 的账户和区域中启用 GuardDuty 。有关启用的更多信息 GuardDuty，请参阅GuardDuty 入门 (p. 2)。

   您还必须在要运行这些脚本的每个区域生成新的 EC2 key pair 或使用现有的 EC2 密钥对。此 EC2 key pair 用作用于创建新 CloudFormation 堆栈的 g uardduty-tester.t emplate 脚本中的参数。有关生成密钥对的更多信息，请参阅 Amazon EC2 钥对。
2. 使用 gu ardduty-tester.templat e 创建一个新 CloudFormation 堆栈。有关创建堆栈的详细说明，请参阅创建堆栈。在运行 guardduty-tester.template 之前，请使用以下参数的值对其进行修改：Stack Name 用于标识您的新堆栈、Availability Zone 为您要运行此堆栈的位置、Key Pair 是您可以用于启动 EC2 实例的密钥对。然后，您可以使用相应的私钥通过 SSH 访问 EC2 实例。

   gu ardduty-tester.temp late 需要大约 10 分钟才能运行和完成。它将创建您的环境并将 guardduty_tester.sh 复制到您的测试用 EC2 实例。
3. 在Amazon CloudFormation 控制台中，选中新运行Amazon CloudFormation堆栈旁边的复选框。在显示的一组选项卡中，选择输出选项卡。记下分配给堡垒主机和测试用 EC2 实例的 IP 地址。要通过 SSH 访问测试器 EC2 实例，您需要这两个 IP 地址。
4. 在您的 ~/.ssh/config 文件中创建以下条目，以通过堡垒主机登录您的实例。

```
Host bastion
        HostName {Elastic IP Address of Bastion}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
Host tester
        ForwardAgent yes
```

```
HostName {Local IP Address of RedTeam Instance}
User ec2-user
IdentityFile ~/.ssh/{your-ssh-key.pem}
ProxyCommand ssh bastion nc %h %p
ServerAliveInterval 240
```

现在，您可以调用 $ ssh 测试器登录您的目标 EC2 实例。有关通过堡垒主机配置和连接到 EC2 实例的更多信息，请参阅 https://aws.amazon.com/blogs/security/securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/。

5. 连接到测试器 EC2 实例后，运行 guardduty_tester.sh 以启动测试人员和目标 EC2 实例之间的交互，模拟攻击并生成 GuardDuty调查结果。

GuardDuty调查结果的严重性级别

每个 GuardDuty 调查结果都有一个指定的严重性级别和值，可反映调查结果给您的网络带来的潜在风险，这些风险由我们的安全工程师确定。严重性值可以为介于 0.1 和 8.9 之间的任何值，该值越高，安全风险就越大。为了帮助您确定对调查结果突出显示的潜在安全问题的响应，GuardDuty 将此范围分为“高”、“中”和“低”严重性级别。

Note

值 0 和 9.0 到 10.0 当前被预留以供未来使用。

以下是当前为 GuardDuty 调查结果定义的严重性级别和值以及每个调查结果的一般建议：

严重性级别	值范围
高	8.9 - 7.0
高严重性级别表示相关资源（一个 EC2 实例或一组 IAM 用户登录证书）已被泄露并被积极用于未经授权的目的。 我们建议您优先处理任何“高”严重性的调查结果安全问题，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，或轮换 IAM 证书。有关更多详细信息，请参阅补救措施 (p. 213)。	
中等	6.9 - 4.0
“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。 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结果系列而异，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确认活动已获得授权，则应考虑资源受损，并按照修复步骤 (p. 213)保护资源。 查看“中”严重性级别的调查结果时，需要注意以下事项： • 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。 • 验证与相关的 IAM 角色、用户、组或证书集相关的权限。可能需要更改或轮换它们。	
低	3.9 - 1.0
“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。	

GuardDuty查找聚合

所有发现都是动态的，这意味着如果GuardDuty检测到与同一安全问题有关的新活动，它将使用新信息更新原始发现，而不是生成新的发现。这种行为使您无需浏览多个类似的报告即可识别持续存在的问题，并减少了您已经意识到的安全问题所带来的总体干扰。

例如，`UnauthorizedAccess:EC2/SSHBruteForce`在查找中，针对您的实例的多次访问尝试将汇总到同一个搜索结果 ID 中，从而增加搜索结果详细信息中的计数数。这是因为该调查结果表示实例的安全问题，指示未针对此类活动正确保护实例上的 SSH 端口。但是，如果 GuardDuty 检测到针对环境中的新实例的 SSH 访问活动，它将创建具有唯一调查结果 ID 的新调查结果，以提醒您存在与新资源关联的安全问题。

汇总调查结果后，将使用该活动最近发生的信息进行更新。这意味着，在上面的示例中，如果您的实例成为来自新参与者的暴力攻击的目标，则搜索结果详细信息将更新以反映最新来源的远程 IP，旧信息将被替换。有关个人活动尝试的完整信息仍可在您的CloudTrail或 VPC 流日志中找到。

发出警报GuardDuty以生成新发现而不是汇总现有发现的标准取决于查找结果类型。每种调查结果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。

定位和分析GuardDuty调查结果

使用以下过程查看和分析您的 GuardDuty 调查结果。

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 选择 Findings (调查结果)，然后选择一个特定的调查结果以查看其详细信息。

   每项发现的详细信息将根据调查结果类型、涉及的资源和活动的性质而有所不同。有关可用的调查结果字段的更多信息，请参阅正在寻找细节 (p. 78)。
3. （可选）如果要存档某个查找结果，请从搜索结果列表中将其选中，然后选择 “操作” 菜单。然后选择 Archive (存档)。

   从 “当前” 下拉列表中选择 “已存档”，即可查看已存档的调查结果。

   目前，来自GuardDuty成员帐户的GuardDuty用户无法存档结果.

   > **Important**
   >
   > 如果您使用上述过程将调查结果手动存档，此调查结果的所有后续匹配项（存档完成后生成）将添加到当前调查结果的列表。如果您永远不希望在当前列表中看到此调查结果，可以将它自动存档。有关更多信息，请参阅抑制规则 (p. 187)：
4. （可选）要下载一个调查结果，请从调查结果列表中选择该调查结果，然后选择 Actions (操作) 菜单。然后选择 Export (导出)。当您 Export (导出) 调查结果时，可以查看其完整 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在调查结果的 JSON 中提供置信度字段，并将其值设置为零。这种方式GuardDuty可以让你知道你可以放心地忽略这些发现。

查找类型

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，请参阅亚马逊的文档历史记录 GuardDuty (p. 294)。

有关查找现已停用的类型的信息，请参见停用的S3 (p. 166)。

GuardDuty EC2 查找类型

以下发现是特定于 Amazon EC2 资源的，其资源类型始终为`Instance`。调查结果的严重性和详细信息因资源角色而异，资源角色表明 EC2 资源是可疑活动的目标还是执行活动的参与者。

此处列出的发现包括用于生成该发现类型的数据源和模型。有关数据源和模型的更多信息，请参阅基础数据来源 (p. 14)。

> Note
>
> 如果某些 EC2 发现的实例已经终止，或者如果底层 API 调用是源自不同区域的 EC2 实例的跨区域 API 调用的一部分，则可能缺少实例详细信息。

对于所有 EC2 调查结果，建议您检查相关资源以确定其行为是否符合预期。如果活动获得授权，则可以使用禁止规则或可信 IP 列表来防止该资源收到误报通知。如果活动出乎意料，则最佳安全做法是假设实例已被入侵，并采取中详述的操作修复受感染的 EC2 实例 (p. 213)。

主题

- Backdoor:EC2/C&CActivity.B (p. 95)
- Backdoor:EC2/C&CActivity.B!DNS (p. 96)
- Backdoor:EC2/DenialOfService.Dns (p. 96)
- Backdoor:EC2/DenialOfService.Tcp (p. 97)
- Backdoor:EC2/DenialOfService.Udp (p. 97)
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts (p. 97)
- Backdoor:EC2/DenialOfService.UnusualProtocol (p. 98)
- Backdoor:EC2/Spambot (p. 98)
- Behavior:EC2/NetworkPortUnusual (p. 98)
- Behavior:EC2/TrafficVolumeUnusual (p. 99)
- CryptoCurrency:EC2/BitcoinTool.B (p. 99)
- CryptoCurrency:EC2/BitcoinTool.B!DNS (p. 100)
- DefenseEvasion:EC2/UnusualDNSResolver (p. 100)
- DefenseEvasion:EC2/UnusualDoHActivity (p. 100)
- DefenseEvasion:EC2/UnusualDoTActivity (p. 101)
- Impact:EC2/AbusedDomainRequest.Reputation (p. 101)
- Impact:EC2/BitcoinDomainRequest.Reputation (p. 101)
- Impact:EC2/MaliciousDomainRequest.Reputation (p. 102)
- Impact:EC2/PortSweep (p. 102)

- Impact:EC2/SuspiciousDomainRequest.Reputation (p. 103)
- Impact:EC2/WinRMBruteForce (p. 103)
- Recon:EC2/PortProbeEMRUnprotectedPort (p. 103)
- Recon:EC2/PortProbeUnprotectedPort (p. 104)
- Recon:EC2/Portscan (p. 104)
- Trojan:EC2/BlackholeTraffic (p. 105)
- Trojan:EC2/BlackholeTraffic!DNS (p. 105)
- Trojan:EC2/DGADomainRequest.B (p. 105)
- Trojan:EC2/DGADomainRequest.C!DNS (p. 106)
- Trojan:EC2/DNSDataExfiltration (p. 106)
- Trojan:EC2/DriveBySourceTraffic!DNS (p. 107)
- Trojan:EC2/DropPoint (p. 107)
- Trojan:EC2/DropPoint!DNS (p. 107)
- Trojan:EC2/PhishingDomainRequest!DNS (p. 108)
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom (p. 108)
- UnauthorizedAccess:EC2/MetadataDNSRebind (p. 108)
- UnauthorizedAccess:EC2/RDPBruteForce (p. 109)
- UnauthorizedAccess:EC2/SSHBruteForce (p. 109)
- UnauthorizedAccess:EC2/TorClient (p. 110)
- UnauthorizedAccess:EC2/TorRelay (p. 110)

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。

默认严重性：高

- 数据源：VPC 流日志

此发现通知您，您的Amazon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。列出的实例可能已被入侵。命令和控制服务器是向僵尸网络成员发出命令的计算机。

僵尸网络是一组连接互联网的设备，可能包括受常见恶意软件感染和控制的 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。

> Note
>
> 如果查询的 IP 与 log4j 相关，则相关查找结果的字段将包含以下值：
>
> - 服务。附加信息。 threatListName = 亚马逊
> - service.additionalInfo.ThreatName = log

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon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。列出的实例可能已被入侵。命令和控制服务器是向僵尸网络成员发出命令的计算机。

僵尸网络是一组连接互联网的设备，可能包括受常见恶意软件感染和控制的 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。

Note

如果查询的域名与 log4j 相关，则相关查找结果的字段将包含以下值：

- 服务。附加信息。 threatListName = 亚马逊
- service.additionalInfo.ThreatName = log

Note

要测试如何 GuardDuty 生成此查找结果类型，您可以从您的实例（用`dig`于 Linux 或`nslookup` Windows）针对测试域发出 DNS 请求`guarddutyc2activityb.com`。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/DenialOfService.Dns

EC2 实例的行为方式可能表明它正被用于使用 DNS 协议执行拒绝服务 (DoS) 攻击。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon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被入侵并被用来使用 DNS 协议执行 denial-of-service (DoS) 攻击。

Note

此调查结果仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/DenialOfService.Tcp

EC2 实例的行为方式表明它正被用于使用 TCP 协议执行拒绝服务 (DoS) 攻击。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon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被入侵并被用来使用 TCP 协议执行 denial-of-service (DoS) 攻击。

> Note
>
> 此调查结果仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/DenialOfService.Udp

EC2 实例的行为方式表明它正被用于使用 UDP 协议执行拒绝服务 (DoS) 攻击。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon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被入侵并被用来使用 UDP 协议执行 denial-of-service (DoS) 攻击。

> Note
>
> 此调查结果仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 实例的行为方式可能表明它正被用于在 TCP 端口上使用 UDP 协议执行拒绝服务 (DoS) 攻击。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例正在生成大量的出站 UDP 流量，这些流量指向通常用于 TCP 通信的端口。这可能表明列出的实例已遭到入侵，正被用来在 TCP 端口上使用 UDP 协议执行 denial-of-service (DoS) 攻击。

Note

此调查结果仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 实例的行为方式可能表明它正被用于使用不寻常协议执行拒绝服务 (DoS) 攻击。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例正在从一种不寻常的协议类型（例如 Internet Group Management Protocol）生成大量出站流量，而 EC2 实例通常不使用这种协议。这可能表明该实例已被入侵，正被用来使用异常协议执行 denial-of-service (DoS) 攻击。此调查结果仅针对公共路由 IP 地址检测 DoS 攻击，这是 DoS 攻击的主要目标。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/Spambot

EC2 实例通过与端口 25 上的远程主机通信表现出异常行为。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例正在与端口 25 上的远程主机通信。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。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Behavior:EC2/NetworkPortUnusual

EC2 实例在异常服务器端口上与远程主机通信。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例的行为偏离了既定基准。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 实例在端口 389 或端口 1389 上通信，则相关的查找严重性将修改为 “高”，并且查找字段将包含以下值：

- service.additionionalInfo.context = 可能的

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Behavior:EC2/TrafficVolumeUnusual

EC2 实例正在生成异常大量的网络流量到远程主机。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例的行为偏离了既定基准。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。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon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相关的 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。比特币是对比特币挖矿的奖励，受到威胁者的高度追捧。

补救建议：

如果您使用此 EC2 实例挖矿或管理加密货币，或者此实例以其他方式参与区块链活动，则此发现可能是您的环境的预期活动。如果您的Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。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 `CryptoCurrency:EC2/BitcoinTool.B`。第二个筛选条件应是涉及区块链活动的实例的 Instance ID (实例 ID)。要了解有关创建隐藏规则的更多信息，请参阅抑制规则 (p. 187)。

如果此活动是意外活动，您的实例可能会受到攻击，请参阅修复受感染的 EC2 实例 (p. 213)。

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。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon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相关的域名。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。比特币是对比特币挖矿的奖励，受到威胁者的高度追捧。

补救建议：

如果您使用此 EC2 实例挖矿或管理加密货币，或者此实例以其他方式参与区块链活动，则此发现可能是您的环境的预期活动。如果您的Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。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 `CryptoCurrency:EC2/BitcoinTool.B!DNS`。第二个筛选条件应是涉及区块链活动的实例的 Instance ID (实例 ID)。要了解有关创建隐藏规则的更多信息，请参阅抑制规则 (p. 187)。

如果此活动是意外活动，您的实例可能会受到攻击，请参阅修复受感染的 EC2 实例 (p. 213)。

DefenseEvasion:EC2/UnusualDNSResolver

一个 Amazon EC2 实例正在与一个不寻常的公有 DNS 解析器通信。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 Amazon EC2 实例的行为与基准行为有所不同。此 EC2 实例最近没有与该公有 DNS 解析器通信的历史记录。 GuardDuty 控制台查找结果详细信息面板中的 “异常” 字段可以提供有关所查询的 DNS 解析器的信息。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 实例正在通过 HTTPS (DoH) 通信执行异常的 DNS。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您Amazon环境中列出的 Amazon EC2 实例的行为偏离了既定基准。此 EC2 实例最近没有任何通过 HTTPS (DoH) 与该公共 DoH 服务器进行 DNS 通信的历史记录。查找结果详细信息中的 “异常” 字段可以提供有关所查询的 DoH 服务器的信息。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 实例正在通过 TLS 进行不寻常的 DNS (DoT) 通信。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例的行为偏离了既定基准。此 EC2 实例最近没有任何通过 TLS 的 DNS (DoT) 与该公共 DoT 服务器进行通信的历史记录。查找结果详细信息面板中的 “异常” 字段可以提供有关所查询的 DoT 服务器的信息。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Impact:EC2/AbusedDomainRequest.Reputation

EC2 实例正在查询与已知的滥用域名相关的低信誉域名。

默认严重性：中等

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中列出的 Amazon EC2 实例正在查询与已知的滥用域或 IP 地址相关的低信誉域名。滥用域名的例子包括提供免费子域名注册的顶级域名 (TLD) 和二级域名 (2LD) 以及动态 DNS 提供商。威胁行为者倾向于使用这些服务免费或低成本注册域名。此类别中的低信誉域名也可能是解析为注册商的停用 IP 地址的过期域名，因此可能不再有效。Parking IP 是注册商引导流量前往未链接到任何服务的域名的地方。列出的 Amazon EC2 实例可能会遭到入侵，因为威胁参与者通常使用这些注册商或服务进行 C&C 和恶意软件分发。

低信誉域基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其成为恶意域名的可能性。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 实例正在查询与加密货币相关活动相关的低信誉域名。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您Amazon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。比特币是对比特币挖矿的奖励，受到威胁者的高度追捧。

低信誉域基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其成为恶意域名的可能性。

补救建议：

如果您使用此 EC2 实例挖矿或管理加密货币，或者此实例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Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。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 `Impact:EC2/BitcoinDomainRequest.Reputation`。第二个筛选条件应是涉及区块链活动的实例的 Instance ID (实例 ID)。要了解有关创建隐藏规则的更多信息，请参阅抑制规则 (p. 187)。

如果此活动是意外活动，您的实例可能会受到攻击，请参阅修复受感染的 EC2 实例 (p. 213)。

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 实例正在查询与已知恶意域相关的低信誉域。

默认严重性：高

- 数据来源：DNS 日志

此发现告知您，您Amazon环境中列出的 Amazon EC2 实例正在查询与已知恶意域或 IP 地址相关的低信誉域名。例如，域可能与已知的污水坑 IP 地址相关联。Sinkholed 域名是以前由威胁行为者控制的域名，向它们发出的请求可能表明该实例已被入侵。这些域名也可能与已知的恶意活动或域名生成算法相关。

低信誉域基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其成为恶意域名的可能性。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Impact:EC2/PortSweep

EC2 实例正在探测大量 IP 地址上的端口。

默认严重性：高

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例正在探测大量可公开路由 IP 地址上的端口。此类活动通常用于寻找易受攻击的主机。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

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 实例正在查询低信誉域名，该域名本质上是可疑的，因为该域名已过时或不受欢迎程度。

默认严重性：低

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中列出的 Amazon EC2 实例正在查询一个可疑为恶意的低信誉域名。注意到该域的特征与之前观察到的恶意域一致，但是，我们的声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，或者接收的流量很少。

低信誉域基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其成为恶意域名的可能性。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Impact:EC2/WinRMBruteForce

一个 EC2 实例正在执行出站 Windows 远程管理暴力攻击。

默认严重性：低*

> Note
>
> 如果您的 EC2 实例是暴力攻击的目标，则此发现的严重性很低。如果您的 EC2 实例是用于执行暴力攻击的参与者，则此发现的严重性很高。

- 数据源：VPC 流日志

此发现告知您，您的Amazon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 的系统上获取 Windows 远程管理服务的访问权限。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Recon:EC2/PortProbeEMRUnprotectedPort

EC2 实例具有未受保护的 EMR 相关端口，已知的恶意主机正在探测该端口。

默认严重性：高

- 数据源：VPC 流日志

此发现告知您，列出的 EC2 实例上属于您Amazon环境中集群的一部分的与 EMR 相关的敏感端口未被安全组、访问控制列表 (ACL) 或 Linux IPtables 等主机防火墙阻止，并且互联网上的已知扫描程序正在积极探测该端口。可以触发此发现的端口，例如端口 8088（YARN Web UI 端口），可能用于远程代码执行。

补救建议：

您应阻止从 Internet 开放访问集群上的端口，并限制仅访问需要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。

默认严重性：低*

> Note
>
> 此发现的默认严重性为 “低”。但是，如果正在探测的端口由（9200 或 9300）使用，则发现的严重性为 “高”。

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例上的端口未被安全组、访问控制列表 (ACL) 或 Linux IPTables 等主机防火墙阻止，并且互联网上的已知扫描程序正在积极探测该端口。

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，请参阅为 Windows 实例授权入站流量。

补救建议：

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Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪个标准。有关创建禁止规则的更多信息，请参阅抑制规则 (p. 187)。

如果此活动是意外活动，您的实例可能会受到攻击，请参阅修复受感染的 EC2 实例 (p. 213)。

Recon:EC2/Portscan

EC2 实例正在执行对远程主机的出站端口扫描。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例可能参与了端口扫描攻击，因为它试图在短时间内连接到多个端口。端口扫描攻击的目的是找到打开的端口，以发现计算机正在运行哪些服务并识别其操作系统。

补救建议：

当在您的环境中的 EC2 实例上部署漏洞评估应用程序时，此发现可能是误报，因为这些应用程序会进行端口扫描，提醒您注意未正确配置的开放端口。如果您的Amazon环境属于这种情况，我们建议您为此发现设

置抑制规则。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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪些标准。有关创建禁止规则的更多信息，请参阅抑制规则 (p. 187)。

如果此活动是意外活动，您的实例可能会受到攻击，请参阅修复受感染的 EC2 实例 (p. 213)。

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。

默认严重性：中等

- 数据源：VPC 流日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例可能会受到威胁，因为它正在尝试与黑洞（或沉孔）的 IP 地址通信。黑洞是网络中传入或传出的流量在不告知来源数据未到达预定接收方的情况下被默默丢弃的地方。黑洞 IP 地址指定没有运行的主机或者未分配主机的地址。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Trojan:EC2/BlackholeTraffic!DNS

EC2 实例正在查询重定向到黑洞 IP 地址的域名。

默认严重性：中等

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例可能会遭到入侵，因为它正在查询被重定向到黑洞 IP 地址的域名。黑洞是网络中传入或传出的流量在不告知来源数据未到达预定接收方的情况下被默默丢弃的地方。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon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 实例可能遭盗用。

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成员发出命令的计算机，僵尸网络是一组受常见恶意软件感染和控制的联网设备。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

这一发现基于使用高级启发式方法对域名的分析，可能会识别出威胁情报源中不存在的新 DGA 域。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon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 实例可能遭盗用。

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成员发出命令的计算机，僵尸网络是一组受常见恶意软件感染和控制的联网设备。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的已知DGA域。 GuardDuty

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Trojan:EC2/DNSDataExfiltration

EC2 实例通过 DNS 查询泄露数据。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中列出的 EC2 实例正在运行使用 DNS 查询进行出站数据传输的恶意软件。这种类型的数据传输表明实例已被泄露，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。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：高

- 数据来源：DNS 日志

此发现告知您，您的Amazon环境中列出的 EC2 实例可能会遭到入侵，因为它正在查询远程主机的域名，而该域名是偷渡式下载攻击的已知来源。这些是从互联网意外下载的计算机软件，可能会触发病毒、间谍软件或恶意软件的自动安装。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：中等

- 数据源：VPC 流日志

此发现告知您，您Amazon环境中的 EC2 实例正试图与已知持有恶意软件捕获的证书和其他被盗数据的远程主机的 IP 地址进行通信。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Trojan:EC2/DropPoint!DNS

EC2 实例正在查询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域名。

默认严重性：中等

- 数据来源：DNS 日志

此发现告知您，您Amazon环境中的 EC2 实例正在查询远程主机的域名，该主机已知持有恶意软件捕获的证书和其他被盗数据。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Trojan:EC2/PhishingDomainRequest!DNS

EC2 实例正在查询涉及网络钓鱼攻击的域。您的 EC2 实例可能遭盗用。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中有一个 EC2 实例正在尝试查询涉及网络钓鱼攻击的域。网络钓鱼域名是由冒充合法机构的人设置的，目的是诱使个人提供敏感数据，例如个人身份信息、银行和信用卡详细信息以及密码。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，或者它可能正在尝试设置网络钓鱼网站。您的 EC2 实例可能遭盗用。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

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。

默认严重性：中等

- 数据源：VPC 流日志

此发现告知您，您Amazon环境中的 EC2 实例正在与您上传的威胁列表中包含的 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。用于生成此调查结果的威胁列表将在调查结果的详细信息中列出。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 实例正在执行解析为实例元数据服务的 DNS 查询。

默认严重性：高

- 数据来源：DNS 日志

此发现告诉您，您的Amazon环境中的 EC2 实例正在查询解析为 EC2 元数据 IP 地址 (169.254.169.254) 的域。此类的 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 重新绑定包括欺骗在 EC2 实例上运行的应用程序从 URL 加载返回数据，其中 URL 中的域名解析为 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，并可能使其为攻击者所用。

只有当 EC2 实例正在运行允许注入 URL 的易受攻击的应用程序，或者有人在 EC2 实例上运行的 Web 浏览器中访问该 URL 时，才有可能使用 DNS 重新绑定访问 EC2 元数据。

补救建议：

为了回应这一发现，您应该评估 EC2 实例上是否有漏洞的应用程序在运行，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，您应该修复漏洞。如果有人浏览了已识别的域，则应屏蔽该域或阻止用户访问该域。如果您确定此发现与上述任一案例有关，请撤消与 EC2 实例关联的会话。

一些Amazon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 `UnauthorizedAccess:EC2/MetaDataDNSRebind`。第二个筛选条件应为 DNS request domain (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 (p. 187)。

UnauthorizedAccess:EC2/RDPBruteForce

EC2 实例涉及到 RDP 暴力攻击中。

默认严重性：低*

> **Note**
>
> 如果您的 EC2 实例是暴力攻击的目标，则此发现的严重性很低。如果您的 EC2 实例是用于执行暴力攻击的参与者，则此发现的严重性很高。

- 数据源：VPC 流日志

此发现告诉您，您Amazon环境中的 EC2 实例参与了暴力攻击，该攻击旨在获取基于 Windows 的系统上的 RDP 服务的密码。这可能表示未经授权访问您的Amazon资源。

补救建议：

如果您的实例的资源角色是`ACTOR`，则表示您的实例已被用于执行 RDP 暴力攻击。除非此实例有正当理由联系列出的 IP 地址`Target`，否则建议您假设您的实例已被入侵，然后采取中列出的操作修复受感染的 EC2 实例 (p. 213)。

如果您的实例的资源角色为`TARGET`，则可以通过安全组、ACL 或防火墙将 RDP 端口保护到可信 IP，从而纠正这一发现。有关更多信息，请参阅保护 EC2 实例的提示 (Linux)。

UnauthorizedAccess:EC2/SSHBruteForce

EC2 实例涉及到 SSH 暴力攻击中。

默认严重性：低*

Note

如果暴力攻击针对的是您的一个 EC2 实例，则此发现的严重性较低。如果您的 EC2 实例被用来执行暴力攻击，则此发现的严重性很高。

- 数据源：VPC 流日志

此发现告诉您，您Amazon环境中的 EC2 实例参与了暴力攻击，该攻击旨在获取基于 Linux 的系统上的 SSH 服务的密码。这可能表示未经授权访问您的Amazon资源。

Note

此调查结果仅通过在端口 22 上监控流量的 生成。如果 SSH 服务配置为使用其他端口，则不会生成此调查结果。

补救建议：

如果暴力攻击的目标是堡垒主机，则这可能代表您的Amazon环境的预期行为。如果是这种情况，我们建议您为此调查结果设置禁止规则。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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪些标准。有关创建禁止规则的更多信息，请参阅抑制规则 (p. 187)。

如果您的环境预计不会出现此活动，而您的实例的资源角色是，则可以通过安全组TARGET、ACL 或防火墙将 SSH 端口仅保护到可信 IP 来纠正这一发现。有关更多信息，请参阅保护 EC2 实例的提示 (Linux)。

如果您的实例的资源角色是`ACTOR`，则表示该实例已被用于执行 SSH 暴力攻击。除非此实例有正当理由联系列出的 IP 地址`Target`，否则建议您假设您的实例已被入侵，然后采取中列出的操作修复受感染的 EC2 实例 (p. 213)。

UnauthorizedAccess:EC2/TorClient

EC2 实例正在连接到一个 Tor Guard 或 Authority 节点。

默认严重性：高

- 数据源：VPC 流日志

这个发现告诉你，你的Amazon环境中的 EC2 实例正在连接到 Tor Guard 或权威节点。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。这些流量可能表明此 EC2 实例已被入侵，正在充当 Tor 网络上的客户端。此发现可能表明未经授权访问您的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

UnauthorizedAccess:EC2/TorRelay

EC2 实例正在以 Tor 中继身份连接到 Tor 网络。

默认严重性：高

- 数据源：VPC 流日志

这个发现告诉你，你Amazon环境中的 EC2 实例正在与 Tor 网络建立连接，这表明它在充当 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性。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅 修复受感染的 EC2 实例 (p. 213)。

EKS 运行时监控查找类型

亚马逊GuardDuty生成以下 EKS 运行时监控结果，根据来自 Amazon EKS 集群中 EC2 主机和容器的操作系统级行为来指出潜在威胁。

> **Note**
>
> 运行时监控查找类型基于从主机收集的运行时日志。日志包含诸如文件路径之类的字段，这些字段可能由恶意行为者控制。这些字段还包含在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审查。例如，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 (p. 112)
- Backdoor:Runtime/C&CActivity.B (p. 112)
- UnauthorizedAccess:Runtime/TorRelay (p. 113)
- UnauthorizedAccess:Runtime/TorClient (p. 113)
- Trojan:Runtime/BlackholeTraffic (p. 114)
- Trojan:Runtime/DropPoint (p. 114)
- CryptoCurrency:Runtime/BitcoinTool.B!DNS (p. 115)
- Backdoor:Runtime/C&CActivity.B!DNS (p. 115)
- Trojan:Runtime/BlackholeTraffic!DNS (p. 116)
- Trojan:Runtime/DropPoint!DNS (p. 116)
- Trojan:Runtime/DGADomainRequest.C!DNS (p. 116)
- Trojan:Runtime/DriveBySourceTraffic!DNS (p. 117)
- Trojan:Runtime/PhishingDomainRequest!DNS (p. 117)
- Impact:Runtime/AbusedDomainRequest.Reputation (p. 118)
- Impact:Runtime/BitcoinDomainRequest.Reputation (p. 118)
- Impact:Runtime/MaliciousDomainRequest.Reputation (p. 119)
- Impact:Runtime/SuspiciousDomainRequest.Reputation (p. 119)
- UnauthorizedAccess:Runtime/MetadataDNSRebind (p. 120)
- Execution:Runtime/NewBinaryExecuted (p. 120)
- PrivilegeEscalation:Runtime/DockerSocketAccessed (p. 121)
- PrivilegeEscalation:Runtime/RuncContainerEscape (p. 121)
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified (p. 122)
- DefenseEvasion:Runtime/ProcessInjection.Proc (p. 122)
- DefenseEvasion:Runtime/ProcessInjection.Ptrace (p. 123)

- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite (p. 123)
- Execution:Runtime/ReverseShell (p. 123)
- DefenseEvasion:Runtime/FilelessExecution (p. 124)
- Impact:Runtime/CryptoMinerExecuted (p. 124)
- Execution:Runtime/NewLibraryLoaded (p. 124)
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory (p. 125)
- PrivilegeEscalation:Runtime/UserfaultfdUsage (p. 125)

CryptoCurrency:Runtime/BitcoinTool.B

Amazon EC2 实例或容器正在查询与加密货币相关活动相关的 IP 地址。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您Amazon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相关的 IP 地址。威胁参与者可能会试图控制计算资源，恶意将其重新用于未经授权的加密货币挖矿。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果您使用此 EC2 实例或容器来开采或管理加密货币，或者其中任何一个以其他方式参与区块链活动，则该CryptoCurrency:Runtime/BitcoinTool.B发现可能代表您环境的预期活动。如果您的Amazon环境是这种情况，我们建议您为此发现设置禁止规则。禁止规则应由两个筛选条件组成。第一个筛选条件应使用值为的查找类型属性`CryptoCurrency:Runtime/BitcoinTool.B`。第二个筛选条件应该是实例的实例 ID 或参与加密货币或区块链相关活动的容器的容器映像 ID。有关更多信息，请参阅禁止规则。

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重性：高

- 功能：运行时监控

此发现通知您，列出的 EC2 实例或Amazon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遭到入侵。命令和控制服务器是向僵尸网络成员发出命令的计算机。

僵尸网络是一组连接互联网的设备，可能包括受常见恶意软件感染和控制的 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。

Note

如果查询的 IP 与 log4j 相关，则相关调查结果的字段将包含以下值：

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

UnauthorizedAccess:Runtime/TorRelay

您的 Amazon EC2 实例或容器正作为 Tor 中继与 Tor 网络建立连接。

默认严重性：高

- 功能：运行时监控

这一发现告诉您，您的Amazon环境中的 EC2 实例或容器正在与 Tor 网络建立连接，这表明它充当了 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性。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

UnauthorizedAccess:Runtime/TorClient

您的亚马逊 EC2 实例或容器正在与 Tor Guard 或授权节点建立连接。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您的Amazon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

实例或容器可能已被入侵，并在 Tor 网络上充当客户端。此发现可能表明未经授权访问了您的Amazon资源，目的是隐藏攻击者的真实身份。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Trojan:Runtime/BlackholeTraffic

Amazon EC2 实例或容器正试图与已知黑洞的远程主机的 IP 地址进行通信。

默认严重程度：中

- 功能：运行时监控

这一发现告诉您，列出的 EC2 实例或Amazon环境中的容器可能遭到入侵，因为它正在尝试与黑洞（或沉洞）的 IP 地址通信。黑洞是指网络中传入或传出的流量在不通知来源数据未到达预定接收方的情况下静默丢弃的地方。黑洞 IP 地址指定没有运行的主机或者未分配主机的地址。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Trojan:Runtime/DropPoint

Amazon EC2 实例或容器正试图与已知持有恶意软件捕获的证书和其他被盗数据的远程主机的 IP 地址进行通信。

默认严重程度：中

- 功能：运行时监控

这一发现通知您，您的Amazon环境中的 EC2 实例或容器正试图与已知持有证书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。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Amazon EC2 实例或容器正在查询与加密货币活动相关的域名。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您Amazon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相关的域名。威胁参与者可能会试图控制计算资源，以便恶意将其重新用于未经授权的加密货币挖矿。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果您使用此 EC2 实例或容器来开采或管理加密货币，或者其中任何一个以其他方式参与区块链活动，则该CryptoCurrency:Runtime/BitcoinTool.B!DNS发现可能是您的环境的预期活动。如果您的Amazon环境是这种情况，我们建议您为此发现设置禁止规则。抑制规则应包含两个过滤标准。第一个条件应使用 Finding type (调查结果类型) 属性，其值为 `CryptoCurrency:Runtime/BitcoinTool.B!DNS`。第二个筛选条件应该是实例的实例 ID 或参与加密货币或区块链活动的容器的容器映像 ID。有关更多信息，请参阅禁止规则。

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重性：高

- 功能：运行时监控

此发现通知您，列出的 EC2 实例或Amazon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成员发出命令的计算机。

僵尸网络是一组连接互联网的设备，可能包括受常见恶意软件感染和控制的 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。

Note

如果查询的域名与 log4j 相关，则相关查找结果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 `nslookup` Windows）针对测试域发出 DNS 请求`guarddutyc2activityb.com`。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重程度：中

- 功能：运行时监控

此发现告知您列出的 EC2 实例或Amazon环境中的容器可能遭到入侵，因为它正在查询被重定向到黑洞 IP 地址的域名。黑洞是指网络中传入或传出的流量在不通知来源数据未到达预定接收方的情况下静默丢弃的地方。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Trojan:Runtime/DropPoint!DNS

Amazon EC2 实例或容器正在查询远程主机的域名，该域名已知持有恶意软件捕获的证书和其他被盗数据。

默认严重程度：中

- 功能：运行时监控

这一发现告知您，您的Amazon环境中的 EC2 实例或容器正在查询远程主机的域名，该域名已知持有恶意软件捕获的凭证和其他被盗数据。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Trojan:Runtime/DGADomainRequest.C!DNS

Amazon EC2 实例或容器正在查询通过算法生成的域。此类域通常被恶意软件使用，可能表明 EC2 实例或容器受损。

默认严重性：高

- 功能：运行时监控

此发现通知您，您Amazon环境中列出的 EC2 实例或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。

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成员发出命令的计算机，僵尸网络是受一种常见恶意软件感染和控制的互联网连接设备的集合。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。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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 Drive-By 下载攻击的已知来源。

默认严重性：高

- 功能：运行时监控

这一发现告诉您，您Amazon环境中列出的 EC2 实例或容器可能遭到入侵，因为它正在查询远程主机的域名，该域名是已知的偷渡式下载攻击来源。这些是从互联网意外下载的计算机软件，可以启动病毒、间谍软件或恶意软件的自动安装。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Trojan:Runtime/PhishingDomainRequest!DNS

Amazon EC2 实例或容器正在查询参与网络钓鱼攻击的域名。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您的Amazon环境中有一个 EC2 实例或容器正试图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，目的是诱使个人提供敏感数据，例如个人身份信息、银行和信用卡详细信息以及密码。您的 EC2 实例或容器可能正在尝试检索存储在钓鱼网站上的敏感数据，或者它可能正在尝试建立网络钓鱼网站。您的 EC2 实例或容器可能遭到入侵。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Impact:Runtime/AbusedDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与已知滥用域名相关的低信誉域名。

默认严重程度：中

- 功能：运行时监控

此发现通知您，您Amazon环境中列出的 EC2 实例或容器正在查询与已知的滥用域名或 IP 地址相关的低信誉域名。滥用域名的示例包括提供免费子域名注册的顶级域名 (TLD) 和二级域名 (2LD) 以及动态 DNS 提供商。威胁参与者倾向于使用这些服务免费或低成本注册域名。此类别中的低信誉域名也可能是解析到注册商的停放 IP 地址的过期域名，因此可能不再处于活动状态。parking IP 是注册商引导未链接到任何服务的域名的流量。列出的 Amazon EC2 实例或容器可能会遭到入侵，因为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。

低信誉域名基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其恶意的可能性。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Impact:Runtime/BitcoinDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与加密货币相关活动相关的低信誉域名。

默认严重性：高

- 功能：运行时监控

这一发现通知您，列出的EC2实例或Amazon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。威胁参与者可能会试图控制计算资源，恶意将其重新用于未经授权的加密货币挖矿。

低信誉域名基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其恶意的可能性。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果您使用此 EC2 实例或容器来开采或管理加密货币，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Amazon环境是这种情况，我们建议您为此发现设置禁止规则。禁止规则应由两个筛选条件组成。第一个筛选条件应使用值为的查找类型属性`Impact:Runtime/BitcoinDomainRequest.Reputation`。第二个筛选条件应该是实例的实例 ID 或者容器的容器映像 ID 涉及加密货币或区块链相关活动。有关更多信息，请参阅禁止规则。

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Impact:Runtime/MaliciousDomainRequest.Reputation

Amazon EC2 实例或容器正在查询与已知恶意域相关的低信誉域名。

默认严重性：高

- 功能：运行时监控

此发现通知您，您Amazon环境中列出的 EC2 实例或容器正在查询与已知恶意域或 IP 地址相关的低信誉域名。例如，域可能与已知的污水洞 IP 地址相关联。Sinkholed 域是以前由威胁参与者控制的域，向它们发出的请求可能表明该实例已被入侵。这些域名也可能与已知的恶意活动或域名生成算法相关。

低信誉域名基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其恶意的可能性。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Impact:Runtime/SuspiciousDomainRequest.Reputation

Amazon EC2 实例或容器正在查询低信誉的域名，该域名因其年代久远或受欢迎程度低而在本质上是可疑的。

默认严重性：低

- 功能：运行时监控

这一发现通知您，您Amazon环境中列出的 EC2 实例或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明确将其与已知威胁联系起来。这些域通常是新观察到的，或者接收的流量很少。

低信誉域名基于信誉评分模型。该模型对域名的特征进行评估和排序，以确定其恶意的可能性。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

UnauthorizedAccess:Runtime/MetadataDNSRebind

Amazon EC2 实例或容器正在执行解析为实例元数据服务的 DNS 查询。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您的Amazon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，包括与该实例相关的 IAM 证书。

DNS 重新绑定涉及欺骗在 EC2 实例上运行的应用程序从 URL 加载返回数据，其中 URL 中的域名解析为 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，并可能使其为攻击者所用。

只有当 EC2 实例正在运行允许注入 URL 的易受攻击的应用程序，或者有人在 EC2 实例上运行的 Web 浏览器中访问该 URL 时，才有可能使用 DNS 重新绑定访问 EC2 元数据。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

作为对这一发现的回应，您应评估 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。如果根本原因是存在漏洞的应用程序，请修复该漏洞。如果有人浏览了已识别的域，请封锁该域或阻止用户访问该域。如果您确定此发现与上述任一案例有关，请撤消与 EC2 实例关联的会话。

一些Amazon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。第一个筛选条件应使用值为的查找类型属性`UnauthorizedAccess:Runtime/MetaDataDNSRebind`。第二个过滤条件应该是容器的 DNS 请求域或容器镜像 ID。DNS 请求域值应与您映射到元数据 IP 地址的域相匹配 (`169.254.169.254`)。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，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Execution:Runtime/NewBinaryExecuted

容器中新创建或最近修改的二进制文件已执行。

默认严重程度：中

- 功能：运行时监控

此发现通知您，容器中新创建或最近修改的二进制文件已执行。最佳做法是在运行时保持容器不可变，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。非常怀疑新创建的二进制文件是在容器环境中执行的。这种行为表明恶意行为者已经获得了工作负载的访问权限，并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。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

PrivilegeEscalation:Runtime/DockerSocketAccessed

容器内的进程正在使用 Docker 套接字与 Docker 守护程序通信。

默认严重程度：中

- 功能：运行时监控

Docker 套接字是一个 Unix 域套接字，Docker 守护程序 (`dockerd`) 使用它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 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 Docket 套接字通信并创建特权容器来逃离容器并获得主机级访问权限。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

PrivilegeEscalation:Runtime/RuncContainerEscape

检测到有人试图获取容器主机访问权限。

默认严重性：高

- 功能：运行时监控

这一发现告知您主机的 runC 二进制文件可能已被覆盖。runC 是低级容器运行时，如 Docker 和 Containerd，用于生成和运行容器。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。过去的一个众所周知的漏洞（CVE-2019-5736 D etail）允许恶意容器覆盖主机的 runC 二进制文件，并在执行修改后的 runC 二进制文件时获得对主机的根级访问权限。

这一发现还可能表明恶意行为者可能在以下两种类型的容器之一中执行了命令：

- 带有攻击者控制图像的新容器。
- 以前具有写入权限的攻击者可以访问的现有容器。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

在 Amazon EKS 集群中检测到通过 runC 逃出容器。

默认严重性：高

- 功能：运行时监控

此发现通知您，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 cgroup 都有一个发布代理文件 (`release_agent`)，这是 Linux 在 cgroup 内部的任何进程终止时执行的脚本。发布代理文件总是在主机级别执行。容器内的威胁参与者可以通过向属于 cgroup 的发布代理文件写入任意命令来逃往主机。当该 cgroup 内部的进程终止时，由操作者编写的命令就会被执行。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重性：高

- 功能：运行时监控

进程注入是威胁参与者用来向进程注入代码以逃避防御并可能提升权限的一种技术。proc 文件系统 (procfs) 是 Linux 中的一种特殊文件系统，它将进程的虚拟内存呈现为文件。该文件的路径是`/proc/PID/mem`，其中`PID`是进程的唯一 ID。威胁参与者可以写入此文件以将代码注入进程。这一发现发现发现了可能有人试图写入此文件。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源类型可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重程度：中

- 功能：运行时监控

进程注入是威胁参与者用来向进程注入代码以逃避防御并可能提升权限的一种技术。一个进程可以使用 ptrace 系统调用将代码注入另一个进程。这一发现表明有人可能试图使用 ptrace 系统调用向进程注入代码。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源类型可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

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。

默认严重性：高

- 功能：运行时监控

进程注入是威胁参与者用来向进程注入代码以逃避防御并可能提升权限的一种技术。一个进程可以使用系统调用，例如`process_vm_writev`将代码直接注入另一个进程的虚拟内存中。这一发现表明有人可能试图使用系统调用向进程注入代码以写入该进程的虚拟内存。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源类型可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Execution:Runtime/ReverseShell

容器或 Amazon EC2 实例中的进程创建了反向外壳。

默认严重性：高

- 功能：运行时监控

反向 shell 是在从目标主机到角色主机的连接上创建的 shell 会话。这与从角色的主机启动到目标宿主的普通外壳相反。威胁行为者在获得对目标的初始访问权限后，会创建反向外壳以对目标执行命令。这一发现表明有人可能试图制造反向外壳。

补救建议：

如果此活动出乎意料，则您的资源类型可能已遭到破坏。

DefenseEvasion:Runtime/FilelessExecution

容器或 Amazon EC2 实例中的进程正在执行内存中的代码。

默认严重程度：中

- 功能：运行时监控

此发现会通知您何时使用磁盘上的内存中的可执行文件执行进程。这是一种常见的防御规避技术，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。尽管恶意软件使用了这种技术，但它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。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

Impact:Runtime/CryptoMinerExecuted

容器或 Amazon EC2 实例正在执行与加密货币挖矿活动相关的二进制文件。

默认严重性：高

- 功能：运行时监控

这一发现通知您，您的Amazon环境中的容器或 EC2 实例正在执行与加密货币挖矿活动相关的二进制文件。威胁参与者可能会试图控制计算资源，恶意将其重新用于未经授权的加密货币挖矿。

运行时代理监视来自多种资源类型的事件。要识别可能被盗的资源，请在GuardDuty控制台的发现面板中查看资源类型。

补救建议：

运行时代理监视来自多个资源的事件。要识别受影响的资源，请在GuardDuty控制台的发现详细信息中查看资源类型，然后参见修复 EKS 运行时监控结果 (p. 220)。

Execution:Runtime/NewLibraryLoaded

新创建或最近修改的库由容器内的进程加载。

默认严重程度：中

- 功能：运行时监控

这一发现告诉你，一个库是在运行时在容器内创建或修改的，并由容器内运行的进程加载。最佳做法是在运行时保持容器不可变，而不是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表示存在可疑活动。此行为表明恶意行为者可能获得了容器的访问权限，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。

运行时代理监视来自多个资源的事件。要识别受影响的资源，请在GuardDuty控制台的发现详细信息中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

容器内的进程在运行时挂载了主机文件系统。

默认严重程度：中

- 功能：运行时监控

多容器转义技术涉及在运行时在容器内安装主机文件系统。这一发现告诉你，容器内的某个进程可能试图装载主机文件系统，这可能表明有人试图逃到主机。

运行时代理监视来自多个资源的事件。要识别受影响的资源，请在GuardDuty控制台的发现详细信息中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅修复 EKS 运行时监控结果 (p. 220)：

PrivilegeEscalation:Runtime/UserfaultfdUsage

容器内的进程在运行时挂载了主机文件系统。

默认严重程度：中

- 功能：运行时监控

通常，页面错误由内核空间中的内核处理。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。这是一项有用的功能，可以实现用户空间文件系统。另一方面，它也可能被潜在的恶意进程用来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赛窗口。使用`userfaultfd`可能表示亚马逊弹性计算云 (Amazon EC2) 实例上存在可疑活动。

运行时代理监视来自多个资源的事件。要识别受影响的资源，请在GuardDuty控制台的发现详细信息中查看资源类型。

补救建议：

如果此活动出乎意料，则您的资源可能已遭到破坏。有关更多信息，请参阅 修复 EKS 运行时监控结果 (p. 220)。

GuardDuty IAM 查找类型

以下发现特定于 IAM 实体和访问密钥，且资源类型始终为AccessKey。发现的严重程度和详细信息因发现类型而异。

此处列出的发现包括用于生成该发现类型的数据源和模型。有关更多信息，请参阅基础数据来源 (p. 14)：

对于所有与 IAM 相关的调查结果，我们建议您检查相关实体，确保其权限遵循最低权限的最佳实践。如果活动出乎意料，则凭证可能会被泄露。有关修复发现的信息，请参阅修复被盗的凭证 Amazon (p. 215)。

主题

- CredentialAccess:IAMUser/AnomalousBehavior (p. 126)
- DefenseEvasion:IAMUser/AnomalousBehavior (p. 127)
- Discovery:IAMUser/AnomalousBehavior (p. 127)
- Exfiltration:IAMUser/AnomalousBehavior (p. 128)
- Impact:IAMUser/AnomalousBehavior (p. 128)
- InitialAccess:IAMUser/AnomalousBehavior (p. 129)
- PenTest:IAMUser/KaliLinux (p. 129)
- PenTest:IAMUser/ParrotLinux (p. 129)
- PenTest:IAMUser/PentooLinux (p. 130)
- Persistence:IAMUser/AnomalousBehavior (p. 130)
- Policy:IAMUser/RootCredentialUsage (p. 130)
- PrivilegeEscalation:IAMUser/AnomalousBehavior (p. 131)
- Recon:IAMUser/MaliciousIPCaller (p. 131)
- Recon:IAMUser/MaliciousIPCaller.Custom (p. 132)
- Recon:IAMUser/TorIPCaller (p. 132)
- Stealth:IAMUser/CloudTrailLoggingDisabled (p. 132)
- Stealth:IAMUser/PasswordPolicyChange (p. 133)
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B (p. 133)
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS (p. 133)
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS (p. 134)
- UnauthorizedAccess:IAMUser/MaliciousIPCaller (p. 135)
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom (p. 135)
- UnauthorizedAccess:IAMUser/TorIPCaller (p. 135)

CredentialAccess:IAMUser/AnomalousBehavior

用于获取Amazon环境访问权限的 API 是以异常方式调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与攻击的凭证访问阶段相关，此时对手试图收集您的环境的密码、用户名和访问密钥。此类别中的 API 是`GetPasswordData`、`GetSecretValue`、和`GenerateDbAuthToken`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

DefenseEvasion:IAMUser/AnomalousBehavior

用于逃避防御措施的 API 以一种反常的方式被调用。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与防御逃避策略有关，在这种策略中，对手试图掩盖自己的踪迹并避开侦查。此类别中的 API 通常是删除、禁用或停止操作，例如`DeleteFlowLogs`、`DisableAlarmActions`、或`StopLogging`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Discovery:IAMUser/AnomalousBehavior

通常用于发现资源的 API 是以异常方式调用的。

默认严重性：低

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与攻击的发现阶段有关，此时对手正在收集信息以确定您的Amazon环境是否容易受到更广泛的攻击。此类别中的 API 通常是获取、描述或列表操作，例如`DescribeInstances`、`GetRolePolicy`、或`ListAccessKeys`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Exfiltration:IAMUser/AnomalousBehavior

通常用于从Amazon环境收集数据的 API 是以异常方式调用的。

默认严重性：高

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与渗透策略有关，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。此查找类型的 API 仅为管理（控制平面）操作，通常与 S3、快照和数据库相关，例如`PutBucketReplication`、`CreateSnapshot`、或`RestoreDBInstanceFromDBSnapshot`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Impact:IAMUser/AnomalousBehavior

通常用于在Amazon环境中篡改数据或进程的 API 是以异常方式调用的。

默认严重性：高

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与影响策略有关，即对手试图破坏操作并操纵、中断或破坏您账户中的数据。此查找结果类型的 API 通常是删除、更新或放置操作，例如`DeleteSecurityGroup`、`UpdateUser`、或`PutBucketPolicy`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

InitialAccess:IAMUser/AnomalousBehavior

通常用于未经授权访问Amazon环境的 API 是以异常方式调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与攻击的初始访问阶段相关，此时攻击的初始访问阶段正试图建立对环境的访问权限。此类别中的 API 通常是获取令牌或会话操作，例如`GetFederationToken`、`StartSession`、或`GetAuthorizationToken`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

PenTest:IAMUser/KaliLinux

一个 API 是从 Kali Linux EC2 机器上调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告诉您，运行 Kali Linux 的计算机正在使用属于您的环境中列出Amazon账户的证书进行 API 调用。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。攻击者也会使用此工具来寻找 EC2 配置漏洞和获取对您 Amazon 环境未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

PenTest:IAMUser/ParrotLinux

API 是从 Parrot Security Linux 计算机上调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告诉您，运行 Parrot Security Linux 的计算机正在使用属于您的环境中列出Amazon账户的证书进行 API 调用。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 Amazon 环境未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

PenTest:IAMUser/PentooLinux

一个 API 是从 Pentoo Linux 机器上调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告诉您，运行 Pentoo Linux 的计算机正在使用属于您的环境中列出Amazon帐户的凭据进行 API 调用。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。攻击者也会使用此工具来寻找 EC2 配置漏洞和获取对您 Amazon 环境未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Persistence:IAMUser/AnomalousBehavior

通常用于维护对Amazon环境的未经授权访问的 API 是以异常方式调用的。

默认严重性：中等

- 数据来源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与持久化策略有关，在这种策略中，对手已经获得了对您的环境的访问权限并试图保持该访问权限。此类别中的 API 通常是创建、导入或修改操作，例如`CreateAccessKey`、`ImportKeyPair`、或`ModifyInstanceAttribute`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Policy:IAMUser/RootCredentialUsage

API 是使用根用户登录凭证调用的。

默认严重性：低

- 数据源：CloudTrail 管理事件或 CloudTrail 数据事件

此发现告诉您，正在使用您的环境Amazon Web Services 账户中列出的根用户登录凭据向Amazon服务发出请求。建议用户切勿使用 root 用户登录凭据来访问Amazon服务。相反，应使用来自Amazon Security Token Service (STS) 的最低权限临时证书访问Amazon服务。Amazon STS对于不支持的情况，建议使用 IAM 用户证书。有关更多信息，请参阅 IAM 最佳实践。

Note

如果为账户启用了 S3 威胁检测，则此发现可能是为了响应尝试使用的 root 用户登录凭证在 S3 资源上运行 S3 数据平面操作而生成的Amazon Web Services 账户。所使用的 API 调用将在查找详细信息中列出。如果未启用 S3 威胁检测，则此发现只能由事件日志 API 触发。有关 S3 威胁检测的更多信息，请参阅 S3 保护。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

PrivilegeEscalation:IAMUser/AnomalousBehavior

通常用于获取Amazon环境高级权限的 API 是以异常方式调用的。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告知您，在您的账户中发现了异常 API 请求。此发现可能包括单个 API 或由单个用户身份在附近发出的一系列相关 API 请求。观察到的 API 通常与权限升级策略有关，在这种策略中，对手试图获得更高级别的环境权限。此类别中的 API 通常涉及更改 IAM 策略、角色和用户的操作，例如`AssociateIamInstanceProfile`、`AddUserToGroup`、或`PutUserPolicy`。

此 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的特定 API。有关调用请求的用户身份不同 API 请求的哪些因素的详细信息可以在查找详细信息中找到。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/MaliciousIPCaller

从已知恶意 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告诉您，可以列出或描述您环境中账户中的Amazon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Amazon资源进行这种类型的侦察，以找到更有价值的凭证或确定他们已经拥有的证书的功能。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/MaliciousIPCaller.Custom

从已知恶意 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告诉您，可以列出或描述您环境中账户中的Amazon资源的 API 操作是从包含在自定义威胁列表中的 IP 地址调用的。使用的威胁列表将在调查结果的详细信息中列出。攻击者可能会使用被盗的凭据对您的Amazon资源进行这种类型的侦察，以找到更有价值的凭证或确定他们已经拥有的凭据的能力。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/TorIPCaller

从 Tor 出口节点 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

这个发现告诉你，一个可以列出或描述你环境中账户中的Amazon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。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。攻击者会使用 Tor 来掩盖他们的真实身份。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Stealth:IAMUser/CloudTrailLoggingDisabled

Amazon CloudTrail日志记录已禁用。

默认严重性：低

- 数据源：CloudTrail 管理事件

此发现告知您Amazon环境中的 CloudTrail 一条路径已被禁用。这可能是攻击者在出于恶意目的获取对您的Amazon资源的访问权限的同时，试图通过消除其活动的任何痕迹来禁用日志记录以掩盖自己的踪迹。成功地删除或更新跟踪会触发此调查结果。成功删除存储与之关联的跟踪中的日志的 S3 存储桶也可以触发此发现 GuardDuty。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Stealth:IAMUser/PasswordPolicyChange

账户密码策略受损。

默认严重性：低*

> **Note**
>
> 此发现的严重性可以为低、中或高，具体取决于密码策略更改的严重性。

- 数据源：CloudTrail 管理事件

您的Amazon环境中列出的Amazon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Amazon账户密码策略也可能触发此发现。Amazon账户密码策略定义了管理可以为您的 IAM 用户设置哪种密码的规则。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。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

发现多个全球范围内的成功控制台登录。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此调查结果通知您，发现同一个 IAM 用户在不同地理位置，大约同一时间多次成功登录控制台。这种异常和危险的访问位置模式表明您的Amazon资源可能遭到未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

通过实例启动角色专门为 EC2 实例创建的证书正在使用其中的其他账户Amazon。

默认严重性：高*

> **Note**
>
> 此发现的默认严重性为 “高”。但是，如果该 API 是由与您的Amazon环境关联的账户调用的，则严重性为 “中”。

- 数据源：CloudTrail 管理事件或 S3 数据事件

此发现会告知您何时使用您的 EC2 实例证书从与运行相关 EC2 实例的Amazon账户不同的 IP 地址调用 API。

Amazon不建议在创建临时证书的实体（例如，Amazon应用程序、EC2 或 Lambda）之外重新分发临时证书。但是，授权用户可以从其 EC2 实例导出凭证以进行合法 API 调用。如果该`remoteAccountDetails.Affiliated`字段为，则`True`该 API 是从与您的Amazon环境关联的账户中调用的。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证的 IAM 用户。

补救建议：

为了回应这一发现，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`现场确定涉及的远程帐户。
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. 如果账户是关联账户，请联系远程账户所有者和 EC2 实例证书的所有者进行调查。
4. 如果账户没有关联关系，则首先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 证书的所有者，以确定远程账户是否存在使用这些证书的用例。
5. 如果证书的所有者无法识别远程帐户，则凭证可能已被在其中活动的威胁行为者泄露Amazon。您应该采取中建议的步骤修复受感染的 EC2 实例 (p. 213)来保护您的环境。此外，您可以向Amazon信任与安全团队提交滥用报告，开始对远程帐户进行调查。向Amazon Trust and Safety 提交报告时，请附上调查结果的完整 JSON 详细信息。

UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltration.OutsideAWS

通过实例启动角色专为某个 EC2 实例创建的凭证正在从外部 IP 地址使用。

默认严重性：高

- 数据源：CloudTrail 管理事件或 S3 数据事件

此发现告知您，外部的主机Amazon已尝试使用在您的Amazon环境中的 EC2 实例上创建的临时Amazon证书运行Amazon API 操作。列出的 EC2 实例可能已被泄露，此实例的临时证书可能已被泄露到外部的远程主机Amazon。 Amazon不建议在创建临时证书的实体（例如，Amazon应用程序、EC2 或 Lambda）之外重新分发临时证书。但是，授权用户可以从其 EC2 实例导出凭证以进行合法 API 调用。要排除潜在攻击并验证活动的合法性，请验证调查结果中是否预期会使用来自远程 IP 的实例证书。

补救建议：

当网络配置为路由互联网流量，使其从本地网关而不是从 VPC Internet Gateway (IGW) 传出时，就会生成此发现。常见配置，例如使用Amazon 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，我们建议您使用禁止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 (调查结果类型)，它应是 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`。第二个筛选条件是 API 调用者 IPv4 地址，其中

包含您的本地互联网网关的 IP 地址或 CIDR 范围。要了解有关创建隐藏规则的更多信息，请参阅抑制规则 (p. 187)。

Note

如果 GuardDuty 观察到来自外部来源的持续活动，其机器学习模型会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发现，并将随着时间的推移重新评估所学到的来源。

如果此活动是意外活动，则您的凭证可能已遭盗用，请参阅修复被盗的凭证 Amazon (p. 215)。

UnauthorizedAccess:IAMUser/MaliciousIPCaller

从已知恶意 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告知您 API 操作（例如，尝试启动 EC2 实例、创建新 IAM 用户或修改您的Amazon权限）是从已知的恶意 IP 地址调用的。这可能表示您环境中的Amazon资源遭到未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

从自定义威胁列表中的 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告知您 API 操作（例如，尝试启动 EC2 实例、创建新 IAM 用户或修改Amazon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。这可能表示您环境中的Amazon资源遭到未经授权的访问。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:IAMUser/TorIPCaller

从 Tor 出口节点 IP 地址调用了 API。

默认严重性：中等

- 数据源：CloudTrail 管理事件

此发现告知您 API 操作（例如，尝试启动 EC2 实例、创建新 IAM 用户或修改您的Amazon权限）是从 Tor 退出节点 IP 地址调用的。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您的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅 修复被盗的凭证 Amazon (p. 215)。

Kubernetes 审计日志查找类型

以下发现特定于 Kubernetes 资源，其资源类型为。 `EKSCluster`发现的严重程度和细节因发现类型而异。

对于所有 Kubernetes 类型的发现，我们建议您检查相关资源，以确定该活动是预期的还是潜在的恶意活动。有关修复发现中发现的受损的 Kubernetes 资源的指导，请参阅。GuardDuty 修复由发现的 EKS 审核日志监控结果 GuardDuty (p. 216)

> **Note**
>
> 如果产生这些发现的活动是预料之中的，可以考虑添加抑制规则 (p. 187)以防止将future 出现警报。

主题

- CredentialAccess:Kubernetes/MaliciousIPCaller (p. 137)
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom (p. 137)
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess (p. 138)
- CredentialAccess:Kubernetes/TorIPCaller (p. 138)
- DefenseEvasion:Kubernetes/MaliciousIPCaller (p. 138)
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom (p. 139)
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess (p. 139)
- DefenseEvasion:Kubernetes/TorIPCaller (p. 140)
- Discovery:Kubernetes/MaliciousIPCaller (p. 140)
- Discovery:Kubernetes/MaliciousIPCaller.Custom (p. 140)
- Discovery:Kubernetes/SuccessfulAnonymousAccess (p. 141)
- Discovery:Kubernetes/TorIPCaller (p. 141)
- Execution:Kubernetes/ExecInKubeSystemPod (p. 142)
- Impact:Kubernetes/MaliciousIPCaller (p. 142)
- Impact:Kubernetes/MaliciousIPCaller.Custom (p. 142)
- Impact:Kubernetes/SuccessfulAnonymousAccess (p. 143)
- Impact:Kubernetes/TorIPCaller (p. 143)
- Persistence:Kubernetes/ContainerWithSensitiveMount (p. 143)
- Persistence:Kubernetes/MaliciousIPCaller (p. 144)
- Persistence:Kubernetes/MaliciousIPCaller.Custom (p. 144)
- Persistence:Kubernetes/SuccessfulAnonymousAccess (p. 145)
- Persistence:Kubernetes/TorIPCaller (p. 145)
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount (p. 145)
- Policy:Kubernetes/AnonymousAccessGranted (p. 146)

- Policy:Kubernetes/ExposedDashboard (p. 146)
- Policy:Kubernetes/KubeflowDashboardExposed (p. 146)
- PrivilegeEscalation:Kubernetes/PrivilegedContainer (p. 147)

Note

在 Kubernetes 版本 1.14 之前，该`system:unauthenticated`组与默认关联且处于关联状态。`system:discovery` `system:basic-user` ClusterRoles此关联可能允许匿名用户进行意外访问。集群更新不会撤消这些权限。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`群组的关联。有关撤消这些权限的指导，请参阅 Amazon EKS 最佳实践指南中的查看和撤消不必要的匿名访问权限。

CredentialAccess:Kubernetes/MaliciousIPCaller

通常用于访问 Kubernetes 集群中的凭证或机密的 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与证书访问策略有关，在这种策略中，对手试图为你的 Kubernetes 集群收集密码、用户名和访问密钥。

补救建议：

如果该`KubernetesUserDetails`部分的调查结果中报告的用户是`system:anonymous`，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

通常用于访问 Kubernetes 集群中的证书或机密的 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的“其他信息”部分中。观察到的 API 通常与证书访问策略有关，在这种策略中，对手试图为你的 Kubernetes 集群收集密码、用户名和访问密钥。

补救建议：

如果该`KubernetesUserDetails`部分的调查结果中报告的用户是`system:anonymous`，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合

法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

一个常用于访问 Kubernetes 集群中的证书或机密的 API 是由未经身份验证的用户调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现告知您`system:anonymous`用户已成功调用 API 操作。发出的 API 调`system:anonymous`用未经身份验证。观察到的 API 通常与证书访问策略有关，在这种策略中，对手试图为你的 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。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您应检查在集群上向`system:anonymous`用户授予的权限，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，则应撤消该用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅查看和撤消不必要的匿名访问权限。

CredentialAccess:Kubernetes/TorIPCaller

通常用于访问 Kubernetes 集群中的凭证或机密的 API 是从 Tor 出口节点 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

这一发现告诉你，API 是从 Tor 出口节点 IP 地址调用的。观察到的 API 通常与证书访问策略有关，在这种策略中，对手试图为你的 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。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您的 Kubernetes 集群资源，意图隐藏攻击者的真实身份。

补救建议：

如果该`KubernetesUserDetails`部分的调查结果中报告的用户是`system:anonymous`，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

DefenseEvasion:Kubernetes/MaliciousIPCaller

通常用于逃避防御措施的 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与防御规避策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。

补救建议：

如果该`KubernetesUserDetails`部分的调查结果中报告的用户是`system:anonymous`，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

通常用于逃避防御措施的 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的 “其他信息” 部分中。观察到的 API 通常与防御规避策略有关，在这种策略中，对手试图隐瞒自己的行为以逃避侦查。

补救建议：

如果该`KubernetesUserDetails`部分的调查结果中报告的用户是`system:anonymous`，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

一个常用于逃避防御措施的 API 是由未经身份验证的用户调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现告知您`system:anonymous`用户已成功调用 API 操作。发出的 API 调`system:anonymous`用未经身份验证。观察到的 API 通常与防御规避策略有关，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。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您应检查在集群上向system:anonymous用户授予的权限，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，则应撤消该用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅查看和撤消不必要的匿名访问权限。

DefenseEvasion:Kubernetes/TorIPCaller

通常用于逃避防御措施的 API 是从 Tor 出口节点 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

这一发现告诉你，API 是从 Tor 出口节点 IP 地址调用的。观察到的 API 通常与防御规避策略有关，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。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您的 Kubernetes 集群，意图隐藏对手的真实身份。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Discovery:Kubernetes/MaliciousIPCaller

通常用于发现 Kubernetes 集群中资源的 API 是从 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常用于攻击的发现阶段，在此阶段，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。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Discovery:Kubernetes/MaliciousIPCaller.Custom

通常用于发现 Kubernetes 集群中资源的 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

此发现通知您，API 是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的 “其他信息” 部分中。观察到的 API 通常用于攻击的发现阶段，在此阶段，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。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Discovery:Kubernetes/SuccessfulAnonymousAccess

一个常用于发现 Kubernetes 集群中资源的 API 是由未经身份验证的用户调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

此发现告知您system:anonymous用户已成功调用 API 操作。发出的 API 调system:anonymous用未经身份验证。观察到的 API 通常与攻击的发现阶段相关，当时对手正在您的 Kubernetes 集群上收集信息。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。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您应检查在集群上向system:anonymous用户授予的权限，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，则应撤消该用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅查看和撤消不必要的匿名访问权限。

Discovery:Kubernetes/TorIPCaller

通常用于发现 Kubernetes 集群中资源的 API 是从 Tor 出口节点 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉你，API 是从 Tor 出口节点 IP 地址调用的。观察到的 API 通常用于攻击的发现阶段，在此阶段，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。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您的 Kubernetes 集群，意图隐藏对手的真实身份。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Execution:Kubernetes/ExecInKubeSystemPod

命令在kube-system命名空间内的 pod 中执行

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉你，命令是使用 Kubernetes e xec API 在kube-system命名空间内的容器中执行的。 kube-system命名空间是默认的命名空间，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 pod 或容器内执行命令的情况非常少见，并且可能表示可疑活动。

补救建议：

如果此命令的执行出乎意料，则用于执行该命令的用户身份的凭证可能会遭到破坏。撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Impact:Kubernetes/MaliciousIPCaller

通常用于篡改 Kubernetes 集群中资源的 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与冲击战术有关，在这种策略中，对手试图操纵、中断或破坏您的Amazon环境中的数据。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Impact:Kubernetes/MaliciousIPCaller.Custom

通常用于篡改 Kubernetes 集群中资源的 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的 “其他信息” 部分中。观察到的 API 通常与冲击战术有关，在这种策略中，对手试图操纵、中断或破坏您的Amazon环境中的数据。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Impact:Kubernetes/SuccessfulAnonymousAccess

一个常用于篡改 Kubernetes 集群中资源的 API 是由未经身份验证的用户调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现告知您system:anonymous用户已成功调用 API 操作。发出的 API 调system:anonymous用未经身份验证。当攻击者篡改集群中的资源时，观察到的 API 通常与攻击的影响阶段相关。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。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您应检查在集群上向system:anonymous用户授予的权限，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，则应撤消该用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅查看和撤消不必要的匿名访问权限。

Impact:Kubernetes/TorIPCaller

通常用于篡改 Kubernetes 集群中资源的 API 是从 Tor 出口节点 IP 地址调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

这一发现告诉你，API 是从 Tor 出口节点 IP 地址调用的。观察到的 API 通常与冲击战术有关，在这种策略中，对手试图操纵、中断或破坏您的Amazon环境中的数据。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您的 Kubernetes 集群，意图隐藏对手的真实身份。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Persistence:Kubernetes/ContainerWithSensitiveMount

启动了一个容器，其中安装了敏感的外部主机路径。

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉您，启动容器的配置在该volumeMounts部分中包含具有写入权限的敏感主机路径。这使得敏感的主机路径可以从容器内部访问和写入。这种技术通常被对手用来获取对主机文件系统的访问权限。

补救建议：

如果这次容器启动是意外的，则用于启动容器的用户身份凭证可能会遭到破坏。撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅修复 Kubernetes 的调查结果。如果预计会启动容器，则建议您使用包含基于该resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix字段的筛选条件的禁止规则。在筛选条件中，该imagePrefix字段应与调查结果中imagePrefix指定的字段相同。要了解有关创建禁止规则的更多信息，请参阅禁止规则。

Persistence:Kubernetes/MaliciousIPCaller

通常用于获取 Kubernetes 集群持续访问权限的 API 是从已知的恶意 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 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 Kubernetes 集群的访问权限并试图保持该访问权限。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Persistence:Kubernetes/MaliciousIPCaller.Custom

通常用于获取 Kubernetes 集群持续访问权限的 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

此发现通知您，API 操作是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的 “其他信息” 部分中。观察到的 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 Kubernetes 集群的访问权限并试图保持该访问权限。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Persistence:Kubernetes/SuccessfulAnonymousAccess

一个通常用于获取 Kubernetes 集群高级权限的 API 是由未经身份验证的用户调用的。

默认严重性：高

- 功能：Kubernetes 审核日志

此发现告知您system:anonymous用户已成功调用 API 操作。发出的 API 调system:anonymous用未经身份验证。观察到的 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。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您应检查在集群上向system:anonymous用户授予的权限，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，则应撤消该用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导，请参阅查看和撤消不必要的匿名访问权限。

Persistence:Kubernetes/TorIPCaller

通常用于获得 Kubernetes 集群永久访问权限的 API 是从 Tor 出口节点 IP 地址调用的。

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉你，API 是从 Tor 出口节点 IP 地址调用的。观察到的 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 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。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的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果该KubernetesUserDetails部分的调查结果中报告的用户是system:anonymous，请调查为什么允许匿名用户调用 API 并在需要时撤消权限。如果用户是经过身份验证的用户，请进行调查以确定该活动是合法的还是恶意的。如果活动是恶意的，则撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

默认服务账户被授予了 Kubernetes 集群的管理员权限。

默认严重性：高

- 功能：Kubernetes 审核日志

这一发现通知您，您的 Kubernetes 集群中命名空间的默认服务帐户已被授予管理员权限。Kubernetes 为集群中的所有命名空间创建一个默认服务帐户。它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 pod。如果默认服务帐户具有管理员权限，则可能会导致以管理员权限无意中启动 pod。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露。

补救建议：

您不应使用默认服务帐号向 pod 授予权限。相反，您应该为每个工作负载创建一个专用服务帐户，并根据需要向该帐户授予权限。要解决此问题，您应该为所有容器和工作负载创建专用服务帐户，并更新容器和工作负载以从默认服务帐户迁移到其专用帐户。然后，您应该从默认服务帐户中删除管理员权限。修复 EKS 审核日志监控结果 (p. 217)有关其他指导和资源，请参见。

Policy:Kubernetes/AnonymousAccessGranted

该system:anonymous用户获得了 Kubernetes 集群上的 API 权限。

默认严重性：高

- 功能：Kubernetes 审核日志

这一发现通知您，您的 Kubernetes 集群上的用户成功创建了ClusterRoleBinding或将该用户绑定RoleBindingsystem:anonymous到角色。这允许在未经身份验证的情况下访问角色允许的 API 操作。如果这种行为不是预料之中的，则可能表示配置错误或您的凭证已泄露

补救建议：

您应检查已向集群上的system:anonymous用户或群system:unauthenticated组授予的权限，并撤消不必要的匿名访问权限。有关指导，请参阅查看和撤消不必要的匿名访问权限。如果权限是恶意授予的，则应撤消授予权限的用户的访问权限，并撤消对手对您的集群所做的任何更改。有关指导，请参阅修复 Kubernetes 的调查结果。

Policy:Kubernetes/ExposedDashboard

Kubernetes 集群的仪表板已暴露在互联网上

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉你，你的集群的 Kubernetes 控制面板已被Load Balancer 服务暴露在互联网上。公开的仪表板使您可以从 Internet 访问集群的管理界面，并允许对手利用可能存在的任何身份验证和访问控制漏洞。

补救建议：

你应该确保在 Kubernetes 控制面板上强制执行强身份验证和授权。您还应实施网络访问控制，以限制特定 IP 地址对仪表板的访问。

Policy:Kubernetes/KubeflowDashboardExposed

Kubernetes 集群的 Kubeflow 仪表板已暴露在互联网上

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现通知您，您的集群的 Kubeflow 控制面板已被Load Balancer 服务暴露给互联网。公开的 Kubeflow 仪表板使您可以从互联网访问您的 Kubeflow 环境的管理界面，并允许对手利用可能存在的任何身份验证和访问控制漏洞。

补救建议：

你应该确保在 Kubeflow 控制面板上强制执行强身份验证和授权。您还应实施网络访问控制，以限制特定 IP 地址对仪表板的访问。

PrivilegeEscalation:Kubernetes/PrivilegedContainer

在您的 Kubernetes 集群上启动了具有根级访问权限的特权容器。

默认严重程度：中

- 功能：Kubernetes 审核日志

这一发现告诉您，在您的 Kubernetes 集群上使用映像启动特权容器以前从未用于在集群中启动特权容器。特权容器拥有主机的根级访问权限。对手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，然后入侵主机。

补救建议：

如果这次容器启动是意外的，则用于启动容器的用户身份凭证可能会遭到破坏。撤消用户的访问权限并撤消对手对您的集群所做的任何更改。有关指导修复 EKS 审核日志监控结果 (p. 216)，请参见。

Lambda 保护查找类型

本节介绍特定于您的Amazon Lambda资源的查找结果类型，其`resourceType`列为`Lambda`。对于所有 Lambda 调查结果，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 和威胁列表来防止该资源收到误报通知。

如果活动出乎意料，则安全最佳做法是假设 Lambda 可能遭到入侵，并遵循补救建议。

主题

- Backdoor:Lambda/C&CActivity.B (p. 147)
- CryptoCurrency:Lambda/BitcoinTool.B (p. 148)
- Trojan:Lambda/BlackholeTraffic (p. 148)
- Trojan:Lambda/DropPoint (p. 149)
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom (p. 149)
- UnauthorizedAccess:Lambda/TorClient (p. 149)
- UnauthorizedAccess:Lambda/TorRelay (p. 150)

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。

默认严重性：高

- 功能：Lambda 网络活动监控

此发现告诉您，您的Amazon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 函数可能遭到入侵。C&C 服务器是向僵尸网络的成员发布命令的计算机。

僵尸网络是连接互联网的设备的集合，可能包括个人电脑、服务器、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。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

CryptoCurrency:Lambda/BitcoinTool.B

Lambda 函数正在查询与加密货币相关活动关联的 IP 地址。

默认严重性：高

- 功能：Lambda 网络活动监控

此发现告诉您，您的Amazon环境中列出的 Lambda 函数正在查询与比特币或其他加密货币相关活动相关的 IP 地址。威胁行为者可能试图控制 Lambda 函数，以便恶意将其重新用于未经授权的加密货币挖矿。

补救建议：

如果您使用此 Lambda 函数来挖掘或管理加密货币，或者此函数以其他方式参与区块链活动，则这可能是您环境的预期活动。如果您的Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。禁止规则应由两个筛选条件组成。第一个标准应使用值为的查找类型属性CryptoCurrency:Lambda/BitcoinTool.B。第二个筛选标准应该是区块链活动中涉及的函数的 Lambda 函数名称。有关创建抑制规则的信息，请参阅抑制规则。

如果此活动出乎意料，则您的 Lambda 函数可能会遭到破坏。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

Trojan:Lambda/BlackholeTraffic

Lambda 函数正在尝试与已知黑洞的远程主机的 IP 地址通信。

默认严重性：中等

- 功能：Lambda 网络活动监控

此发现告诉您，您的Amazon环境中列出的 Lambda 函数正在尝试与黑洞（或漏洞）的 IP 地址通信。黑洞是网络中传入或传出的流量在不告知来源数据未到达预定接收方的情况下被默默丢弃的地方。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。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

Trojan:Lambda/DropPoint

Lambda 函数正在尝试与远程主机的 IP 地址通信，该主机已知该主机持有恶意软件捕获的证书和其他被盗数据。

默认严重性：中等

- 功能：Lambda 网络活动监控

此发现告知您，您的Amazon环境中列出的 Lambda 函数正在尝试与已知持有恶意软件捕获的证书和其他被盗数据的远程主机的 IP 地址进行通信。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

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。

默认严重性：中等

- 功能：Lambda 网络活动监控

此发现告知您，您Amazon环境中的 Lambda 函数正在与您上传的威胁列表中包含的 IP 地址通信。中 GuardDuty，威胁列表包含已知的恶意 IP 地址。 GuardDuty 根据上传的威胁列表生成调查结果。您可以在GuardDuty控制台的查找详细信息中查看威胁列表的详细信息。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

UnauthorizedAccess:Lambda/TorClient

Lambda 函数正在连接到 Tor Guard 或权威节点。

默认严重性：高

- 功能：Lambda 网络活动监控

这个发现告诉你，你Amazon环境中的 Lambda 函数正在连接到 Tor Guard 或权威节点。Tor 是用于实现匿名通信的软件。Tor Guards 和 Authority 节点充当 Tor 网络的初始网关。此流量可能表明此 Lambda 函数可能已被入侵。它现在充当 Tor 网络上的客户端。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅修复受损的 Lambda 函数 (p. 223)：

UnauthorizedAccess:Lambda/TorRelay

一个 Lambda 函数正在以 Tor 中继的形式连接到 Tor 网络。

默认严重性：高

- 功能：Lambda 网络活动监控

这一发现告诉你，你Amazon环境中的 Lambda 函数正在与 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 通过将客户端的潜在非法流量从一个 Tor 中继转发到另一个中继来实现匿名通信。

补救建议：

如果此活动出乎意料，则您的 Lambda 函数可能会受到攻击。有关更多信息，请参阅 修复受损的 Lambda 函数 (p. 223)。

恶意软件防护查找类型

GuardDuty 恶意软件保护为扫描 EC2 实例或容器工作负载期间检测到的所有威胁提供单一的恶意软件保护调查结果。该发现包括扫描期间检测到的总次数，并根据严重性提供其检测到的前 32 个威胁的详细信息。与其他 GuardDuty 发现不同，当再次扫描相同的 EC2 实例或容器工作负载时，恶意软件保护调查结果不会更新。

每次检测到恶意软件的扫描都会生成新的恶意软件防护结果。恶意软件保护发现包括有关产生该发现的相应扫描以及启动该扫描的 GuardDuty发现的信息。这样可以更轻松地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，恶意软件保护不会生成 EC2 级别的调查结果。

以下发现特定于 GuardDuty 恶意软件防护。

主题

- Execution:EC2/MaliciousFile (p. 150)
- Execution:ECS/MaliciousFile (p. 151)
- Execution:Kubernetes/MaliciousFile (p. 151)
- Execution:Container/MaliciousFile (p. 151)
- Execution:EC2/SuspiciousFile (p. 151)
- Execution:ECS/SuspiciousFile (p. 152)
- Execution:Kubernetes/SuspiciousFile (p. 152)
- Execution:Container/SuspiciousFile (p. 153)

Execution:EC2/MaliciousFile

已在 EC2 实例上检测到恶意文件。

默认严重程度：因检测到的威胁而异。

此发现表明，GuardDuty 恶意软件保护扫描已在您的Amazon环境中列出的 EC2 实例上检测到一个或多个恶意文件。此列出的实例可能已被入侵。有关更多信息，请参阅调查结果详细信息中的 “检测到的威胁” 部分。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅 修复受感染的 EC2 实例 (p. 213)。

Execution:ECS/MaliciousFile

已在 ECS 群集上检测到恶意文件。

默认严重程度：因检测到的威胁而异。

此发现表明，GuardDuty 恶意软件保护扫描在属于 ECS 群集的容器工作负载中检测到一个或多个恶意文件。有关更多信息，请参阅调查结果详细信息中的 “检测到的威胁” 部分。

补救建议：

如果此活动出乎意料，则您属于 ECS 集群的容器可能会遭到入侵。有关更多信息，请参阅 修复受感染的 ECS 集群 (p. 215)。

Execution:Kubernetes/MaliciousFile

已在 Kubernetes 集群上检测到恶意文件。

默认严重程度：因检测到的威胁而异。

此发现表明，GuardDuty 恶意软件保护扫描在属于 Kubernetes 集群的容器工作负载中检测到一个或多个恶意文件。如果这是 EKS 管理的集群，则调查结果详细信息将提供有关受影响的 EKS 资源的更多信息。有关更多信息，请参阅调查结果详细信息中的 “检测到的威胁” 部分。

补救建议：

如果此活动出乎意料，则您的容器工作负载可能会受到影响。有关更多信息，请参阅 修复由发现的 EKS 审核日志监控结果 GuardDuty (p. 216)。

Execution:Container/MaliciousFile

已在独立容器上检测到恶意文件。

默认严重程度：因检测到的威胁而异。

此发现表明，GuardDuty 恶意软件保护扫描已在容器工作负载中检测到一个或多个恶意文件，并且未发现任何群集信息。有关更多信息，请参阅调查结果详细信息中的 “检测到的威胁” 部分。

补救建议：

如果此活动出乎意料，则您的容器工作负载可能会受到影响。有关更多信息，请参阅 修复受感染的独立容器 (p. 216)。

Execution:EC2/SuspiciousFile

已在 EC2 实例上检测到可疑文件。

默认严重程度：因检测到的威胁而异。

此发现表明， GuardDuty 恶意软件保护扫描已在 EC2 实例上检测到一个或多个可疑文件。有关更多信息，请参阅调查结果详细信息中的 “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有害的程序，例如广告软件、间谍软件或双重用途工具。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，网络工具可以被对手合法或恶意地用作黑客工具，试图破坏资源。

检测到可疑文件后，评估您是否希望在Amazon环境中看到检测到的文件。如果文件出乎意料，请执行下一节中提供的补救建议。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅 修复受感染的 EC2 实例 (p. 213)。

Execution:ECS/SuspiciousFile

已在 ECS 群集上检测到可疑文件。

默认严重程度：因检测到的威胁而异。

此发现表明， GuardDuty 恶意软件保护扫描已在属于 ECS 群集的容器上检测到一个或多个可疑文件。有关更多信息，请参阅调查结果详细信息中的 “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有害的程序，例如广告软件、间谍软件或双重用途工具。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，网络工具可以被对手合法或恶意地用作黑客工具，试图破坏资源。

检测到可疑文件后，评估您是否希望在Amazon环境中看到检测到的文件。如果文件出乎意料，请执行下一节中提供的补救建议。

补救建议：

如果此活动出乎意料，则您属于 ECS 集群的容器可能会遭到入侵。有关更多信息，请参阅 修复受感染的 ECS 集群 (p. 215)。

Execution:Kubernetes/SuspiciousFile

已在 Kubernetes 集群上检测到可疑文件。

默认严重程度：因检测到的威胁而异。

此发现表明， GuardDuty 恶意软件保护扫描已在属于 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，则调查结果的详细信息将提供有关受影响的 EKS 的更多信息。有关更多信息，请参阅调查结果详细信息中的 “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有害的程序，例如广告软件、间谍软件或双重用途工具。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，网络工具可以被对手合法或恶意地用作黑客工具，试图破坏资源。

检测到可疑文件后，评估您是否希望在Amazon环境中看到检测到的文件。如果文件出乎意料，请执行下一节中提供的补救建议。

补救建议：

如果此活动出乎意料，则您的容器工作负载可能会受到影响。有关更多信息，请参阅 修复由发现的 EKS 审核日志监控结果 GuardDuty (p. 216)。

Execution:Container/SuspiciousFile

已在独立容器上检测到可疑文件。

默认严重程度：因检测到的威胁而异。

此发现表明，GuardDuty 恶意软件保护扫描在没有群集信息的容器上检测到一个或多个可疑文件。有关更多信息，请参阅调查结果详细信息中的“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有害的程序，例如广告软件、间谍软件或双重用途工具。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，网络工具可以被对手合法或恶意地用作黑客工具，试图破坏资源。

检测到可疑文件后，评估您是否希望在Amazon环境中看到检测到的文件。如果文件出乎意料，请执行下一节中提供的补救建议。

补救建议：

如果此活动出乎意料，则您的容器工作负载可能会受到影响。有关更多信息，请参阅修复受感染的独立容器 (p. 216)。

GuardDuty RDS 保护查找类型

GuardDuty RDS 保护可检测您的数据库实例上的异常登录行为。以下发现是特定于的支持的亚马逊 Aurora 数据库 (p. 68)，其资源类型将为RDSDBInstance。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 (p. 153)
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin (p. 154)
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce (p. 154)
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin (p. 155)
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin (p. 155)
- Discovery:RDS/MaliciousIPCaller (p. 156)
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin (p. 156)
- CredentialAccess:RDS/TorIPCaller.FailedLogin (p. 156)
- Discovery:RDS/TorIPCaller (p. 157)

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**
>
> 根据与该发现相关的异常行为，默认严重性为“低”、“中”和“高”。
>
> - 低 — 如果与此发现相关的用户名是从与专用网络关联的 IP 地址登录的。
> - 中等 — 如果与此发现相关的用户名是从公共 IP 地址登录的。

- 高 — 如果存在从公有 IP 地址尝试登录失败的持续模式，则表明访问策略过于宽松。

- 功能：RDS 登录活动监控

此发现告诉您，在您的Amazon环境中的 RDS 数据库上观察到异常成功登录。这可能表明以前的隐身用户是第一次登录到 RDS 数据库。常见的情况是内部用户登录到数据库，该数据库由应用程序而不是单个用户以编程方式访问。

异常检测机器学习（ML）模型将这次成功的登录确定为 GuardDuty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 数据库 (p. 68)并识别与对手使用的技术相关的异常事件。ML 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，请参阅基于 RDS 登录活动的异常 (p. 88)。

补救建议：

如果关联数据库的此活动出乎意料，建议更改关联数据库用户的密码，并查看可用的审计日志以了解异常用户执行的活动。中等和高严重性调查结果可能表明数据库访问策略过于宽松，用户凭证可能已被泄露或泄露。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，请参阅使用成功的登录事件修复可能受损的数据库 (p. 221)：

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

在您账户的 RDS 数据库上观察到一次或多次异常失败的登录尝试。

默认严重性：低

- 功能：RDS 登录活动监控

此发现告诉您，在您的Amazon环境中的 RDS 数据库上观察到一次或多次异常登录失败。尝试从公有 IP 地址登录失败可能表明您账户中的 RDS 数据库遭到了潜在恶意行为者的暴力攻击。

这些失败的登录被异常检测机器学习（ML）模型确定为 GuardDuty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 数据库 (p. 68)并识别与对手使用的技术相关的异常事件。ML 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。有关可能不寻常的 RDS 登录活动的信息，请参阅基于 RDS 登录活动的异常 (p. 88)。

补救建议：

如果此活动对关联数据库来说出乎意料，则可能表明该数据库已公开或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，请参阅修复带有失败登录事件的潜在受损数据库 (p. 222)：

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

在连续出现异常的登录尝试失败后，用户以异常方式成功从公有 IP 地址登录到您账户中的 RDS 数据库。

默认严重性：高

- 功能：RDS 登录活动监控

此发现告知您，在您的Amazon环境中的 RDS 数据库上观察到异常登录，表明暴力破解成功。在异常成功登录之前，观察到一贯的异常登录尝试失败模式。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。

这种成功的暴力登录被异常检测机器学习 (ML) 模型确定为 GuardDuty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 数据库 (p. 68)并识别与对手使用的技术相关的异常事件。ML 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。有关可能不寻常的 RDS 登录活动的信息，请参阅基于 RDS 登录活动的异常 (p. 88)。

补救建议：

此活动表明数据库凭证可能已被泄露或泄露。建议更改关联数据库用户的密码，并查看可用的审核日志，了解可能被入侵的用户执行的活动。一贯的异常登录尝试失败模式表明，对数据库的访问政策过于宽松，或者数据库也可能已公之于众。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，请参阅使用成功的登录事件修复可能受损的数据库 (p. 221)：

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

用户从已知的恶意 IP 地址成功登录到您账户中的 RDS 数据库。

默认严重性：高

- 功能：RDS 登录活动监控

此发现告知您，成功的 RDS 登录活动是从与您的Amazon环境中已知恶意活动相关的 IP 地址发生的。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。

补救建议：

如果此活动对关联数据库来说是意外的，则可能表明用户凭证可能已泄露或泄露。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。此活动还可能表明数据库访问政策过于宽松，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，请参阅使用成功的登录事件修复可能受损的数据库 (p. 221)：

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

与已知恶意活动相关的 IP 地址尝试登录您账户中的 RDS 数据库，但未成功。

默认严重性：中等

- 功能：RDS 登录活动监控

此发现通知您，与已知恶意活动相关的 IP 地址试图登录您Amazon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。

补救建议：

如果此活动对关联数据库来说出乎意料，则可能表明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，请参阅修复带有失败登录事件的潜在受损数据库 (p. 222)：

Discovery:RDS/MaliciousIPCaller

与已知恶意活动相关的 IP 地址探测了您账户中的 RDS 数据库；未尝试进行身份验证。

默认严重性：中等

- 功能：RDS 登录活动监控

此发现告知您，与已知恶意活动相关的 IP 地址探测了您Amazon环境中的 RDS 数据库，但未尝试登录。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。

补救建议：

如果此活动对关联数据库来说出乎意料，则可能表明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，请参阅修复带有失败登录事件的潜在受损数据库 (p. 222)：

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。

默认严重性：高

- 功能：RDS 登录活动监控

此发现告诉您，用户从 Tor 出口节点 IP 地址成功登录到您Amazon环境中的 RDS 数据库。Tor 是一款用于启用匿名通信的软件。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，目的是隐藏匿名用户的真实身份。

补救建议：

如果此活动对关联数据库来说是意外的，则可能表明用户凭证可能已泄露或泄露。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。此活动还可能表明数据库访问政策过于宽松，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，请参阅使用成功的登录事件修复可能受损的数据库 (p. 221)：

CredentialAccess:RDS/TorIPCaller.FailedLogin

Tor IP 地址尝试登录您账户中的 RDS 数据库，但未成功。

默认严重性：中等

- 功能：RDS 登录活动监控

此发现告知您 Tor 出口节点 IP 地址试图登录您Amazon环境中的 RDS 数据库，但未能提供正确的用户名或密码。Tor 是一款用于启用匿名通信的软件。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，目的是隐藏匿名用户的真实身份。

补救建议：

如果此活动对关联数据库来说出乎意料，则可能表明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，请参阅修复带有失败登录事件的潜在受损数据库 (p. 222)：

Discovery:RDS/TorIPCaller

Tor 出口节点 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。

默认严重性：中等

- 功能：RDS 登录活动监控

这个发现告诉你，Tor 出口节点 IP 地址探测了你Amazon环境中的 RDS 数据库，尽管没有尝试登录。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 是一款用于启用匿名通信的软件。它通过一系列网络节点之间的中继对通信进行加密和随机反弹。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行为者的真实身份。

补救建议：

如果此活动对关联数据库来说出乎意料，则可能表明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 修复带有失败登录事件的潜在受损数据库 (p. 222)。

GuardDuty S3 查找类型

以下发现是特定于 Amazon S3 资源的，**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。调查结果的严重性和详细信息将因调查结果类型和与存储桶关联的权限而异。

此处列出的发现包括用于生成该发现类型的数据源和模型。有关数据源和模型的更多信息，请参阅基础数据来源 (p. 14)。

> **Important**
>
> 只有在启用了 S3 保护时，才会生成具有 S3CloudTrail 数据源事件的调查结果 GuardDuty。默认情况下，在 2020 年 7 月 31 日之后创建的所有账户中启用 S3 保护。有关如何启用或禁用 S3 保护的信息，请参阅亚马逊的Amazon S3 保护 GuardDuty (p. 74)

对于所有S3Bucket类型的调查结果，建议您检查相关存储段的权限以及调查结果中涉及的任何用户的权限，如果活动出乎意料，请参阅中详细的补救建议修复受感染的 S3 存储桶 (p. 213)。

主题

- Discovery:S3/AnomalousBehavior (p. 158)
- Discovery:S3/MaliciousIPCaller (p. 158)

- Discovery:S3/MaliciousIPCaller.Custom (p. 159)
- Discovery:S3/TorIPCaller (p. 159)
- Exfiltration:S3/AnomalousBehavior (p. 159)
- Exfiltration:S3/MaliciousIPCaller (p. 160)
- Impact:S3/AnomalousBehavior.Delete (p. 160)
- Impact:S3/AnomalousBehavior.Permission (p. 161)
- Impact:S3/AnomalousBehavior.Write (p. 161)
- Impact:S3/MaliciousIPCaller (p. 162)
- PenTest:S3/KaliLinux (p. 162)
- PenTest:S3/ParrotLinux (p. 162)
- PenTest:S3/PentooLinux (p. 163)
- Policy:S3/AccountBlockPublicAccessDisabled (p. 163)
- Policy:S3/BucketAnonymousAccessGranted (p. 163)
- Policy:S3/BucketBlockPublicAccessDisabled (p. 164)
- Policy:S3/BucketPublicAccessGranted (p. 164)
- Stealth:S3/ServerAccessLoggingDisabled (p. 165)
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom (p. 165)
- UnauthorizedAccess:S3/TorIPCaller (p. 165)

Discovery:S3/AnomalousBehavior

通常用于发现 S3 对象的 API 是以异常方式调用的。

默认严重性：低

- 数据源：3CloudTrail 的数据事件

此发现告知您 IAM 实体已调用 S3 API 来发现您的环境中的 S3 存储桶，例如`ListObjects`。此类活动与攻击的发现阶段有关，在该阶段攻击者收集信息以确定您的Amazon环境是否容易受到更广泛的攻击。此活动是可疑的，因为 IAM 实体以不寻常的方式调用了 API。例如，没有先前历史记录的 IAM 实体调用 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。它跟踪 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。有关 API 请求的哪些因素对于调用请求的用户身份而言异常的更多信息，请参阅查找详细信息。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Discovery:S3/MaliciousIPCaller

通常用于发现Amazon环境中资源的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您 S3 API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与攻击的发现阶段相关，此时对手正在收集有关您的Amazon环境的信息。示例包括 `GetObjectAcl` 和 `ListObjects`。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Discovery:S3/MaliciousIPCaller.Custom

S3 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现通知您，S3 API（例如`GetObjectAcl`或`ListObjects`）是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的“附加信息”部分中。此类活动与攻击的发现阶段有关，在该阶段攻击者正在收集信息，以确定您的Amazon环境是否容易受到更广泛的攻击。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Discovery:S3/TorIPCaller

S3 API 是从 Tor 出口节点 IP 地址调用的。

默认严重性：中等

- 数据源：3CloudTrail 的数据事件

此发现告知您 S3 API（例如`GetObjectAcl`或`ListObjects`）是从 Tor 出口节点 IP 地址调用的。此类活动与攻击的发现阶段有关，在该阶段攻击者正在收集信息，以确定您的Amazon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。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您的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Exfiltration:S3/AnomalousBehavior

一个 IAM 实体以可疑的方式调用了 S3 API。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您 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已建立的基准不同。此活动中使用的 API 调用与攻击的渗透阶段相关，在该阶段攻击者试图收集数据。此活动是可疑的，因为 IAM 实体以不寻常的方式调用了 API。例如，没有先前历史记录的 IAM 实体调用 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。它跟踪 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。有关 API 请求的哪些因素对于调用请求的用户身份而言异常的更多信息，请参阅查找详细信息。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Exfiltration:S3/MaliciousIPCaller

通常用于从Amazon环境收集数据的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您 S3 API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与渗透策略有关，在这种策略中，对手正试图从你的网络收集数据。示例包括 `GetObject` 和 `CopyObject`。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Impact:S3/AnomalousBehavior.Delete

一个 IAM 实体调用了 S3 API，试图以可疑的方式删除数据。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您，您的Amazon环境中的 IAM 实体正在进行涉及 S3 存储桶的 API 调用，并且此行为与该实体既定的基准不同。此活动中使用的 API 调用与试图删除数据的攻击相关。此活动是可疑的，因为 IAM 实体以不寻常的方式调用了 API。例如，没有先前历史记录的 IAM 实体调用 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。它跟踪 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。有关 API 请求的哪些因素对于调用请求的用户身份而言异常的更多信息，请参阅查找详细信息。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

我们建议对您的 S3 存储桶的内容进行审计，以确定您是否可以或应该恢复以前的对象版本。

Impact:S3/AnomalousBehavior.Permission

通常用于设置访问控制列表 (ACL) 权限。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您，您Amazon环境中的 IAM 实体已更改了列出的 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Amazon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。它跟踪 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。有关 API 请求的哪些因素对于调用请求的用户身份而言异常的更多信息，请参阅查找详细信息。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

我们建议对您的 S3 存储桶的内容进行审计，以确保不允许意外公开访问任何对象。

Impact:S3/AnomalousBehavior.Write

一个 IAM 实体调用了 S3 API，试图以可疑的方式写入数据。

默认严重性：中等

- 数据源：3CloudTrail 的数据事件

此发现告知您，您的Amazon环境中的 IAM 实体正在进行涉及 S3 存储桶的 API 调用，并且此行为与该实体既定的基准不同。此活动中使用的 API 调用与尝试写入数据的攻击相关。此活动是可疑的，因为 IAM 实体以不寻常的方式调用了 API。例如，没有先前历史记录的 IAM 实体调用 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。它跟踪 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。有关 API 请求的哪些因素对于调用请求的用户身份而言异常的更多信息，请参阅查找详细信息。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

我们建议对您的 S3 存储桶的内容进行审计，以确保此 API 调用没有写入恶意或未经授权的数据。

Impact:S3/MaliciousIPCaller

通常用于篡改Amazon环境中数据或进程的 S3 API 是从已知的恶意 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您 S3 API 操作是从与已知恶意活动相关的 IP 地址调用的。观察到的 API 通常与影响策略有关，在这种策略中，对手试图操纵、中断或破坏Amazon环境中的数据。示例包括 `PutObject` 和 `PutObjectAcl`。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

PenTest:S3/KaliLinux

S3 API 是从 Kali Linux 计算机上调用的。

默认严重性：中等

- 数据源：3CloudTrail 的数据事件

此发现告诉您，运行 Kali Linux 的计算机正在使用属于您Amazon账户的证书进行 S3 API 调用。您的凭证可能遭盗用。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。攻击者也会使用此工具来寻找 EC2 配置漏洞和获取对您 Amazon 环境未经授权的访问。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

PenTest:S3/ParrotLinux

S3 API 是从 Parrot Security Linux 计算机上调用的。

默认严重性：中等

- 数据源：3CloudTrail 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Amazon账户的证书进行 S3 API 调用。您的凭证可能遭盗用。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 Amazon 环境未经授权的访问。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

PenTest:S3/PentooLinux

S3 API 是从 Pentoo Linux 机器上调用的。

默认严重性：中等

- 数据源：3CloudTrail 的数据事件

此发现告诉你，运行 Pentoo Linux 的计算机正在使用属于你Amazon账户的证书进行 S3 API 调用。您的凭证可能遭盗用。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。攻击者也会使用此工具来寻找 EC2 配置漏洞和获取对您 Amazon 环境未经授权的访问。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Policy:S3/AccountBlockPublicAccessDisabled

一个 IAM 实体调用了用于禁用账户上的 S3 Block 公共访问的 API。

默认严重性：低

- 数据源：CloudTrail 管理事件

此发现告知您 Amazon S3 Block 公共访问已在账户级别禁用。启用 S3 Block Public Access 设置后，它们用于筛选存储段上的策略或访问控制列表 (ACL)，以此作为一项安全措施，以防止无意中向公众泄露数据。

通常，在账户中关闭 S3 Block Public Access，以允许公众访问存储段或存储段中的对象。当某个账户禁用 S3 Block Public Access 时，对您的存储段的访问权限将由应用于您的各个存储段的策略、ACL 或存储段级封锁公共访问设置控制。这并不一定意味着存储分区是公开共享的，但您应该审核应用于存储段的权限，以确认它们提供了适当的访问级别。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Policy:S3/BucketAnonymousAccessGranted

IAM 委托人已通过更改存储桶策略或 ACL 授予对 S3 存储段的互联网访问权限。

默认严重性：高

- 数据源：CloudTrail 管理事件

此发现告知您，列出的 S3 存储桶已在互联网上公开访问，因为 IAM 实体更改了该存储桶的存储桶策略或 ACL。检测到策略或 ACL 更改后，使用由 Zelkova 支持的自动推理来确定存储段是否可公开访问。

Note

如果存储段的 ACL 或存储段策略配置为显式拒绝或全部拒绝，则此发现可能无法反映存储段的当前状态。此发现不会反映可能已为您的 S3 存储桶启用的任何 S3 Block 公共访问设置。在这种情况下，发现结果中的`effectivePermission`值将标记为`UNKNOWN`。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Policy:S3/BucketBlockPublicAccessDisabled

一个 IAM 实体调用了用于禁用存储段上的 S3 Block 公共访问的 API。

默认严重性：低

- 数据源：CloudTrail 管理事件

此发现通知您，列出的 S3 存储桶的阻止公共访问已被禁用。启用后，S3 Block Public Access 设置用于筛选应用于存储段的策略或访问控制列表 (ACL)，以此作为一项安全措施，以防止无意中向公众泄露数据。

通常，在存储段上关闭 S3 Block Public Access，以允许公众访问该存储段或其中的对象。禁用存储分区的 S3 Block 公共访问时，对该存储桶的访问由应用于该存储段的策略或 ACL 控制。这并不意味着将公开共享存储桶，但您应该审核应用于该存储桶的策略和 ACL，以确认应用适当的权限。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Policy:S3/BucketPublicAccessGranted

IAM 委托人已通过更改存储桶策略或 ACL 向所有Amazon用户授予对 S3 存储桶的公共访问权限。

默认严重性：高

- 数据源：CloudTrail 管理事件

此发现告知您，列出的 S3 存储桶已向所有经过身份验证的Amazon用户公开，因为 IAM 实体更改了该 S3 存储桶的存储段策略或 ACL。检测到策略或 ACL 更改后，使用由 Zelkova 支持的自动推理来确定存储段是否可公开访问。

Note

如果存储段的 ACL 或存储段策略配置为显式拒绝或全部拒绝，则此发现可能无法反映存储段的当前状态。此发现不会反映可能已为您的 S3 存储桶启用的任何 S3 Block 公共访问设置。在这种情况下，发现结果中的`effectivePermission`值将标记为`UNKNOWN`。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Stealth:S3/ServerAccessLoggingDisabled

对存储桶的 3 服务器3 服务器3 服务器访问日志记录。

默认严重性：低

- 数据源：CloudTrail 管理事件

此发现告知您，您的Amazon环境中的存储段已禁用 S3 服务器访问日志记录。如果禁用，则不会为任何访问已识别的 S3 存储桶的尝试创建 Web 请求日志，但是，仍会跟踪对该存储桶的 S3 管理 API 调用 DeleteBucket，例如。如果 CloudTrail 为此存储段启用了 S3 数据事件日志记录，则仍将跟踪对该存储段内对象的 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 服务器访问日志和 S3 日志记录选项。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

S3 API 是从自定义威胁列表上的 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您，S3 API 操作（例如`PutObject`或`PutObjectAcl`）是从您上传的威胁列表中包含的 IP 地址调用的。与该发现相关的威胁列表列在调查结果详细信息的“附加信息”部分中。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

UnauthorizedAccess:S3/TorIPCaller

S3 API 是从 Tor 出口节点 IP 地址调用的。

默认严重性：高

- 数据源：3CloudTrail 的数据事件

此发现告知您 S3 API 操作（例如`PutObject`或`PutObjectAcl`）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。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。此发现可能表明未经授权访问了您的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅 修复受感染的 S3 存储桶 (p. 213)。

停用的S3

调查结果是一个通知，包含有关 GuardDuty 发现的潜在安全问题的详细信息。有关对 GuardDuty 查找结果类型进行重要更改（包括新添加或停用的查找结果类型）的信息，请参阅亚马逊的文档历史记录 GuardDuty (p. 294)。

以下查找结果类型已停用，不再由生成 GuardDuty。

> **Important**
>
> 您无法重新激活已停用的 GuardDuty 查找结果类型。

主题

- Exfiltration:S3/ObjectRead.Unusual (p. 166)
- Impact:S3/PermissionsModification.Unusual (p. 167)
- Impact:S3/ObjectDelete.Unusual (p. 167)
- Discovery:S3/BucketEnumeration.Unusual (p. 167)
- Persistence:IAMUser/NetworkPermissions (p. 168)
- Persistence:IAMUser/ResourcePermissions (p. 168)
- Persistence:IAMUser/UserPermissions (p. 169)
- PrivilegeEscalation:IAMUser/AdministrativePermissions (p. 169)
- Recon:IAMUser/NetworkPermissions (p. 170)
- Recon:IAMUser/ResourcePermissions (p. 170)
- Recon:IAMUser/UserPermissions (p. 170)
- ResourceConsumption:IAMUser/ComputeResources (p. 171)
- Stealth:IAMUser/LoggingConfigurationModified (p. 171)
- UnauthorizedAccess:IAMUser/ConsoleLogin (p. 172)
- UnauthorizedAccess:EC2/TorIPCaller (p. 172)
- Backdoor:EC2/XORDDOS (p. 172)
- Behavior:IAMUser/InstanceLaunchUnusual (p. 173)
- CryptoCurrency:EC2/BitcoinTool.A (p. 173)
- UnauthorizedAccess:IAMUser/UnusualASNCaller (p. 173)

Exfiltration:S3/ObjectRead.Unusual

一个 IAM 实体以可疑的方式调用了 S3 API。

默认严重性：中等*

> **Note**
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

- SCloudTrail 3 事件

此发现告知您，您Amazon环境中的 IAM 实体正在进行 API 调用，这些调用涉及 S3 存储桶，并且与该实体已建立的基准不同。此活动中使用的 API 调用与攻击的渗透阶段相关，在该阶段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的 API 的历史，或者该 API 是从一个不寻常的位置调用的。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Impact:S3/PermissionsModification.Unusual

一个 IAM 实体调用 API 来修改一个或多个 S3 资源的权限。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现告诉您，一个 IAM 实体正在进行 API 调用，旨在修改您Amazon环境中一个或多个存储段或对象的权限。攻击者可能会执行此操作，以允许在帐户之外共享信息。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的 API 的历史，或者该 API 是从一个不寻常的位置调用的。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Impact:S3/ObjectDelete.Unusual

Aimple Storage S3 ）。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现告知您，您Amazon环境中的特定 IAM 实体正在进行 API 调用，旨在通过删除存储段本身来删除列出的 S3 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的 API 的历史，或者该 API 是从一个不寻常的位置调用的。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Discovery:S3/BucketEnumeration.Unusual

一个 IAM 实体调用了一个 S3 API，用于发现您的网络中的 S3 存储桶。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现告知您 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，在该阶段攻击者正在收集信息，以确定您的Amazon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的 API 的历史，或者该 API 是从一个不寻常的位置调用的。

补救建议：

如果此活动对关联委托人来说出乎意料，则可能表明证书已泄露或您的 S3 权限不够严格。有关更多信息，请参阅修复受感染的 S3 存储桶 (p. 213)：

Persistence:IAMUser/NetworkPermissions

一个 IAM 实体调用了一个 API，通常用于更改您Amazon账户中安全组、路由和 ACL 的网络访问权限。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现表明，您的Amazon环境中的特定委托人（Amazon Web Services 账户根用户IAM 角色或用户）的行为与既定基准不同。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，例如当委托人调用`CreateSecurityGroup` API 时没有这样做的历史记录。攻击者经常尝试更改安全组，允许不同端口上的某些入站流量，以提高他们访问 EC2 实例的能力。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Persistence:IAMUser/ResourcePermissions

委托人调用了通常用于更改您中各种资源的安全访问策略的APIAmazon Web Services 账户。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果调用 API 使用在实例上创建的临时Amazon证书，则该发现的严重性为 “高”。

此发现表明，您的Amazon环境中的特定委托人（Amazon Web Services 账户根用户IAM 角色或用户）的行为与既定基准不同。此委托人以前没有调用此 API 的历史记录。

当检测到与Amazon资源相关的策略或权限发生更改时，例如当您Amazon环境中的委托人调用`PutBucketPolicy` API 时，此发现即触发。一些服务（如 Amazon S3 imple Storage Simple Storage

Simple Storage Simple Storage Sime ） 利用被盗的凭证，攻击者可以更改附加到资源的策略以获得对该资源的访问权限。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Persistence:IAMUser/UserPermissions

委托人调用了一个 API，通常用于在您的Amazon账户中添加、修改或删除 IAM 用户、群组或策略。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现表明，您的Amazon环境中的特定委托人（Amazon Web Services 账户根用户IAM 角色或用户）的行为与既定基准不同。此委托人以前没有调用此 API 的历史记录。

此发现是由您的Amazon环境中与用户相关的权限的可疑更改触发的，例如，当您Amazon环境中的委托人调用`AttachUserPolicy` API 时没有调用历史记录。即使原始访问点已关闭，攻击者也可以使用被盗的凭据来创建新用户、为现有用户添加访问策略或创建访问密钥以最大限度地提高他们对账户的访问权限。例如，账户的所有者可能会注意到特定 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以欺诈手段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Amazon帐户。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

PrivilegeEscalation:IAMUser/AdministrativePermissions

委托人尝试给自己分配高度宽松的策略。

默认严重性：低*

> Note
>
> 如果尝试权限升级不成功，则此发现的严重性为 “低”；如果尝试权限升级成功，则此发现的严重性为 “中”。

此发现表明您Amazon环境中的特定 IAM 实体表现出可能表明存在权限升级攻击的行为。当 IAM 用户或角色尝试为自己分配高度宽松的策略时，就会触发此发现。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。

即使原始访问点已关闭，攻击者也会使用被盗的凭据来创建新用户、为现有用户添加访问策略或创建访问密钥以最大限度地提高他们对账户的访问权限。例如，账户所有者可能会注意到特定 IAM 用户的登录凭证被盗并将其从账户中删除，但可能无法删除由以欺诈手段创建的管理员委托人创建的其他用户，从而使攻击者仍然可以访问他们的Amazon账户。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/NetworkPermissions

委托人调用了一个 API，通常用于更改您Amazon账户中安全组、路由和 ACL 的网络访问权限。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现表明，您的Amazon环境中的特定委托人（Amazon Web Services 账户根用户IAM 角色或用户）的行为与既定基准不同。此委托人以前没有调用此 API 的历史记录。

当在可疑情况下探测到您Amazon账户中的资源访问权限时，就会触发此发现。例如，如果委托人调用了`DescribeInstances` API，而之前没有这样做的历史。攻击者可能会使用被盗的凭据对您的Amazon资源进行此类侦察，以找到更有价值的凭证或确定他们已经拥有的凭据的能力。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/ResourcePermissions

委托人调用了一个 API，通常用于更改您Amazon账户中各种资源的安全访问策略。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现表明，您的Amazon环境中的特定委托人（Amazon Web Services 账户根用户IAM 角色或用户）的行为与既定基准不同。此委托人以前没有调用此 API 的历史记录。

当在可疑情况下探测到您Amazon账户中的资源访问权限时，就会触发此发现。例如，如果委托人调用了`DescribeInstances` API，而之前没有这样做的历史。攻击者可能会使用被盗的凭据对您的Amazon资源进行此类侦察，以找到更有价值的凭证或确定他们已经拥有的凭据的能力。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Recon:IAMUser/UserPermissions

委托人调用了一个 API，通常用于在您的Amazon账户中添加、修改或删除 IAM 用户、群组或策略。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

此发现是在可疑情况下探测Amazon环境中的用户权限时触发的。例如，如果委托人（Amazon Web Services 账户根用户IAM 角色或 IAM 用户）在没有调用过`ListInstanceProfilesForRole` API 的历史记录的情况下调用了 API。攻击者可能会使用被盗的凭据对您的Amazon资源进行此类侦察，以找到更有价值的凭证或确定他们已经拥有的凭据的能力。

此发现表明，您Amazon环境中的特定主体的行为与既定基准不同。此委托人以前没有通过此方法调用该 API 的历史记录。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

ResourceConsumption:IAMUser/ComputeResources

委托人调用了一个 API，该 API 通常用于启动计算资源，如 EC2 实例。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

当您的Amazon环境中列出的账户中的 EC2 实例在可疑情况下启动时，就会触发此发现。此发现表明您Amazon环境中的特定委托人的行为与既定基准不同；例如，如果委托人（Amazon Web Services 账户根用户IAM 角色或 IAM 用户）在没有调用过`RunInstances` API 的历史记录的情况下调用了 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)。这也可能表明攻击者使用您Amazon环境中的 EC2 实例及其证书来维护对您账户的访问权限。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

Stealth:IAMUser/LoggingConfigurationModified

委托人调用了一个 API，通常用于停止 CloudTrail 记录、删除现有日志以及以其他方式消除Amazon账户中的活动痕迹。

默认严重性：中等*

Note

此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “高”。

当在可疑情况下修改环境中列出的Amazon账户中的日志配置时，就会触发此发现。此发现告诉您，您Amazon环境中的特定委托人的行为与既定基准不同；例如，如果委托人（Amazon Web Services 账户根用户IAM 角色或 IAM 用户）在没有调用过`StopLogging` API 的历史记录的情况下调用了 API。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。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:IAMUser/ConsoleLogin

在您的Amazon账户中观察到委托人不寻常地登录控制台。

默认严重性：中等*

> Note
>
> 此发现的默认严重性为 “中”。但是，如果使用在实例上创建的临时Amazon证书调用 API，则发现的严重性为 “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，如果校长之前没有这样做的历史，则从 never-before-used 客户端或异常地点调用了 ConsoleLogin API。这可能表明被盗的凭证被用来访问您的Amazon帐户，或者有效用户以无效或不太安全的方式（例如，不是通过经批准的 VPN）访问该帐户。

这一发现告诉你，你的Amazon环境中的特定主体的行为与既定基准不同。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。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

UnauthorizedAccess:EC2/TorIPCaller

EC2 实例正在接收来自 Tor 退出节点的入站连接。

默认严重性：中等

此发现告诉您，您Amazon环境中的 EC2 实例正在接收来自 Tor 出口节点的入站连接。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。此发现可能表明未经授权访问了您的Amazon资源，目的是隐藏攻击者的真实身份。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Backdoor:EC2/XORDDOS

EC2 实例正在尝试与与 XOR DDoS 恶意软件关联的 IP 地址进行通信。

默认严重性：高

此发现告知您，您Amazon环境中的 EC2 实例正试图与与 XOR DDoS 恶意软件关联的 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 凭证并成功登录后，它会使用 root 用户权限运行下载和安装 XOR DDoS 的脚本。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。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

Behavior:IAMUser/InstanceLaunchUnusual

用户启动了一个异常类型的 EC2 实例。

默认严重性：高

此发现告诉您，您Amazon环境中的特定用户的行为与既定基准不同。此用户之前没有启动此类的 EC2 实例的历史。您的登录凭证可能会被泄露。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：

CryptoCurrency:EC2/BitcoinTool.A

EC2 实例与比特币矿池通信。

默认严重性：高

这一发现告诉你，你Amazon环境中的 EC2 实例正在与比特币矿池通信。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。

补救建议：

如果此活动出乎意料，则您的实例可能会遭到入侵。有关更多信息，请参阅修复受感染的 EC2 实例 (p. 213)：

UnauthorizedAccess:IAMUser/UnusualASNCaller

从异常网络的 IP 地址调用了 API。

默认严重性：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。在所描述用户的整个Amazon使用历史中，从未观察到过该网络。此活动可能包括控制台登录、尝试启动 EC2 实例、创建新 IAM 用户、修改您的Amazon权限等。这可能表示未经授权访问您的Amazon资源。

补救建议：

如果此活动出乎意料，您的凭证可能会被泄露。有关更多信息，请参阅 修复被盗的凭证 Amazon (p. 215)。

按资源类型划分的调查结果

以下页面按与GuardDuty发现相关的资源类型进行分类：

- EC2 查找类型 (p. 94)
- EKS 运行时监控查找类型 (p. 111)
- AS3 结果类型 (p. 126)
- Kubernetes 审计日志查找类型 (p. 136)
- Lambda 保护查找类型 (p. 147)
- 恶意软件防护查找类型 (p. 150)

- RDS 保护查找类型 (p. 153)
- S3 查找类型 (p. 157)

调查结果表

下表显示了按基础数据源或功能排序的所有活动查找类型（如果适用）。以下某些查找类型可能具有不同的严重性，由星号 (*) 表示。有关查找结果类型的可变严重性的信息，请查看该查找结果类型的详细描述。

结果类型	资源类型	基础数据源/功能	查找严重程度
Discovery:S3/AnomalousBehavior (p. 158)	Amazon S3	CloudTrailS3 的数据事件	低
Discovery:S3/MaliciousIPCaller (p. 158)	Amazon S3	CloudTrailS3 的数据事件	高
Discovery:S3/MaliciousIPCaller.Custom (p. 159)	Amazon S3	CloudTrailS3 的数据事件	高
Discovery:S3/TorIPCaller (p. 159)	Amazon S3	CloudTrailS3 的数据事件	中
Exfiltration:S3/AnomalousBehavior (p. 159)	Amazon S3	CloudTrailS3 的数据事件	高
Exfiltration:S3/MaliciousIPCaller (p. 160)	Amazon S3	CloudTrailS3 的数据事件	高
Impact:S3/AnomalousBehavior.Delete (p. 160)	Amazon S3	CloudTrailS3 的数据事件	高
Impact:S3/AnomalousBehavior.Permission (p. 161)	Amazon S3	CloudTrailS3 的数据事件	高
Impact:S3/AnomalousBehavior.Write (p. 161)	Amazon S3	CloudTrailS3 的数据事件	中
Impact:S3/MaliciousIPCaller (p. 162)	Amazon S3	CloudTrailS3 的数据事件	高
PenTest:S3/KaliLinux (p. 162)	Amazon S3	CloudTrailS3 的数据事件	中
PenTest:S3/ParrotLinux (p. 162)	Amazon S3	CloudTrailS3 的数据事件	中
PenTest:S3/PentooLinux (p. 163)	Amazon S3	CloudTrailS3 的数据事件	中
UnauthorizedAccess:S3/TorIPCaller (p. 165)	Amazon S3	CloudTrailS3 的数据事件	高
UnauthorizedAccess:S3/MaliciousIPCaller.Custom (p. 165)	Amazon S3	CloudTrailS3 的数据事件	高
CredentialAccess:IAMUser/AnomalousBehavior (p. 126)	IAM	CloudTrail管理活动	中

结果类型	资源类型	基础数据源/功能	查找严重程度
DefenseEvasion:IAMUser/AnomalousBehavior (p. 127)	IAM	CloudTrail管理活动	中
Discovery:IAMUser/AnomalousBehavior (p. 127)	IAM	CloudTrail管理活动	低
Exfiltration:IAMUser/AnomalousBehavior (p. 128)	IAM	CloudTrail管理活动	高
Impact:IAMUser/AnomalousBehavior (p. 128)	IAM	CloudTrail管理活动	高
InitialAccess:IAMUser/AnomalousBehavior (p. 129)	IAM	CloudTrail管理活动	中
PenTest:IAMUser/KaliLinux (p. 129)	IAM	CloudTrail管理活动	中
PenTest:IAMUser/ParrotLinux (p. 129)	IAM	CloudTrail管理活动	中
PenTest:IAMUser/PentooLinux (p. 130)	IAM	CloudTrail管理活动	中
Persistence:IAMUser/AnomalousBehavior (p. 130)	IAM	CloudTrail管理活动	中
Stealth:IAMUser/PasswordPolicyChange (p. 133)	IAM	CloudTrail管理活动	低*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS (p. 133)	IAM	CloudTrail管理活动	高*
Policy:S3/AccountBlockPublicAccessDisabled (p. 163)	Amazon S3	CloudTrail管理活动	低
Policy:S3/BucketAnonymousAccessGranted (p. 163)	Amazon S3	CloudTrail管理活动	高
Policy:S3/BucketBlockPublicAccessDisabled (p. 164)	Amazon S3	CloudTrail管理活动	低
Policy:S3/BucketPublicAccessGranted (p. 164)	Amazon S3	CloudTrail管理活动	高
PrivilegeEscalation:IAMUser/AnomalousBehavior (p. 131)	IAM	CloudTrail管理活动	中
Recon:IAMUser/MaliciousIPCaller (p. 131)	IAM	CloudTrail管理活动	中
Recon:IAMUser/MaliciousIPCaller.Custom (p. 132)	IAM	CloudTrail管理活动	中
Recon:IAMUser/TorIPCaller (p. 132)	IAM	CloudTrail管理活动	中
Stealth:IAMUser/CloudTrailLoggingDisabled (p. 132)	IAM	CloudTrail管理活动	低

结果类型	资源类型	基础数据源/功能	查找严重程度
Stealth:S3/ServerAccessLoggingDisabled (p. 165)	Amazon S3	CloudTrail管理活动	低
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B (p. 133)	IAM	CloudTrail管理活动	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller (p. 135)	IAM	CloudTrail管理活动	中
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom (p. 135)	IAM	CloudTrail管理活动	中
UnauthorizedAccess:IAMUser/TorIPCaller (p. 135)	IAM	CloudTrail管理活动	中
Policy:IAMUser/RootCredentialUsage (p. 130)	IAM	CloudTrailS3 的管理事件或CloudTrail数据事件	低
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS (p. 134)	IAM	CloudTrailS3 的管理事件或CloudTrail数据事件	高
Backdoor:EC2/C&CActivity.B!DNS (p. 96)	Amazon EC2	DNS 日志	高
CryptoCurrency:EC2/BitcoinTool.B!DNS (p. 100)	Amazon EC2	DNS 日志	高
Impact:EC2/AbusedDomainRequest.Reputation (p. 101)	Amazon EC2	DNS 日志	中
Impact:EC2/BitcoinDomainRequest.Reputation (p. 101)	Amazon EC2	DNS 日志	高
Impact:EC2/MaliciousDomainRequest.Reputation (p. 102)	Amazon EC2	DNS 日志	高
Impact:EC2/SuspiciousDomainRequest.Reputation (p. 103)	Amazon EC2	DNS 日志	低
Trojan:EC2/BlackholeTraffic!DNS (p. 105)	Amazon EC2	DNS 日志	中
Trojan:EC2/DGADomainRequest.B (p. 105)	Amazon EC2	DNS 日志	高
Trojan:EC2/DGADomainRequest.C!DNS (p. 106)	Amazon EC2	DNS 日志	高
Trojan:EC2/DNSDataExfiltration (p. 106)	Amazon EC2	DNS 日志	高
Trojan:EC2/DriveBySourceTraffic!DNS (p. 107)	Amazon EC2	DNS 日志	高

结果类型	资源类型	基础数据源/功能	查找严重程度
Trojan:EC2/DropPoint!DNS (p. 107)	Amazon EC2	DNS 日志	中
Trojan:EC2/PhishingDomainRequest!DNS (p. 108)	Amazon EC2	DNS 日志	高
UnauthorizedAccess:EC2/MetadataDNSRebind (p. 108)	Amazon EC2	DNS 日志	高
Execution:Container/MaliciousFile (p. 151)	容器	EBS 卷	因检测到的威胁而异
Execution:Container/SuspiciousFile (p. 153)	容器	EBS 卷	因检测到的威胁而异
Execution:EC2/MaliciousFile (p. 150)	EC2	EBS 卷	因检测到的威胁而异
Execution:EC2/SuspiciousFile (p. 151)	EC2	EBS 卷	因检测到的威胁而异
Execution:ECS/MaliciousFile (p. 151)	ECS	EBS 卷	因检测到的威胁而异
Execution:ECS/SuspiciousFile (p. 152)	ECS	EBS 卷	因检测到的威胁而异
Execution:Kubernetes/MaliciousFile (p. 151)	Kubernetes	EBS 卷	因检测到的威胁而异
Execution:Kubernetes/SuspiciousFile (p. 152)	Kubernetes	EBS 卷	因检测到的威胁而异
CredentialAccess:Kubernetes/MaliciousIPCaller (p. 137)	Kubernetes	Kubernetes 审计日志	高
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom (p. 137)	Kubernetes	Kubernetes 审计日志	高
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess (p. 138)	Kubernetes	Kubernetes 审计日志	高
CredentialAccess:Kubernetes/TorIPCaller (p. 138)	Kubernetes	Kubernetes 审计日志	高
DefenseEvasion:Kubernetes/MaliciousIPCaller (p. 138)	Kubernetes	Kubernetes 审计日志	高
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom (p. 139)	Kubernetes	Kubernetes 审计日志	高
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess (p. 139)	Kubernetes	Kubernetes 审计日志	高
DefenseEvasion:Kubernetes/TorIPCaller (p. 140)	Kubernetes	Kubernetes 审计日志	高

结果类型	资源类型	基础数据源/功能	查找严重程度
Discovery:Kubernetes/MaliciousIPCaller (p. 140)	Kubernetes	Kubernetes 审计日志	中
Discovery:Kubernetes/MaliciousIPCaller.Custom (p. 140)	Kubernetes	Kubernetes 审计日志	中
Discovery:Kubernetes/SuccessfulAnonymousAccess (p. 141)	Kubernetes	Kubernetes 审计日志	中
Discovery:Kubernetes/TorIPCaller (p. 141)	Kubernetes	Kubernetes 审计日志	中
Execution:Kubernetes/ExecInKubeSystemPod (p. 142)	Kubernetes	Kubernetes 审计日志	中
Impact:Kubernetes/MaliciousIPCaller (p. 142)	Kubernetes	Kubernetes 审计日志	高
Impact:Kubernetes/MaliciousIPCaller.Custom (p. 142)	Kubernetes	Kubernetes 审计日志	高
Impact:Kubernetes/SuccessfulAnonymousAccess (p. 143)	Kubernetes	Kubernetes 审计日志	高
Impact:Kubernetes/TorIPCaller (p. 143)	Kubernetes	Kubernetes 审计日志	高
Persistence:Kubernetes/ContainerWithSensitiveMount (p. 143)	Kubernetes	Kubernetes 审计日志	中
Persistence:Kubernetes/MaliciousIPCaller (p. 144)	Kubernetes	Kubernetes 审计日志	中
Persistence:Kubernetes/MaliciousIPCaller.Custom (p. 144)	Kubernetes	Kubernetes 审计日志	中
Persistence:Kubernetes/SuccessfulAnonymousAccess (p. 145)	Kubernetes	Kubernetes 审计日志	高
Persistence:Kubernetes/TorIPCaller (p. 145)	Kubernetes	Kubernetes 审计日志	中
Policy:Kubernetes/AdminAccessToDefaultServiceAccount (p. 145)	Kubernetes	Kubernetes 审计日志	高
Policy:Kubernetes/AnonymousAccessGranted (p. 146)	Kubernetes	Kubernetes 审计日志	高
Policy:Kubernetes/KubeflowDashboardExposed (p. 146)	Kubernetes	Kubernetes 审计日志	中
Policy:Kubernetes/ExposedDashboard (p. 146)	Kubernetes	Kubernetes 审计日志	中
PrivilegeEscalation:Kubernetes/PrivilegedContainer (p. 147)	Kubernetes	Kubernetes 审计日志	中
Backdoor:Lambda/C&CActivity.B (p. 147)	Lambda	Lambda 网络活动监控	高

结果类型	资源类型	基础数据源/功能	查找严重程度
CryptoCurrency:Lambda/BitcoinTool.B (p. 148)	Lambda	Lambda 网络活动监控	高
Trojan:Lambda/BlackholeTraffic (p. 148)	Lambda	Lambda 网络活动监控	中
Trojan:Lambda/DropPoint (p. 149)	Lambda	Lambda 网络活动监控	中
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom (p. 149)	Lambda	Lambda 网络活动监控	中
UnauthorizedAccess:Lambda/TorClient (p. 149)	Lambda	Lambda 网络活动监控	高
UnauthorizedAccess:Lambda/TorRelay (p. 150)	Lambda	Lambda 网络活动监控	高
CredentialAccess:RDS/AnomalousBehavior.FailedLogin (p. 154)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	低
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce (p. 154)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	高
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin (p. 153)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	变量*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin (p. 155)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	中
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin (p. 155)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	高
CredentialAccess:RDS/TorIPCaller.FailedLogin (p. 156)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	中
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin (p. 156)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	高
Discovery:RDS/MaliciousIPCaller (p. 156)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	中
Discovery:RDS/TorIPCaller (p. 157)	支持的亚马逊 Aurora 数据库 (p. 68)	RDS 登录活动监控	中
Backdoor:Runtime/C&CActivity.B (p. 157)	实例、eksCluster 或容器	运行时监控	高

结果类型	资源类型	基础数据源/功能	查找严重程度
Backdoor:Runtime/C&CActivity.B!DNS (p. 115)	实例、eksCluster或容器	运行时监控	高
CryptoCurrency:Runtime/BitcoinTool.B (p. 113)	实例、eksCluster或容器	运行时监控	高
CryptoCurrency:Runtime/BitcoinTool.B!DNS (p. 115)	实例、eksCluster或容器	运行时监控	高
DefenseEvasion:Runtime/FilelessExecution (p. 116)	实例、eksCluster或容器	运行时监控	中
DefenseEvasion:Runtime/ProcessInjection.Proc (p. 122)	实例、eksCluster或容器	运行时监控	高
DefenseEvasion:Runtime/ProcessInjection.Ptrace (p. 123)	实例、eksCluster或容器	运行时监控	中
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite (p. 123)	实例、eksCluster或容器	运行时监控	高
Execution:Runtime/NewBinaryExecuted (p. 120)	实例、eksCluster或容器	运行时监控	中
Execution:Runtime/NewLibraryLoaded (p. 120)	实例、eksCluster或容器	运行时监控	中
Execution:Runtime/ReverseShell (p. 123)	实例、eksCluster或容器	运行时监控	高
Impact:Runtime/AbusedDomainRequest.Reputation (p. 118)	实例、eksCluster或容器	运行时监控	中
Impact:Runtime/BitcoinDomainRequest.Reputation (p. 118)	实例、eksCluster或容器	运行时监控	高
Impact:Runtime/CryptoMinerExecuted (p. 124)	实例、eksCluster或容器	运行时监控	高
Impact:Runtime/MaliciousDomainRequest.Reputation (p. 119)	实例、eksCluster或容器	运行时监控	中
Impact:Runtime/SuspiciousDomainRequest.Reputation (p. 119)	实例、eksCluster或容器	运行时监控	低
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified (p. 122)	实例、eksCluster或容器	运行时监控	高
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory (p. 125)	实例、eksCluster或容器	运行时监控	中
PrivilegeEscalation:Runtime/DockerSocketAccessed (p. 121)	实例、eksCluster或容器	运行时监控	中
PrivilegeEscalation:Runtime/RuncContainerEscape (p. 121)	实例、eksCluster或容器	运行时监控	高

结果类型	资源类型	基础数据源/功能	查找严重程度
PrivilegeEscalation:Runtime/UserfaultfdUsage (p. 实例、eksCluster或容器		运行时监控	中
Trojan:Runtime/BlackholeTraffic (p. 实例、eksCluster或容器		运行时监控	中
Trojan:Runtime/BlackholeTraffic!DNS (p. 116)	实例、eksCluster或容器	运行时监控	中
Trojan:Runtime/DropPoint (p. 114)	实例、eksCluster或容器	运行时监控	中
Trojan:Runtime/DGADomainRequest.B!DNS (p. 116)	实例、eksCluster或容器	运行时监控	高
Trojan:Runtime/DriveBySourceTraffic!DNS (p. 117)	实例、eksCluster或容器	运行时监控	高
Trojan:Runtime/DropPoint!DNS (p. 116)	实例、eksCluster或容器	运行时监控	中
Trojan:Runtime/PhishingDomainRequest!DNS (p. 117)	实例、eksCluster或容器	运行时监控	高
UnauthorizedAccess:Runtime/MetadataDNSRebind (p. 120)	实例、eksCluster或容器	运行时监控	高
UnauthorizedAccess:Runtime/TorClient (p. 113)	实例、eksCluster或容器	运行时监控	高
UnauthorizedAccess:Runtime/TorRelay (p. 113)	实例、eksCluster或容器	运行时监控	高
Backdoor:EC2/C&CActivity.B (p. 95)	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Dns (p. 96)	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Tcp (p. 97)	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.Udp (p. 97)	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.UdpOnTcpPorts (p. 97)	EC2	VPC 流日志	高
Backdoor:EC2/DenialOfService.UnusualProtocol (p. 98)	EC2	VPC 流日志	高
Backdoor:EC2/Spambot (p. 98)	EC2	VPC 流日志	Mediu

结果类型	资源类型	基础数据源/功能	查找严重程度
Behavior:EC2/NetworkPortUnusual (p. 98)	EC2	VPC 流日志	中
Behavior:EC2/TrafficVolumeUnusual (p. 99)	EC2	VPC 流日志	中
CryptoCurrency:EC2/BitcoinTool.B (p. 99)	EC2	VPC 流日志	高
DefenseEvasion:EC2/UnusualDNSResolver (p. 100)	EC2	VPC 流日志	中
DefenseEvasion:EC2/UnusualDoHActivity (p. 100)	EC2	VPC 流日志	中
DefenseEvasion:EC2/UnusualDoTActivity (p. 101)	EC2	VPC 流日志	中
Impact:EC2/PortSweep (p. 102)	EC2	VPC 流日志	高
Impact:EC2/WinRMBruteForce (p. 103)	EC2	VPC 流日志	低*
Recon:EC2/PortProbeEMRUnprotectedPort (p. 103)	EC2	VPC 流日志	高
Recon:EC2/PortProbeUnprotectedPort (p. 104)	EC2	VPC 流日志	低*
Recon:EC2/Portscan (p. 104)	EC2	VPC 流日志	中
Trojan:EC2/BlackholeTraffic (p. 105)	EC2	VPC 流日志	中
Trojan:EC2/DropPoint (p. 107)	EC2	VPC 流日志	中
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom (p. 108)	EC2	VPC 流日志	中
UnauthorizedAccess:EC2/RDPBruteForce (p. 109)	EC2	VPC 流日志	低*
UnauthorizedAccess:EC2/SSHBruteForce (p. 109)	EC2	VPC 流日志	低*
UnauthorizedAccess:EC2/TorClient (p. 110)	EC2	VPC 流日志	高
UnauthorizedAccess:EC2/TorRelay (p. 110)	EC2	VPC 流日志	高

管理亚马逊的GuardDuty调查结果

GuardDuty提供多项重要功能，可帮助您排序、存储和管理发现。这些功能将帮助您根据特定环境量身定制调查结果，减少低价值发现带来的干扰，并帮助您专注于独特Amazon环境面临的威胁。查看本页上的主题，了解如何使用这些功能来提高发现GuardDuty的价值。

话题：

筛选结果 (p. 183)

了解如何根据您指定的标准筛选GuardDuty调查结果。

抑制规则 (p. 187)

了解如何通过隐藏规则自动筛选发现的GuardDuty警报提醒。抑制规则会根据过滤器自动存档调查结果。

处理可信 IP 列表和威胁列表 (p. 191)

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，而威胁 Intel 列表将促使 GuardDuty 提醒您来自用户定义的 IP 的活动。

导出调查结果 (p. 196)

配置自动将您的发现结果导出到 S3 存储桶，这样您就可以维护超过 90 天调查结果保留期的记录。这些历史数据可用于跟踪您账户中的可疑活动，并帮助您评估补救措施是否成功。

使用 Amazon Ev CloudWatch ents 创建对GuardDuty调查结果的自定义 (p. 202)

通过亚马逊CloudWatch活动为GuardDuty发现情况设置自动通知。您还可以通过CloudWatch事件自动执行其他任务，以帮助您对调查结果做出回应。

了解恶意软件防护扫描期间跳过资源 CloudWatch 的日志和原因 (p. 209)

了解如何审核GuardDuty恶意软件防护CloudWatch日志，以及在扫描过程中跳过受影响的 Amazon EC2 实例或 Amazon EBS 卷的原因是什么。

报告 GuardDuty 恶意软件保护中的误报 (p. 212)

了解GuardDuty恶意软件防护中的误报体验以及如何报告误报威胁检测。

筛选结果

查找结果筛选器允许您查看与指定条件匹配的查找结果，并筛选出任何不匹配的查找结果。您可以使用亚马逊GuardDuty控制台轻松创建查找过滤器，也可以使用 JSON 使用 CreateFilterAPI 创建它们。查看以下部分以了解如何在控制台中创建过滤器。要使用这些过滤器自动存档传入的调查结果，请参阅抑制规则 (p. 187)。

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过滤器，以便在禁止规则或future 过滤器操作中使用。过滤器由至少一个筛选条件组成，该筛选条件由一个过滤器属性与至少一个值配对组成。

在创建过滤器，请注意以下事项：

- 过滤器不接受通配符。
- 您可以指定最少一个属性和最多 50 个属性作为特定筛选器的标准。
- 当您使用等于或不等于条件筛选属性值（例如账户 ID）时，最多可以指定 50 个值。

- 每个筛选条件属性都作为AND运算符进行评估。同一属性的多个值的计算结果为AND/OR。

筛选调查结果（控制台）

1. 在显示的GuardDuty发现列表上方选择添加筛选条件。
2. 在扩展的属性列表中，选择要指定为筛选条件的属性，例如账户 ID 或操作类型。

   Note

   有关可用于创建筛选条件的属性列表，请参阅本页上的过滤器属性表。
3. 在显示的文本字段中，为每个选定属性指定一个值，然后选择 A pply。

   Note

   应用过滤器后，您可以通过选择筛选器名称左侧的黑点将过滤器转换为排除与筛选器匹配的搜索结果。这实际就为所选属性创建了一个“不等于”筛选条件。
4. 要将指定的属性及其值 (筛选条件) 另存为筛选器，请选择保存。输入筛选器名称和描述，然后选择 “完成”。

过滤器属性

使用 API 操作创建筛选器或对结果进行排序时，必须在 JSON 中指定筛选条件。这些筛选条件与调查结果的详细信息 JSON 相关。下表包含过滤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
账户 ID	accountId
结果 ID	id
区域	区域
严重性	severity
结果类型	type
更新时间	updatedAt
访问密钥 ID	资源。 accessKeyDetails。 accessKeyId
委托人 ID	资源。 accessKeyDetails.principalID
Username	资源。 accessKeyDetails.userName
用户类型	资源。 accessKeyDetails.用户类型
IAM 实例配置文件 ID	资源.instanceDetails。 iamInstanceProfile.id
实例 ID	resource.instanceDetails.instanceId
实例映像 ID	resource.instanceDetails.imageId
实例标签键	resource.instanceDetails.tags.key
实例标签值	resource.instanceDetails.tags.value
IPv6 地址	resource.instanceDetails.networkInterfaces.ipv6Addresses

控制台字段名称	JSON 字段名称
私有 IPv4 地址	资源。实例详情。网络接口。 privateIpAddresses。privateIpAddress
公有 DNS 名称	资源。实例详情。网络接口。 publicDnsName
公有 IP	resource.instanceDetails.networkInterfaces.publicIp
安全组 ID	resource.instanceDetails.networkInterfaces.securityGroups.groupI
安全组名称	resource.instanceDetails.networkInterfaces.securityGroups.groupN
子网 ID	resource.instanceDetails.networkInterfaces.subnetId
VPC ID	resource.instanceDetails.networkInterfaces.vpcId
Outpost ARN	resource.instanceDetails.outpostARN
资源类型	resource.resourceType
存储桶权限	资源.s3 .publicAccess.有效权限 BucketDetails
Bucket name（桶名称）	资源.s3 .name BucketDetails
Bucket tag key	资源.s3 .tags.key BucketDetails
Bucket tag value	资源.s3 .tags.value BucketDetails
存储桶类型	资源.s3 .type BucketDetails
操作类型	service.action.actionType
调用的 API	服务.action。 awsApiCallAction.api
API 调用方类型	服务.action。 awsApiCall操作。呼叫者类型
API 错误码	服务.action。 awsApiCallaction.错误代码
API 调用方城市	服务.action。 awsApiCall行动。remoteIpDetails.city.cityName
API 调用方国家/地区	服务.action。 awsApiCall行动。remoteIpDetails.country.countr
API 调用方 IPv4 地址	服务.action。 awsApiCall行动。remoteIpDetails.ipAddressv4
API 调用方 ASN ID	服务.action。 awsApiCall行动。remoteIpDetails.organizon.asn
API 调用方 ASN 名称	服务.action。 awsApiCall行动。remoteIpDetails.organizon.asnorg
API 调用方服务名称	服务.action。 awsApiCall操作.serviceName
DNS 请求域	服务.action。 dnsRequestAction. 域
网络连接受阻	服务.action。 networkConnectionAction. 已阻止
网络连接方向	服务.action。 networkConnectionAction. 连接方向

控制台字段名称	JSON 字段名称
网络连接本地端口	服务.action。 networkConnectionAction。 localPortDetails. 端口
网络连接协议	服务.action。 networkConnectionAction. 协议
网络连接城市	服务.action。 networkConnectionAction。 remoteIpDetails.city.cityName
网络连接国家/地区	服务.action。 networkConnectionAction。 remoteIpDetails.country.countr
网络连接远程 IPv4 地址	服务.action。 networkConnectionAction。 remoteIpDetails.ipAddressv4
网络连接远程 IP ASN ID	服务.action。 networkConnectionAction。 remoteIpDetails.organizon.asn
网络连接远程 IP ASN 名称	服务.action。 networkConnectionAction。 remoteIpDetails.organizon.asnorg
网络连接远程端口	服务.action。 networkConnectionAction。 remotePortDetails. 端口
关联的远程帐户	服务.action。 awsApiCall行动。 remoteAccountDetails. 关联
Kubernetes API 调用者 IPv4 地址	服务.action。 kubernetesApiCall行动。 remoteIpDetails.ipAddressv4
Kubernetes API 调用请求 URI	服务.action。 kubernetesApiCall操作。请求 URI
网络连接本地 IPv4 地址	服务.action。 networkConnectionAction。 localIpDetails.ipAddressv4
协议	服务.action。 networkConnectionAction. 协议
API 调用服务名称	服务.action。 awsApiCall操作.serviceName
API 呼叫者账户 ID	服务.action。 awsApiCall行动。 remoteAccountDetails.accountId
威胁列表名称	服务。附加信息。 threatListName
资源角色	service.resourceRole
EKS 集群名称	资源。 eksClusterDetails.name
Kubernetes 工作负载名称	资源.kubernetes详情。 kubernetesWorkloadDetails.name
Kubernetes 工作负载命名空间	资源.kubernetes详情。 kubernetesWorkloadDetails.命名空间
Kubernetes 用户名	资源.kubernetes详情。 kubernetesUserDetails.用户名
Kubernetes 容器镜像	资源.kubernetes详情。 kubernetesWorkloadDetails.containers.im

控制台字段名称	JSON 字段名称
Kubernetes 容器镜像前缀	资源.kubernetes详情。kubernetesWorkloadDetails. 容器.图片前缀
扫描	sect。 ebsVolumeScan详细信息.scanID
威胁者名称	sect。 ebsVolumeScan详细信息。扫描检测。threatDetectedBy名称.threatnames.Name
威胁的严重性	sect。 ebsVolumeScan详细信息。扫描检测。threatDetectedBy名称。威胁名称。严重性
文件 SHA	sect。 ebsVolumeScan详细信息。扫描检测。threatDetectedByname.threatnames.filepaths
ECS 集群名称	资源。 ecsClusterDetails.name
ECS 容器镜像	资源。 ecsClusterDetails.taskdetails.Containers
ECS 任务定义 ARN	资源。 ecsClusterDetails.taskDetails.definit
独立的容器映像	资源.容器详细信息.图片
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详情。引擎
数据库用户	资源。 rdsDbUser详细信息。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详细信息.tags.value
可执行文件 SHA-256	service.runtimeDetails.process.ex
Process name	service.runtimeDetails.pro
可执行文件路径	service.runtimeDetails.process.
Lambda 函数名称	资源.lambdaDetails.函数名称
Lambda 函数 ARN	resource.lambdaDetails.f
Lambda 函数标签键	资源.lambdaDetails.tags.key
Lambda 函数标签值	资源.lambdaDetails.tags.value

抑制规则

隐藏规则是一组条件，由筛选属性与值配对组成，用于通过自动存档与指定条件相匹配的新发现结果来筛选查找结果。隐藏规则可用于筛选低价值调查结果、误报调查结果或您不打算应对的威胁，以便更轻松地识别对环境影响最大的安全威胁。

创建隐藏规则后，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结果。您可以使用现有筛选器创建抑制规则，也可以从您定义的新过滤器创建抑制规则。您可以配置禁止规则以禁止整个调查结果类型，或者定义更精细的筛选条件，仅禁止特定调查结果类型的特定实例。可以随时编辑您的隐藏规则。

隐藏的调查结果不会发送给Amazon Security Hub亚马逊 Simple Storage Service、Amazon Detective 或亚马逊 EventBridge，如果您通过 Security Hub、第三方 SIEM 或其他警报和票务应用程序使用 GuardDuty 调查结果，则会降低查找结果的噪音水平。如果您已启用GuardDuty恶意软件防护 (p. 48)，则隐藏的 GuardDuty 发现结果将不会启动恶意软件扫描。

GuardDuty 即使搜索结果与您的抑制规则相符，仍会继续生成结果，但是，这些发现会自动标记为已存档。存档的调查结果存储 90 天，在此期间可以随时查看。 GuardDuty 您可以通过从发现结果表中选择 “已存档” 来在 GuardDuty 控制台中查看隐藏的调查结果，也可以使用`findingCriteria`条件`service.archived`等于 true 的 ListFindingsAPI 通过 API 查看隐藏的调查结果。 GuardDuty

Note

在多账户环境中，只有 GuardDuty 管理员可以创建禁止规则。

抑制规则的常见用例和示例

以下查找结果类型有应用隐藏规则的常见用例，选择查找结果名称以了解有关该查找结果的更多信息，或者查看信息以从控制台为该查找结果类型生成隐藏规则。

Important

GuardDuty 建议您响应性地制定抑制规则，并且仅针对您反复发现了误报的发现制定抑制规则。

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS (p. 134)— 使用抑制规则自动存档在 VPC 网络配置为路由互联网流量，使其从本地网关而不是从 VPC InterInternet Gateway et 网关传出时生成的调查结果。

  当网络配置为路由互联网流量，使其从本地网关而不是从 VPC Internet Gateway (IGW) 传出时，就会生成此发现。常见配置，例如使用Amazon 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，则建议您在 中使用隐藏规则，并创建一个由两个筛选标准组成的规则。第一个标准是 finding type (调查结果类型)，它应是 `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration`。第二个筛选条件是 API 调用者 IPv4 地址以及您的本地互联网网关的 IP 地址或 CIDR 范围。以下示例显示了根据 API 调用者 IP 地址隐藏此查找类型的过滤器。

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration API caller IPv4
 address: 198.51.100.6
```

  Note

  要包含多个 API 调用方 IP，您可以为每个调用方 IP 添加新的 API 调用者 IPv4 地址过滤器。

- Recon:EC2/Portscan (p. 104)— 使用漏洞评估应用程序时，使用抑制规则自动存档调查结果。

  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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪些标准。以下示例显示了您可以根据具有特定 AMI 的实例来隐藏此查找类型的过滤器。

```
Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
```

- UnauthorizedAccess:EC2/SSHBruteForce (p. 109)— 当发现以堡垒实例为目标时，使用抑制规则自动存档结果。

  如果暴力攻击的目标是堡垒主机，则这可能代表您的Amazon环境的预期行为。如果是这种情况，我们建议您为此调查结果设置禁止规则。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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪些标准。以下示例显示了根据具有特定实例标签值的实例隐藏此查找类型的过滤器。

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort (p. 104)— 当发现的目标是故意暴露的实例时，使用抑制规则自动归档结果。

  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Amazon环境属于这种情况，我们建议您为此发现设置抑制规则。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 `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 Tag value 属性，具体取决于托管这些工具的实例可以识别哪个标准。以下示例显示了您可以根据控制台中具有特定实例标签密钥的实例来隐藏此查找类型的过滤器。

```
Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
```

EKS 运行时监控结果的推荐抑制规则

- PrivilegeEscalation:Runtime/DockerSocketAccessed (p. 121)当容器内的进程与 Docker 套接字通信时生成。出于正当理由，您的环境中可能有些容器可能需要访问 Docker 套接字。从此类容器访问将生成PrivilegeEscalation:Runtime/DockerSocketAccessed搜索结果。如果您的Amazon环境属于这种情况，我们建议您为该查找类型设置抑制规则。第一个条件应使用值等于的查找类型字段`PrivilegeEscalation:Runtime/DockerSocketAccessed`。第二个筛选条件是可执行路径字段，其值等于生成的查找结果`executablePath`中进程的值。或者，第二个筛选条件可以使用可执行的 SHA-256 字段，其值等于生成的查找结果`executableSha256`中进程的值。
- Kubernetes 集群以 pod 的形式运行自己的 DNS 服务器，例如`coredns`。因此，每次从 pod 查找 DNS 时，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 调查结果生成重复项：
  - Backdoor:Runtime/C&CActivity.B!DNS (p. 115)
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS (p. 115)
  - Impact:Runtime/AbusedDomainRequest.Reputation (p. 118)
  - Impact:Runtime/BitcoinDomainRequest.Reputation (p. 118)
  - Impact:Runtime/MaliciousDomainRequest.Reputation (p. 119)
  - Impact:Runtime/SuspiciousDomainRequest.Reputation (p. 119)
  - Trojan:Runtime/BlackholeTraffic!DNS (p. 116)
  - Trojan:Runtime/DGADomainRequest.C!DNS (p. 116)
  - Trojan:Runtime/DriveBySourceTraffic!DNS (p. 117)
  - Trojan:Runtime/DropPoint!DNS (p. 116)
  - Trojan:Runtime/PhishingDomainRequest!DNS (p. 117)

  重复的发现将包括与您的 DNS 服务器 pod 对应的 pod、容器和进程的详细信息。您可以设置禁止规则，使用这些字段隐藏这些重复的发现。第一个筛选条件应使用查找类型字段，其值等于本节前面提供的发现列表中的 DNS 查找类型。第二个筛选条件可以是值等于您的 DNS 服务器的可执行路径，**`executablePath`**也可以是值等于生成的查找结果**`executableSHA256`**中的 DNS 服务器的可执行路径 SHA-256。作为可选的第三个筛选条件，您可以使用 Kubernetes 容器图像字段，其值等于生成的查找结果中您的 DNS 服务器 pod 的容器映像。

在中创建抑制规则 GuardDuty

选择您的访问方法以在中创建或管理禁止规则 GuardDuty。

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过滤器相同，现有已保存的过滤器可用作抑制规则。有关创建过滤器的更多信息，，，筛选结果 (p. 183)。

使用控制台创建禁止规则

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在“发现结果”页面上，选择“隐藏调查结果”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**filter criteria**中输入。您可以从列表中选择标准。输入所选标准的有效值。

   Note

   要确定有效值，请查看发现结果表并选择要隐藏的查找结果。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，并确保只有那些要隐藏的查找结果出现在表格中。
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 (.)、短划线 (-) 和空格。
5. 选择保存。

您还可以从现有已保存的过滤器中创建抑vate。有关创建过滤器的更多信息，，，筛选结果 (p. 183)。

要从已保存的过滤器创建抑制规则，请执行以下操作：

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在“发现结果”页面上，选择“隐藏查找结果”以打开隐藏规则面板。
3. 从“保存的规则”下拉列表中，选择已保存的过滤器。
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，跳过此步骤。

   要打开筛选条件菜单，请在添加筛选条件**filter criteria**中输入。您可以从列表中选择标准。输入所选标准的有效值。

   Note

   要确定有效值，请查看发现结果表并选择要隐藏的查找结果。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 (.)、短划线 (-) 和空格。
6. 选择保存。

删除规则

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在“发现结果”页面上，选择“隐藏查找结果”以打开隐藏规则面板。
3. 从“保存的规则”下拉列表中，选择已保存的过滤器。
4. 选择 Delete rule (删除规则)。

API

要使用 API 创建抑制规则，请执行以下操作：

1. 您可以通过 CreateFilterAPI 创建禁止规则。为此，请按照下面详述的示例的格式在 JSON 文件中指定筛选条件。以下示例将抑制向 test.example.com 发出 DNS 请求的任何未存档的结果。

```
{
```

```
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        }
    }
}
```

有关 JSON 字段名及其控制台等效项的列表，请参阅过滤器属性 (p. 184)。

要测试您的筛选条件，请在 ListFindingsAPI 中使用相同的 JSON 标准，并确认选择了正确的结果。要使用您自己的 detectorId 和.json 文件来测试您的筛选条件，Amazon CLI请按照示例进行操作。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. CreateFilter通过 API 上传您的过滤器以用作抑制规则，或者按照以下示例使用Amazon CLI 使用您自己的检测器 ID、抑制规则的名称和.json 文件。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

您可以使用 ListFilterAPI 以编程方式查看过滤器列表。您可以通过向 GetFilterAPI 提供筛选器名称来查看单个筛选器的详细信息。使用 DeleteFilterAPI 更新过滤器UpdateFilter或将其删除。

处理可信 IP 列表和威胁列表

Amazon 通过分析和处理 VPC 流日志、Amazon CloudTrail事件日志和 DNS 日志来 GuardDuty 监控您的Amazon环境安全。您可以通过配置 GuardDuty 为停止来自您自己的可信 IP 列表的可信 IP 的警报并对您自己的威胁列表中的已知恶意 IP 发出警报来自定义此监控范围。

可信 IP 列表和威胁列表仅适用于发往可公开路由 IP 地址的流量。列表的影响适用于所有 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，用于与您的Amazon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。您最多可以在单

个受信任的 IP 列表中包括 2000 个 IP 地址和 CIDR 范围。在任何给定时间，每个区域的每个Amazon账户只能上传一个可信 IP 列表。

威胁 IP 列表

威胁列表包含已知的恶意 IP 地址。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。除了根据潜在的可疑活动生成调查结果外， GuardDuty 还会根据这些威胁列表生成调查结果。在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的 IP 地址和 CIDR 范围的活动生成调查结果，不会根据域名生成调查结果。在任何给定时间，每个区域的每个Amazon账户最多可以上传六个威胁列表。

Note

如果您在可信 IP 列表和威胁列表中包含相同的 IP，则将首先由可信 IP 列表处理，不会生成调查结果。

在多账户环境中，只有 GuardDuty 管理员账户的用户才能上传和管理可信 IP 列表和威胁列表。管理员帐户上传的可信 IP 列表和威胁列表受其成员帐户的 GuardDuty 功能限制。换句话说，在成员账户 GuardDuty 中，根据涉及管理员威胁列表中已知恶意 IP 地址的活动生成调查结果，而不是根据涉及管理员可信 IP 列表中的 IP 地址的活动生成调查结果。有关更多信息，请参阅在亚马逊管理多个账户 GuardDuty (p. 224)：

列表格式

GuardDuty 接受以下格式的列表。

托管您的可信 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。仅接受 IPv4 地址。

- 纯文本 (TXT)

  此格式支持 CIDR 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 块和单个 IP 地址。以下样本列表使用 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">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- 开放威胁交易所 (OTX) ™ CSV

  此格式支持 CIDR 块和单个 IP 地址。以下示例列表使用OTX™ CSV 格式。

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ iSight 威胁情报 CSV

  此格式支持 CIDR 块和单个 IP 地址。以下示例列表使用FireEye™ CSV 格式。

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
 recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
 sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
 filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port, protocol,
 registrantEmail, registrantName, networkType, url, malwareFamily, malwareFamilyId,
 actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , ,
 Related, 198.51.100.1, , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint [TM] ET 情报提要

  此格式仅支持单个 IP 地址。以下示例列表使用Proofpoint CSV 格式。ports 参数是可选的。如果您跳过端口，请确保在末尾留下逗号 (,)。

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVault[TM] 声誉提要

  此格式仅支持单个 IP 地址。以下示例列表使用该AlienVault格式。

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

上传可信 IP 列表和威胁列表所需的权限

各种 IAM 身份需要特殊权限才能使用中的可信 IP 列表和威胁列表 GuardDuty。附带AmazonGuardDutyFullAccess (p. 266)托管策略的身份只能重命名和停用上传的可信 IP 列表和威胁列表。

要授予各种身份使用可信 IP 列表和威胁列表的完全访问权限（除了重命名和停用之外，还包括上传、激活、删除和更新列表的位置），请确保附加到用户、组或角色的权限策略中存在以下操作：

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> 这些操作不包含在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 支持以下列表加密类型：SSE-AES256 和 SSE-KMS。不支持 SSE-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。

如果您的列表是使用服务器端加密 SSE-KMS 加密的，则必须授予 GuardDuty 服务相关角色解密文件的AWSServiceRoleForAmazonGuardDuty权限才能激活该列表。将以下语句添加到 KMS 密钥策略中，并将账户 ID 替换为你自己的账户 ID：

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

上传可信 IP 列表和威胁列表

以下过程描述了如何使用 GuardDuty 控制台上传可信 IP 列表和威胁列表。

上传可信 IP 列表和威胁列表 (控制台)

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Settings 下，选择 Lists。
3. 在 List management 页面上，选择 Add a trusted IP list 或 Add a threat list。
4. 在对话框中，执行以下操作：
   - 对于列表名称，输入列表的名称。
   - 对于 Location，指定列表的位置 – 这是 S3 存储桶，您在其中存储可信 IP 列表或威胁列表以及包含您列表的文件。

     Note

     您可以按下列格式指定位置 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
   - 对于 Format，选择列表的文件类型。
   - 选中 “我同意” 复选框。
   - 选择 Add list。

激活或停用可信 IP 列表和威胁列表

以下过程描述了如何在可信 IP 列表和威胁列表上传 GuardDuty 后激活或停用它们。 GuardDuty 仅当上传的列表处于活动状态时，才将其包含在其对您的Amazon环境的监控中。

激活可信 IP 列表和威胁列表 (控制台)

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Settings 下，选择 Lists。
3. 在 List management (列表管理) 页面上，找到要激活的可信 IP 集或威胁列表，然后选择 Active (激活) 列下的单选按钮。

取消激活可信 IP 列表和威胁列表 (API 或 CLI)

- 您可以通过运行UpdateThreatIntelSet和UpdateIPSet操作或update-ip-set和 update-threat-intel-setCLI 命令来停用您的可信 IP 列表或威胁列表。

  例如，您可以运行以下命令：

  确保分别使用有效的*### ID* 和*ip-set-id*可信 IP 列表 ID 替换。

  你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws  guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0 --ip-set-
id ip-set-id --no-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

如果您对已上传并激活的可信 IP 列表或威胁列表进行更改 GuardDuty （例如，重命名该列表或向其添加更多 IP 地址），则必须更新此列表 GuardDuty 并重新激活它，才能在其安全监控范围内使用该列表的最新版本。 GuardDuty 要更新可信 IP 或威胁列表，您可以使用以下步骤或运行 GuardDuty API 的UpdateThreatIntelSet和UpdateIPSet操作。

更新可信 IP 列表和威胁列表 (控制台)

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中的 Settings 下，选择 Lists。
3. 在 List management (列表管理) 页面上，找到要更新的可信 IP 集或威胁列表，然后选择 Active (激活) 列下的铅笔图标。
4. 在 Update list 弹出窗口中，验证所有指定列表信息，选择 I agree，然后选择 Update list。
5. 在 List management (列表管理) 页面上，找到要再次激活的可信 IP 集或威胁列表，然后选择 Active (激活) 列下的单选按钮。

导出调查结果

GuardDuty 支持将活动发现导出到 CloudWatch 事件，也可以导出到 Amazon S3 存储桶。生成的新有效发现将在发现结果 GuardDuty 生成后大约 5 分钟内自动导出。您可以设置将活动发现的更新导出到 CloudWatch 事件的频率。您选择的频率适用于将新出现的现有发现导出到 CloudWatch 事件、您的 S3 存储桶（如果已配置）和 Detective（如果已集成）。有关现有调查结果更新的更多信息，请参阅GuardDuty查找聚合 (p. 93)。

请注意以下有关发现结果导出设置的注意事项：

- 导出设置是区域性的，这意味着您需要为所使用的每个区域配置导出选项 GuardDuty。但是，您可以在单个区域中使用相同的存储桶作为您使用的每个区域的导出目的 GuardDuty 地。
- 不会导出已存档的调查结果，包括隐藏的发现结果的新实例。如果您取消存档某个查找结果，则其状态将更新为 “活动”，并将在下一个间隔内将其导出。
- 如果您在 GuardDuty 管理员帐户中启用查找结果导出，则在当前区域中生成的关联成员帐户的所有发现结果也将导出到您为管理员帐户配置的相同位置。

要配置将活动发现导出到 Amazon S3 存储桶的设置，您需要一个 GuardDuty 可用于加密发现的 KMS 密钥和一个具有允许 GuardDuty 上传对象的权限的 S3 存储桶。查看本主题以了解如何配置发现结果导出和频率。

配置发现结果导出所需的权限

配置导出发现结果的选项时，您可以选择存储发现结果的存储桶和用于数据加密的 KMS 密钥。除了 GuardDuty 操作权限外，您还必须具有以下操作的权限，才能成功配置导出发现结果的选项。

- kms:ListAliases
- s3:CreateBucket
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:PutBucketAcl
- s3:PutBucketPublicAccessBlock
- s3:PutBucketPolicy
- s3:PutObject

> **Important**
>
> 如果你的政策明确拒绝，`putObjectAcl`你将无法发布调查结果。

向 KMS 密钥授予 GuardDuty 权限

GuardDuty 使用对存储桶中的发现数据进行加密Amazon Key Management Service。要成功配置发现结果导出，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。

如果您计划使用新的 KMS 密钥来 GuardDuty 查找结果，请参阅创建密钥。如果您使用来自其他账户的 KMS 密钥，则需要通过登录到拥有Amazon Web Services 账户该密钥的账户来应用密钥策略。配置导出发现结果时，还需要此账户的密钥 ARN。

修改 KMS 密钥策略以允许 GuardDuty 使用此密钥的步骤

1. 在 Amazon KMShttps://console.aws.amazon.com/kms 打开 控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（区域选择器）。
3. 创建新密钥或选择计划用于加密导出的发现结果的现有密钥。密钥必须与存储段位于同一区域，但是，对于要从中导出发现结果的每个区域，您可以使用相同的存储桶和key pair。
4. 选择您的密钥。在 “常规配置” 面板下，复制密钥 ARN。
5. 在 Key policy（密钥策略）部分，选择 Edit（编辑）。

   > **Tip**
   >
   > 如果显示 “切换到策略视图”，请选择该视图以显示密钥策略，然后选择编辑。

6. 将以下密钥策略添加到您的 KMS 密钥，授予对密钥的 GuardDuty 访问权限。此语句仅 GuardDuty 允许使用您更改策略的密钥。编辑密钥策略时，请确保 JSON 语法有效，如果您在最终语句之前添加语句，则必须在右括号后添加逗号。

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

```
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

7. 将## 1 替换为 KMS 密钥的区域。将 444455556666 替换为用于创建 KMS 密钥的Amazon账户 ID。将 KMSKeyId 替换为您选择用于加密的 KMS 密钥的密钥 ID。要识别这些值，请查看此 KMS 密钥的 ARN。

   将 123456789012 替换为Amazon账户的 GuardDuty 账户 ID。将 Region2 替换为 GuardDuty 账户的区域。将 SourceDetectorID 替换为当前区域来源账户的 GuardDuty 检测器 ID。detectorID

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

   Note

   如果您在手动启用的区域 GuardDuty 中使用，请将 “服务” 的值替换为该区域的区域终端节点。例如，如果您 GuardDuty 在中东（巴林）(me-south-1) 中"Service": "guardduty.amazonaws.com"使用"Service": "guardduty.me-south-1.amazonaws.com"。
8. 选择保存。
9. （可选）如果您计划使用现有 KMS 密钥，请将密钥 ARN 复制到记事本以供后续步骤使用。要找到密钥 ARN，请参阅查找密钥 ID 和 ARN。

向存储桶授予 GuardDuty 权限

在您的账户或其他账户中使用预先存在的存储桶时，您必须授予向该存储桶上传对象的 GuardDuty 权限。Amazon您可以通过添加 S3 存储桶策略来授予这些权限。如果您使用的是预先存在的存储桶，请展开以下部分，了解有关添加存储桶策略的 step-by-step 说明。

添加允许上传您的存储桶对象 GuardDuty 的存储桶策略

1. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
2. 选择您计划用于导出的调查结果的存储桶。
3. 选择 Permissions，然后选择 Bucket Policy。
4. 复制示例策略并将其粘贴到存储桶策略编辑器中。
5. 将示例策略中的占位符值替换为适合您环境的值。

   替换myBucketName。将 [####] 替换为导出的发现结果的文件夹位置（如果该位置尚不存在，则GuardDuty 将在设置期间创建）。将##替换为 KMS 密钥所在的区域。将 123456789012 替换 GuardDuty 为设置账户的账号。Amazon将 KMSKeyId 替换为您选择用于加密的密钥的密钥 ID，将 SourceDetectorID 替换为当前区域的源账户的 GuardDuty 检测器 ID。

示例策略

以下示例策略显示如何授予向您的 Amazon S3 存储桶发送调查结果的 GuardDuty 权限。如果在配置调查结果导出后更改路径，则必须修改策略以授予新位置的权限。

```
{
    "Version": "2012-10-17",
```

```
   "Statement": [
       {
           "Sid": "AllowGuardDutygetBucketLocation",
           "Effect": "Allow",
           "Principal": {
               "Service": "guardduty.amazonaws.com"
           },
           "Action": "s3:GetBucketLocation",
           "Resource": "arn:aws:s3:::myBucketName",
           "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "111122223333",
                   "aws:SourceArn":
"arn:aws:guardduty:Region:111122223333:detector/SourceDetectorID"

               }
           }
       },
       {
           "Sid": "AllowGuardDutyPutObject",
           "Effect": "Allow",
           "Principal": {
               "Service": "guardduty.amazonaws.com"
           },
           "Action": "s3:PutObject",
           "Resource": "arn:aws:s3:::myBucketName/[optional prefix]/*",
           "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "111122223333",
                   "aws:SourceArn":
"arn:aws:guardduty:Region:111122223333:detector/SourceDetectorID"

               }
           }
       },
       {
           "Sid": "DenyUnencryptedUploadsThis is optional",
           "Effect": "Deny",
           "Principal": {
               "Service": "guardduty.amazonaws.com"
           },
           "Action": "s3:PutObject",
           "Resource": "arn:aws:s3:::myBucketName/[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": "arn:aws:s3:::myBucketName/[optional prefix]/*",
           "Condition": {
               "StringNotEquals": {
                   "s3:x-amz-server-side-encryption-aws-kms-key-id":
"arn:aws:kms:Region:111122223333:key/KMSKeyId"
               }
           }
       },
       {
           "Sid": "DenyNon-HTTPS",
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Note

如果您在手动启用的区域 GuardDuty 中使用，请将服务的值替换为该区域的区域终端节点。例如，如果您 GuardDuty 在中东（巴林）(me-south-1) 中"Service": "guardduty.amazonaws.com"使用"guardduty.me-south-1.amazonaws.com"。

使用控制台将发现结果导出到存储桶

配置发现结果导出时，您可以选择现有的 S3 存储桶或 GuardDuty创建新的存储桶来存储导出的调查结果。如果您选择使用新的存储桶，则 GuardDuty 将所有必要的权限应用于创建的存储桶。如果您使用现有存储桶必须先更新存储桶策略 GuardDuty 以允许将发现放入存储桶中。

您也可以将发现结果导出到另一个账户中的现有存储桶。

在账户中选择新的或现有的存储桶时，您可以添加前缀。配置发现结果导出时，会在 S3 存储桶中为您的发现 GuardDuty 创建一个新文件夹。前缀将在创建的默认文件夹结构前面加上 GuardDuty，即/AWSLogs/*111122223333*/GuardDuty/*Region*。

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，请确保您已配置 KMS 密钥，如果使用现有存储桶，则添加了 GuardDuty 允许创建对象的存储段策略。

New bucket in your account

要配置调查结果，请使用新存储桶导出

1. 向 KMS 密钥添加用于加密发现结果的策略。 GuardDuty 例如策略，请参见向 KMS 密钥授予 GuardDuty 权限 (p. 197)。
2. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
3. 选择 Settings。
   a. 在“设置”页面的“查找导出选项”部分的 S3 存储桶下，选择“立即配置”。
   b. 选择 Ne w buck et 创建一个新存储段来存储导出的调查结果。

      在 Name the bucket (命名存储桶) 字段中，输入存储桶的名称。此名称在所有 S3 存储桶中必须是唯一的。存储桶名称必须以小写字母或数字开头。
   c. 如果您在存储桶策略[optional prefix]中使用了，则必须在日志文件前缀下输入该前缀，否则这是可选的。当您输入值时，字段下方的示例路径将更新，以反映存储导出的发现结果的存储分区位置的路径。
   d. 在 KMS 加密下，请执行以下操作之一：
      - 选择 Choose key from your account (从您的账户中选择密钥)。

        然后从密钥别名列表中选择您更改策略的密钥别名。

- 选择 Choose key from another account (从其他账户中选择密钥)。

  然后在您更改策略的密钥中输入完整 ARN。

  您选择的密钥必须与存储桶位于同一区域。要了解如何查找密钥 ARN，请参阅查找密钥 ID 和 ARN。

e. 选择保存。

Existing bucket in your account

使用现有存储桶配置发现结果导出

1. 向 KMS 密钥添加策略，该密钥 GuardDuty 将用于加密调查结果。有关政策的示例，请参见向 KMS 密钥授予 GuardDuty 权限 (p. 197)
2. 附上授 GuardDuty 予将对象上载到您的 S3 桶的权限的策略。有关政策的示例，请参见向存储桶授予 GuardDuty 权限 (p. 198)
3. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
4. 选择 Settings。

   a. 在 “设置” 页面的 “查找导出选项” 部分的 S3 存储桶下，选择 “立即配置”。
   b. 在您的账户中选择现有存储桶。

      在存储桶名称字段中输入存储桶的名称。
   c. 可选。在日志文件前缀下，输入要使用的路径前缀。 GuardDuty 将在存储段中创建一个具有指定前缀名称的新文件夹。当您输入值时，该字段下方的示例路径将更新，以反映存储段中导出的查找结果的路径。
   d. 在 KMS 加密下，请执行以下操作之一：
      - 选择 Choose key from your account (从您的账户中选择密钥)。

        然后从密钥别名列表中选择您更改策略的密钥别名。
      - 选择 Choose key from another account (从其他账户中选择密钥)。

        然后在您更改策略的密钥中输入完整 ARN。

        您选择的密钥必须与存储桶位于同一区域。要了解如何查找密钥 ARN，请参阅Amazon Key Management Service开发人员指南中的查找密钥 ID 和 ARN。
   e. 选择保存。

Existing bucket in another account

配置发现结果，请使用其他账户中的现有存储桶导出

1. 向 KMS 密钥添加策略，该密钥 GuardDuty 将用于加密调查结果。有关政策的示例，请参见向 KMS 密钥授予 GuardDuty 权限 (p. 197)
2. 附加一项策略，授 GuardDuty 予将对象上传到另一个账户中的 S3 存储桶的权限。有关策略示例，请参阅 向存储桶授予 GuardDuty 权限 (p. 198)。

   Note

   在策略中使用拥有存储段的账户的账户 ID。
3. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
4. 选择 Settings。

   a. 选择另一个账户中的现有存储桶。

b. 在 Bucket ARN field (存储桶 ARN 字段) 中，输入要使用的来自其他账户的存储桶的 ARN。
c. 在 KMS 加密下，输入您更改策略的密钥的完整 ARN。

   您选择的密钥必须与存储桶位于同一区域。要了解如何查找密钥 ARN，请参阅查找密钥 ID 和 ARN。
d. 选择保存。

导出访问错误

配置查找结果导出选项后，如果无法导出查找结果， GuardDuty 则设置页面上会显示一条错误消息。当 GuardDuty 无法再访问目标资源时，例如删除 S3 存储桶或更改存储桶的权限，就会发生这种情况。当用于加密存储桶中数据的 KMS 密钥变得无法访问时，也会发生这种情况。

导出失败时， GuardDuty 会向与账户关联的电子邮件发送通知，告知您问题。如果您未解决问题，则 GuardDuty 禁用在账户中查找导出内容。您可以随时更新配置以重新启动调查结果导出。

如果您收到此错误，请查看本主题中有关如何启用和配置发现结果导出的信息。例如，查看密钥策略并确认正确的策略应用于您选择进行加密的 KMS 密钥。

设置导出更新的有效发现的频率

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结果。这意味着，在最近一次导出之后更新的任何调查结果都包含在下一次导出的内容中。如果每 6 小时导出更新的发现结果并且在 12:00 导出，则在 12:00 之后更新的任何发现都将在 18:00 导出。

设置频率

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 选择 Settings。
3. 在 “查找结果导出选项” 部分，选择 “频率” 以获取更新的调查结果。这设置了将更新的活动发现导出到 CloudWatch 事件和 Amazon S3 的频率。可从以下选项中进行选择：
   - 每 15 分钟更新 CWE 和 S3
   - 每 1 小时更新 CWE 和 S3
   - 每 6 小时更新 CWE 和 S3 (默认)
4. 选择保存。

使用 Amazon Ev CloudWatch ents 创建对 GuardDuty调查结果的自定义

GuardDuty当发现发生任何变化时，为亚马逊CloudWatch活动创建一个活动。查找将创建 CloudWatch 事件的更改，包括新生成的调查结果或新聚合的调查结果。尽最大努力发出事件。

向每个 GuardDuty 结果分配一个结果 ID。GuardDuty使用唯一的查找结果 ID 为每个查找结果创建 CloudWatch事件。现有调查结果的所有后续实例都会聚合到原始调查结果中。有关更多信息，请参阅GuardDuty查找聚合 (p. 93)：

> 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调查结果揭示的安全问题。

要接收有关基于CloudWatch事件的GuardDuty发现的通知，必须为创建CloudWatch事件规则和目标GuardDuty。此规则CloudWatch允许将GuardDuty生成的发现结果的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 (p. 208)：

主题

- CloudWatch的事件通知频率 GuardDuty (p. 203)
- CloudWatch的事件格式 GuardDuty (p. 203)
- 创建CloudWatch事件规则以通知您GuardDuty发现的情况（ 控制台 ） (p. 204)
- 为 GuardDuty (CLI) 创建CloudWatch事件规则和目标 (p. 208)
- CloudWatchGuardDuty多账户环境的事件 (p. 209)

CloudWatch的事件通知频率 GuardDuty

使用唯一的调查结果 ID 发送新生成的调查结果的通知

GuardDuty在发现后 5 分钟内根据其CloudWatch事件发送通知。此事件 (和此通知) 还包括在生成带唯一 ID 的此结果后前 5 分钟内发生的此结果的所有后续匹配项。

Note

默认情况下，有关新生成的调查结果的通知频率为 5 分钟。无法更新此频率，无法更新频率。

后续发现事件的通知

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 小时间隔内发生的特定查找类型的所有后续事件汇总为一个事件。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发现结果，每隔 6 小时GuardDuty发送一次基于CloudWatch事件的通知。

只有管理员帐户可以自定义发送有关后续结果匹配项的通知的默认频率，只有管理员帐户可以自定义发送通知的默认频率，只有管理员帐户可以自定义发送有关后续匹配项的通知的CloudWatch默认频来自成员账户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将强加于其所有成员帐户的GuardDuty功能。如果来自管理员帐户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，请参阅在亚马逊管理多个账户GuardDuty (p. 224)：

Note

作为管理员，可以自定义有关后续结果匹配项的默认通知频率，可以自定义通知的默认频率，可以自定义通知的默认频率，可以自定义通知的默认频率，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。有关设置这些通知频率的信息，请参阅设置导出更新的有效发现的频率 (p. 202)。

使用CloudWatch事件监控存档的GuardDuty调查结果

对于手动存档的查找结果，这些发现的初次和所有后续事件（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事件（存档完成后生成）不会发送到Events。CloudWatch

CloudWatch的事件格式 GuardDuty

的CloudWatch活动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

详细值将单个查找结果的 JSON 详细信息作为对象返回，而不是返回“发现”值，后者可以支持数组中的多个发现。

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结果 ID。

创建CloudWatch事件规则以通知您GuardDuty发现的情况（控制台）

您可以使用 Ev CloudWatch ents GuardDuty with 来设置自动查找警报，方法是将GuardDuty查找事件发送到消息中心，以帮助提高GuardDuty发现的可见性。本主题向您介绍如何通过设置 SNS 主题，然后将该主题连接到CloudWatch事件规则来向电子邮件、Slack 或 Amazon Chime 发送发现警报。

设置 Amazon SNS 主题和终端节点

首先，您必须先在 Amazon 简单通知服务中设置一个主题并添加一个终端节点。有关更多信息，请参阅 SNS 指南。

此过程可确定要将GuardDuty搜索数据发送到何处。在CloudWatch事件规则创建期间或之后，可以将 SNS 主题添加到事件事件规则中。

Email setup

创建 SNS 主题

1. 通过以下网址登录 Amazon SNS S S S NS S S 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. 在创建主题部分中，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 Create Topic。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 Protocol (协议) 菜单中，选择 Email (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. 通过以下网址登录 Amazon SNS S S S NS S S 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. 在创建主题部分中，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” 以完成操作。

配置Amazon Chatbot客户端

1. 导航到控制Amazon Chatbot台
2. 从 “已配置的客户端” 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，您必须通过选择 “允许” Amazon Chatbot 来确认访问您的频道的权限。
4. 选择 “配置新频道” 以打开配置详细信息窗格。
   a. 输入通道名称。输入通道名称。
   b. 对于 Slack 通道，选择要使用的通道，选择要使用的通道，选择要使用的通道，选择要 要使用私人 Slack 频道Amazon Chatbot，请选择私人频道。
   c. 在 Slack 中，右键单击频道名称并选择 “复制链接”，复制私人频道的频道 ID。
   d. 在Amazon管理控制台的Amazon Chatbot窗口中，将您从 slack 复制的 ID 粘贴到私有频道 ID 字段中。
   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。这是的 IAM 策略模板Amazon Chatbot。它为CloudWatch警报、事件和日志以及 Amazon SNS 主题提供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 Amazon SNS 主题以向 Slack 频道发送通知。
5. 选择 Configure (配置)。

Chime setup

创建 SNS 主题

1. 通过以下网址登录 Amazon SNS S S S NS S S 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. 在创建主题部分中，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” 以完成操作。

配置Amazon Chatbot客户端

1. 导航到控制Amazon Chatbot台
2. 从 “已配置的客户端” 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，输入通道名称，输入通道名称，输入通道名称。
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 Manage webhooks and bots (管理 Webhook 和自动程序)。

b. 选择 “复制 URL” 将 webhook 网址复制到剪贴板。

6. 在Amazon管理控制台的Amazon Chatbot窗口中，将您复制的 URL 粘贴到 Webhook URL 字段中。
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。这是的 IAM 策略模板Amazon Chatbot。它为CloudWatch警报、事件和日志以及 Amazon SNS 主题提供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 Amazon SNS 主题以向 Chime 聊天室发送通知。
10. 选择 Configure (配置)。

为GuardDuty调查结果设置CloudWatch活动

1. 打开 CloudWatch 控制台 (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结果发出提醒。

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。

    - 如果您正在为 Chime 或 Slack 设置通知，请跳至步骤 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，请按照以下步骤使用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。

```
"Amazon <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 Name (名称) 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

以下过程显示如何使用Amazon CLI命令为其创建CloudWatch事件规则和目标GuardDuty。具体而言，该过程向您演示如何创建规则，该规则允许 CloudWatch 为 GuardDuty 生成的所有调查结果发送事件，并将 Amazon Lambda 函数作为规则的目标添加。

> **Note**
>
> 除了 Lambda 函数，GuardDuty并CloudWatch支持以下目标类型：Amazon EC2 实例、Amazon Kinesis 流、Amazon ECS 任务、Amazon Step Functions状态机、命令和内置目标：Amazon ECS 任务、run命令和内置目标：Amazon EC

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，请参阅创建对事件进行触发的事件规则，请参阅创建对CloudWatch事件进行触发的事件规则，请参阅创建对事件进行触发的事件 在 “事件源” 部分，选择 “**GuardDuty**服务名称” 和 **GuardDuty Finding** “事件类型”。

创建规则和目标

1. 要创建允许 CloudWatch 为 GuardDuty 生成的所有调查结果发送事件的规则，请运行以下 CloudWatch CLI 命令。

   ```
   Amazon events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > 您可以进一步自定义您的规则，以便它指示 CloudWatch 仅针对 GuardDuty 生成的一部分调查结果发送事件。此子集基于规则中指定的一个或多个查找属性。例如，使用以下 CLI 命令创建一个规则，该规则使 CloudWatch 能够仅针对严重性为 5 或 8 的 GuardDuty 调查结果发送事件：
   > ```
   > Amazon events put-rule --name Test --event-pattern "{\"source\":
   > [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail
   > \":{\"severity\":[5,8]}}"
   > ```
   > 为此，您可以对 GuardDuty 调查结果使用 JSON 中可用的任何属性值。

2. 要将 Lambda 函数连接为您在步骤 1 中创建规则的目标，请运行以下 CLI 命令，请运行以下 CLI 命令，以下 CLI 命令，以下 CloudWatch CLI 命令，

   ```
   Amazon events put-targets --rule Test --targets Id=1,Arn=arn:aws:lambda:us-
   east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > 确保将<your_function>上述命令中的GuardDuty事件替换为实际的 Lambda 函数。

3. 要添加调用目标所需的权限，请运行以下 Lambda CLI 命令。

   ```
   Amazon lambda add-permission --function-name <your_function> --statement-id
   1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

Note

确保将<your_function>上述命令中的GuardDuty事件替换为实际的 Lambda 函数。

Note

在上述步骤中，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Amazon资源配置为触发CloudWatch事件的目标。有关更多信息，请参阅PutTargets：

CloudWatchGuardDuty多账户环境的事件

作为GuardDuty管理员，您的账户中的CloudWatch活动规则将根据您的成员账户的适用发现触发。这意味着，如果您通过管理员帐户中的CloudWatch事件设置查找通知（如上一节所述），则除了您自己的帐户外，还将收到由您的成员账户生成的高度和中等严重性调查结果的通知。

您可以使用GuardDuty调查结果的 JSON 详细信息`accountId`字段来识别发现结果来源的成员账户。

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，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

此示例将在发现列出的账户 ID 时触发。可以添加多个 ID，按照 JSON 语法用逗号分隔。

了解恶意软件防护扫描期间跳过资源 CloudWatch 的日志和原因

GuardDuty 恶意软件保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。在恶意软件保护扫描期间，可能跳过了某些 Amazon EC2 资源和 Amazon EBS 卷。

GuardDuty 恶意软件保护中的审计 CloudWatch 日志

/aws/guardduty/malware-scan-events CloudWatch 日志组支持三种类型的扫描事件。

恶意软件防护扫描事件名称	说明
EC2_SCAN_STARTED	在 GuardDuty 恶意软件保护启动恶意软件扫描过程（例如准备拍摄 EBS 卷的快照）时创建。

恶意软件防护扫描事件名称	说明
EC2_SCAN_COMPLETED	在对受影响资源的至少一个 EBS 卷完成 GuardDuty 恶意软件保护扫描时创建。此事件还包括snapshotId属于已扫描的 EBS 卷的。扫描完成后，扫描结果将为Clean或Infected。
EC2_SCAN_SKIPPED	在 GuardDuty 恶意软件保护扫描跳过受影响资源的所有 EBS 卷时创建。要确定跳过原因，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，请参见恶意软件扫描期间跳过资源的原因 (p. 210)下文。

Note

如果您使用的是Amazon Organizations，则来自Organizations 中成员账户 CloudWatch 的日志事件将同时发布到管理员和成员账户的日志组。

Console

1. 登录 https://console.aws.amazon.com/cloudwatch/ 控制台。
2. 在 Logep s（目标组）。选择 /aws/guardduty/malware-scan-events 日志组查看 GuardDuty 恶意软件防护的扫描事件。

   要运行查询，请选择 Log Insights。

   有关如何运行查询的信息，请参阅亚马逊 CloudWatch 用户指南中的使用 Logs Insights 分析 CloudWatch 日志数据。
3. 选择 Scan ID 可监控受影响资源和恶意软件发现的详细信息。例如，您可以运行以下查询来使用筛选 CloudWatch 日志事件scanId。确保使用您自己的有效*## ID*。

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API

- 要使用日志组，请参阅亚马逊 CloudWatch 用户指南Amazon CLI中的使用搜索日志条目。

  选择 /aws/guardduty/malware-scan-events 日志组查看 GuardDuty 恶意软件防护的扫描事件。
- 要查看和筛选日志事件，请分别参阅 GetLogEventsAmazon CloudWatch API 参考中的和。FilterLogEvents

GuardDuty 恶意软件防护日志保留

/aws/guardduty/malware-scan-events 日志组的默认日志保留期为 90 天，之后将自动删除日志事件。要更改您的日志组的日 CloudWatch 志保留策略，请参阅更改日志中的 CloudWatch 日志数据保留期或PutRetentionPolicy。

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，某些 EC2 资源和 EBS 卷可能在扫描过程中被跳过。下表列出了 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 GuardDuty 恶意软件保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进展情况，因此不可采取行动。

不原因	说明	拟议的步骤	
RESOURCE_NOT_FOUND	在resourceArn您的Amazon环境中找不到用于启动按需恶意软件扫描的。	验证您resourceArn的Amazon EC2 实例或容器工作负载，然后重试。	
ACCOUNT_INELIGIBLE	您尝试启动按需恶意软件扫描的Amazon账户 ID 尚未启用 GuardDuty。	验证此Amazon账户 GuardDuty 是否已启用。 启用新Amazon Web Services 区域版本时 GuardDuty ，最多可能需要 20 分钟才能同步。	
UNSUPPORTED_KEY_ENCRYPTION	GuardDuty 恶意软件保护支持未加密和使用客户管理的密钥加密的卷。它不支持扫描使用 Amazon EBS 加密加密的 EBS 卷。	用客户托管式密钥代 有关 GuardDuty 支持的加密类型的更多信息，请参阅恶意软件防护中支持的容量 (p. 49)。	
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：要么标签已添加到包含列表但资源与该标签无关；标签已添加到排除列表并且资源与此标签相关联；要true么将此资源的GuardDutyExcluded标签设置为。	更新您的扫描选项或与 Amazon EC2 资源关联的标签。有关更多信息，请参阅带有用户定义标签的扫描选项 (p. 52)：	
UNSUPPORTED_VOLUME_SIZE	该容量大于 1024 GB。	不可操作。	
NO_VOLUMES_ATTACHED	GuardDuty 恶意软件保护在您的账户中找到了该实例，但未将 EBS 卷连接到该实例，无法继续扫描。	不可操作。	
UNABLE_TO_SCAN	这是不原因。	不可操作。	
SNAPSHOT_NOT_FOUND	找不到从 EBS 卷创建并与服务帐户共享的快照， GuardDuty 恶意软件保护无法继续扫描。	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，还可以防止创建新的快照。	您可以删除旧快照或请求增加配额。您可以在《Amazon一般参考指南》的服务配额下查看每个区域的快照默认限	

不原因	说明	拟议的步骤	
		制以及如何申请增加配额。	
MAX_NUMBER_OF_ATTACHED_EC2_INSTANCES_REACHED	有 EC2 实例上附加的 EC2 实例。 GuardDuty 恶意软件保护扫描了前 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productCode例marketplace。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的付原因。 有关信息productCode，请参阅ProductCode《Amazon EC2 API 参考手册》。	不可操作。	

报告 GuardDuty 恶意软件保护中的误报

GuardDuty 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。为了改善您使用恶意软件保护和 GuardDuty 服务的体验，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. 当您发现似乎是误报结果时，请联系Amazon Web Services Support以启动误报文件提交流程。
3. 选择 “恶意软件扫描”。
4. 选择扫描件以查看其 “查找ID”。
5. 提供调查结果 ID。您还必须提供文件的 SHA-256 哈希值。这是确保 GuardDuty 恶意软件保护收到正确的文件所必需的。
6. 该Amazon Web Services Support团队将为您提供Amazon Simple Storage Service (S3) URL，您可以使用该网址上传文件和 SHA-256 哈希。成功上传文件后通知Amazon Web Services Support团队。

   Warning

   请勿直接向其提供文件或 SHA-256 哈希值Amazon Web Services Support。您只应通过提供的 URL 将文件和哈希上传到 Amazon S3。如果您在收到 URL 后的七天内未能上传文件和哈希，它将失效。如果该网址失效，您必须联系Amazon Web Services Support以接收新的网址。

   GuardDuty 不超过 30 天未解决。 GuardDuty 团队成员将分析您提交的内容，并采取适当措施改善您在恶意软件防护和 GuardDuty服务方面的体验。

修复由发现的安全问题 GuardDuty

亚马逊GuardDuty得出的调查结果 (p. 78)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 EC2 实例或容器工作负载受损，或者您的Amazon环境中有一组证书被泄露。以下部分介绍了这些方案的建议补救步骤。如果有其他补救方案，则将在该特定发现类型的条目中对其进行描述。您可以通过从“活动查找结果类型” 表中选择查找结果类型来访问有关该查找结果类型的 (p. 94)完整信息。

主题

- 修复受感染的 EC2 实例 (p. 213)
- 修复受感染的 S3 存储桶 (p. 213)
- 修复受感染的 ECS 集群 (p. 215)
- 修复被盗的凭证 Amazon (p. 215)
- 修复受感染的独立容器 (p. 216)
- 修复由发现的 EKS 审核日志监控结果 GuardDuty (p. 216)
- 修复 EKS 运行时监控结果 (p. 220)
- 修复受损的数据库 (p. 221)
- 修复受损的 Lambda 函数 (p. 223)

修复受感染的 EC2 实例

按照以下推荐步骤修复Amazon环境中受感染的 EC2 实例：

1. 隔离受影响的 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。您可以查看，Amazon Web Services Marketplace看看是否有有帮助的合作伙伴产品可以识别和删除恶意软件。
2. 如果您无法识别和阻止 EC2 实例上未经授权的活动，我们建议您终止遭盗用的 EC2，然后根据需要使用新实例来替换它。以下是可以保护您 EC2 实例的其他资源：
   - Amazon EC2 最佳实践中的安全与网络部分
   - 适用@@ 于 Linux 实例的Amazon EC2 安全组和适用于 Windows 实例的Amazon EC2 安全组
   - Amazon EC2 中的安全
   - 保护 EC2 实例的技巧 (Linux)。
   - Amazon安全最佳实践
   - 基础架构域事件开启 Amazon
3. 在Amazon开发者论坛上浏览更多帮助：https://forums.aws.amazon.com/index.jspa
4. 如果您是高级支持包订阅者，则可以提交技术支持请求。

修复受感染的 S3 存储桶

按照以下推荐步骤修复Amazon环境中受感染的 Amazon S3 存储桶：

1. 识别受影响的 S3 资源。

S3 的GuardDuty搜索结果将在搜索结果详细信息中列出 S3 存储桶、该存储段的 Amazon 资源名称 (ARN) 和存储桶所有者。

2. 确定可疑活动的来源和使用的 API 调用。

   使用的 API 调用将在调查结果详细信息中作为 `API` 列出。来源将是 IAM 委托人（IAM 角色、用户或账户），识别细节将在调查结果中列出。根据来源类型，将提供远程 IP 地址或源域信息，并可以帮助您评估来源是否已获得授权。如果调查结果涉及来自 EC2 实例的证书，则该资源的详细信息也将包括在内。

3. 确定呼叫来源是否有权访问已识别的资源。

   例如，请考虑以下事项：

   - 如果 IAM 用户参与其中，他们的证书是否可能已被泄露？ 请参阅以下有关修复被盗Amazon凭证的部分。
   - 如果 API 是从以前没有调用此类API历史的主体调用的，则此源是否需要访问权限才能进行此操作？ 存储桶权限可以进一步限制吗？
   - 如果从用户名中看到访问权限**`ANONYMOUS_PRINCIPAL`**，则表示**`AWSAccount`**该存储桶是公共的，并且已被访问。这个桶应该公开吗？ 如果不是，请查看以下安全建议，了解共享 S3 资源的替代解决方案。
   - 如果从用户名中看到访问成功，则用户类型**`PreflightRequest`**为`ANONYMOUS_PRINCIPAL`，则表示`AWSAccount`该存储桶设置了跨源资源共享 (CORS) 策略。这个存储桶应该有 CORS 策略吗？ 否则，请确保存储桶不会在无意中被公开，并查看以下安全建议，以获取共享 S3 资源的替代解决方案。有关 CORS 的更多信息，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，如个人身份信息（PII）、财务数据或凭证。如果您的 Macie 账户启用了自动敏感数据发现功能，请查看 S3 存储桶的详细信息，以便更好地了解您的 S3 存储桶的内容。如果您的 Macie 帐户禁用了此功能，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任务，检查 S3 存储桶的对象中是否有敏感数据。有关更多信息，请参阅使用 Macie 发现敏感数据。

如果访问权限已获授权，您可以忽略该发现。https://console.aws.amazon.com/guardduty/ 控制台允许你设置规则来完全隐藏单个发现，这样它们就不会再出现。有关更多信息，请参阅抑制规则 (p. 187)：

如果您确定您的 S3 数据已被未经授权的一方泄露或访问，请查看以下 S3 安全建议，以加强权限和限制访问。适当的补救解决方案将取决于您特定环境的需求。

以下是基于特定 S3 访问需求的一些建议：

- 要以集中方式限制公众对您的 S3 数据的访问，请使用 S3 阻止公共访问。可以通过四种不同的设置为接入点、存储分区和Amazon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 阻止公有访问设置。
- Amazon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Virtual Private Cloud (VPC) 终端节点来限制访问特定 VPC 终端节点。有关更多信息，请参阅 Amazon S3 的 VPC 终端节点的示例存储桶策略。
- 要暂时允许账户外部的可信实体访问您的 S3 对象，您可以通过 S3 创建预签名 URL。此访问权限是使用您的账户凭证创建的，可能持续 6 小时到 7 天，具体取决于所使用的证书。有关更多信息，请参阅使用 S3 生成预签名 URL。
- 对于需要在不同来源之间共享 S3 对象的用例，您可以使用 S3 接入点创建权限集，将访问权限集限制为仅限私有网络中的用户。有关更多信息，请参阅 Amazon S3 接入点管理数据访问。
- 要安全地向其他Amazon账户授予对 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 ACL 管理 S3 访问权限。

有关 S3 安全选项的完整概述，请参阅 S3 安全最佳实践。

修复受感染的 ECS 集群

请按照以下推荐步骤修复Amazon环境中受感染的 ECS 集群：

1. 识别受影响的 ECS 集群。

   ECS 的GuardDuty恶意软件保护调查结果在发现的详细信息面板中提供了 ECS 群集的详细信息。
2. 评估恶意软件的来源

   评估检测到的恶意软件是否在容器的映像中。如果图像中有恶意软件，请识别使用此映像正在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通过切断与任务的所有连接来帮助阻止已经在进行的攻击。

如果访问权限已获授权，您可以忽略该发现。https://console.aws.amazon.com/guardduty/ 控制台允许你设置规则来完全隐藏单个发现，这样它们就不会再出现。有关更多信息，请参阅抑制规则 (p. 187)：

修复被盗的凭证 Amazon

请按照以下推荐步骤修复Amazon环境中被盗的证书：

1. 确定受影响的 IAM 实体和使用的 API 调用。

   使用的 API 调用将在调查结果详细信息中作为 API 列出。IAM 实体（IAM 角色或用户）及其识别信息将在调查结果详情的资源部分列出。所涉及的 IAM 实体的类型可由 User Type (用户类型) 字段确定，IAM 实体的名称将位于 User name (用户名) 字段中。调查结果中涉及的 IAM 实体的类型也可以由使用的 Access key ID (访问密钥 ID) 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证书。Amazon Web Services 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 Amazon 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Amazon管理控制台中查看或管理。IAM 角色将始终使用Amazon STS证书，但也可以为 IAM 用户生成证书，有关更多信息，Amazon STS请参阅 IAM：临时安全证书。

   如果使用了角色，则用户名字段将指示所用角色的名称。您可以Amazon CloudTrail通过检查 CloudTrail日志条目的sessionIssuer元素来确定密钥是如何请求的，有关更多信息，请参阅 IAM 和中的Amazon STS信息CloudTrail。
2. 查看 IAM 实体的权限。

   打开 IAM 控制台，根据使用的实体类型选择 Users (用户) 或 Roles (角色) 选项卡，然后通过在搜索字段中键入已识别的名称来查找受影响的实体。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. 确定是否合法使用了 IAM 实体凭证。

   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 API 操作

- 从 GuardDuty 调查结果中列出的 IP 地址调用了 API 操作

如果此活动是Amazon凭证的合法用途，则可以忽略GuardDuty调查结果。https://console.aws.amazon.com/guardduty/ 控制台允许你设置规则来完全隐藏单个发现，这样它们就不会再出现。有关更多信息，请参阅抑制规则 (p. 187)：

如果您无法确认此活动是否为合法用途，则可能是特定访问密钥、IAM 用户的登录凭证泄露或整个Amazon Web Services 账户泄露的结果。如果您怀疑自己的凭证已被泄露，请查看 “我的Amazon Web Services 账户可能被泄露” 一文中的信息以修复此问题。

修复受感染的独立容器

1. 隔离容器

   要识别恶意容器工作负载，请执行以下步骤：
   - 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
   - 在 “调查结果” 页面上，选择相应的查找结果以打开调查结果面板。
   - 在查找结果面板的受影响资源部分下，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。有关如何冻结容器的信息，请参阅暂停容器。

   停下容器

   如果上述步骤失败并且容器没有暂停，请停止容器运行。如果您已启用该快照保留 (p. 51)功能，则GuardDuty将保留包含恶意软件的 EBS 卷的快照。

   有关如何停止容器的信息，请参阅停止容器。
3. 评估恶意软件的存在

   评估容器的映像中是否有恶意软件。

如果访问权限已获授权，您可以忽略该发现。https://console.aws.amazon.com/guardduty/ 控制台允许你设置规则来完全隐藏单个发现，这样它们就不会再出现。GuardDuty控制台允许您设置规则以完全隐藏单个发现结果，使其不再出现。有关更多信息，请参阅 抑制规则 (p. 187)。

修复由发现的 EKS 审核日志监控结果 GuardDuty

为您的账户启用 EKS 审核日志监控后，亚马逊GuardDuty会生成调查结果 (p. 78)，表明存在潜在的 Kubernetes 安全问题。有关更多信息，请参阅EKS 审核日志监控 (p. 16)：以下部分介绍了针对这些情形的建议补救步骤。该特定查找结果类型的条目中描述了具体的补救措施。您可以通过从 “活动查找结果类型” 表中选择查找结果类型来访问有关该查找结果类型的 (p. 94)完整信息。

如果任何 EKS Audit Log Monitoring 查找类型是预期生成的，则可以考虑添加抑制规则 (p. 187)以防止future出现警报。

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集群GuardDuty发现的根本原因，并概述适当的补救指南。以下是导致 GuardDuty Kubernetes 发现的主要根本原因：

- 配置问题 (p. 217)

- 泄露用户所属 (p. 217)
- 泄露用户组 (p. 219)
- 泄露节点 (p. 220)
- 泄露的容器映像 (p. 219)

Note

在 Kubernetes 版本 1.14 之前，该`system:unauthenticated`组与默认关联且处于关联状态。`system:discovery` `system:basic-user` ClusterRoles这可能允许匿名用户进行意外访问。集群更新不会撤消这些权限，这意味着即使您已将集群更新到版本 1.14 或更高版本，这些权限可能仍然有效。我们建议您取消这些权限与`system:unauthenticated`群组的关联。有关删除这些权限的说明，请参阅查看和撤消不必要的匿名访问权限。

配置问题

如果调查结果表明存在配置问题，请参阅该调查结果的补救部分，以获取有关解决该特定问题的指南。有关更多信息，请参阅以下表明配置问题的查找类型：

- Policy:Kubernetes/AnonymousAccessGranted (p. 146)
- Policy:Kubernetes/ExposedDashboard (p. 146)
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount (p. 145)
- Policy:Kubernetes/KubeflowDashboardExposed (p. 146)
- 任何以此结尾的发现SuccessfulAnonymousAccess。

修复受感染的 Kubernetes 用户

当GuardDuty发现中确定的用户执行了意外的 API 操作时，该发现可能表明 Kubernetes 用户遭到入侵。您可以在控制台中查找详细信息的 Kubernetes 用户详细信息部分或发现 JSON `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` 中识别用户。列`user name`出用户所`uid`属的 Kubernetes 组。

如果用户使用 IAM 实体访问工作负载，则可以使用该`Access Key details`部分来确定 IAM 角色或用户的详细信息。请参阅以下用户类型及其补救指南。

Note

您可以使用 Amazon Detective 进一步调查调查结果中确定的 IAM 角色或用户。在GuardDuty控制台中查看发现细节时，选择 “在Detective 中调查”。然后从列出的项目中选择Amazon用户或角色以在 Detective 中进行调查。

内@@ 置 Kubernetes 管理员 — 亚马逊 EKS 为创建集群的 IAM 身份分配的默认用户。此用户类型由用户名标识`kubernetes-admin`。

要撤消内置 Kubernetes 管理员的访问权限，请执行以下操作：

- `userType`从该`Access Key details`部分中找出。
  - 如果`userType`是角色并且该角色属于 EC2 实例角色：
    - 识别该实例，然后按照中的说明进行操作修复受感染的 EC2 实例 (p. 213)。
  - 如果`userType`是用户，或者是用户担任的角色：
    1. 轮换该用户的访问密钥。
    2. 轮换用户有权访问的所有机密。
    3. 查看 “我的Amazon帐户可能被泄露” 中的信息，以了解更多详细信息。

OIDC 认证用户 — 通过 OIDC 提供商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检查您的集群是否使用 OIDC：`aws eks list-identity-provider-configs --cluster-name your-cluster-name`

要撤消已通过 OIDC 身份验证的用户的访问权限，请执行以下操作：

1. 轮换 OIDC 提供商中该用户的证书。
2. 轮换用户有权访问的所有机密。

Amazon-Auth ConfigMap 定义的用户 — 通过-auth 获得访问权限的 IAM 用户。Amazon ConfigMap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他们的权限：`kubectl edit configmaps aws-auth --namespace kube-system`

要撤消AmazonConfigMap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. 识别 map roles 或 m apUsers 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，其中已在调查结果中识别出管理员用户。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-standard-
wo-NodeInstanceRole-1WP3NUE3O6UCF
      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. 将该用户从中删除ConfigMap。参见以下示例，其中管理员用户已被删除。

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-standard-
wo-NodeInstanceRole-1WP3NUE3O6UCF
      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，或者是用户担任的角色：
   a. 轮换该用户的访问密钥。
   b. 轮换用户有权访问的所有机密。

c. 查看 “我的Amazon帐户可能被泄露” 中的信息，以了解更多详细信息。

如果调查结果没有`resource.accessKeyDetails`章节，则该用户是 Kubernetes 服务帐户。

服务帐户 —服务帐户为容器提供身份，可以通过以下格式的用户名进行识别:`system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

要撤消对服务帐号的访问权限，请执行以下操作：

1. 轮换服务帐号凭证。
2. 查看下一节中的 pod 入侵指南。

修复受感染的 Kubernetes 容器

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会受到损害。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。有关如何识别一个或多个已被入侵的 pod 的指导，请参阅以下入侵场景。

单舱折衷方案

如果该`resource.kubernetesDetails.kubernetesWorkloadDetails`部分内的`type`字段是 pod，则该发现可识别出单个 pod。名称字段是容器`name`的，`namespace`字段是其命名空间。使用识别违规容器和工作节点中的说明来识别运行容器的工作节点。

Pod 通过工作负载资源遭到入侵

如果该`resource.kubernetesDetails.kubernetesWorkloadDetails`部分中的`type`字段标识了工作负载资源，例如 `aDeployment`，则该工作负载资源中的所有 Pod 都可能已遭到破坏。按照使用工作负载名称识别违规容器和工作节点中的说明来识别工作负载资源的所有 Pod 及其正在运行的节点。

Pods 通过服务账户遭到入侵

如果GuardDuty发现了该`resource.kubernetesDetails.kubernetesUserDetails`部分中的服务帐号，则使用已识别服务帐号的 pod 很可能遭到入侵。如果调查结果报告的用户名具有以下格式，则为服务帐户:`system:serviceaccount:`*`namespace`*`:`*`service_account_name`*. 按照使用服务帐号名称识别违规容器和工作节点中的说明，使用服务帐号识别所有 Pod 及其正在运行的节点。

确定所有受感染的 Pod 及其正在运行的节点后，按照 EKS 最佳实践指南中的以下说明隔离 pod、轮换其凭证并收集数据以进行取证分析。

要修复受感染的 pod，请执行以下操作：

1. 找出危害 pod 的漏洞。
2. 修复该漏洞并启动新的替换 pod。
3. 删除有漏洞的 Pod。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 获得其他Amazon资源访问权限的 IAM 角色，请从实例中移除这些角色以防止攻击造成进一步损害。同样，如果已为 Pod 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安全地从角色中删除 IAM 策略。

修复泄露的容器映像

当GuardDuty发现表明 pod 遭到入侵时，用于启动 pod 的图像可能是恶意的或已泄露的。GuardDuty发现可识别`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image`字段内的容器图像。您可以通过扫描图像中的恶意软件来确定图像是否为恶意图像。

要修复受损的容器映像，请执行以下操作：

1. 立即停止使用该图像并将其从您的映像存储库中删除。
2. 使用图像识别所有容器。有关更多信息，请参阅识别具有易受攻击或受损容器映像和工作节点的 pod。
3. 隔离受感染的 pod，轮换凭证并收集数据进行分析。有关更多信息，请参阅 EKS 最佳实践指南中的以下说明。
4. 使用受感染的图像删除所有容器。

修复受感染的 Kubernetes 节点

如果GuardDuty发现中识别的用户代表节点标识，或者发现结果表明使用了特权容器，则该发现可能表明节点已遭到入侵。

如果用户名字段具有以下格式，则用户身份是工作节点:`system:node:node name`. 例如，`system:node:ip-192-168-3-201.ec2.internal`。这表明对手已获得该节点的访问权限，并且正在使用该节点的证书与 Kubernetes API 端点通信。

如果查找结果中列出的一个或多个容器的查找结果字段设置为，则该`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.privileg`找结果表示正在使用特权容器`True`。

要修复受感染的节点，请执行以下操作：

1. 使用 EKS 最佳实践指南中的说明隔离 pod、轮换其凭证并收集数据以进行取证分析。
2. 确定节点上运行的所有 Pod 使用的服务帐户。查看他们的权限，并在需要时轮换服务帐户。
3. 终止节点。

修复 EKS 运行时监控结果

当您为账户启用 EKS 运行时监控时，亚马逊 GuardDuty 可能会生成EKS 运行时监控查找类型 (p. 111)表明您的Amazon环境中存在潜在安全问题的信息。因为EKS 运行时监控 (p. 21)，潜在的安全问题表明您的Amazon环境中存在受损的 EC2 实例、容器工作负载、EKS 集群或一组证书被泄露。安全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控制台中生成的查找结果详细信息中查看资源类型。以下小节介绍每种资源的推荐的修复步骤。有关替代或其他补救建议，请参阅Kubernetes 审计日志查找类型 (p. 136)。

Instance

如果查找结果详细信息中的资源类型为实例，则表示 EC2 实例或 EKS 节点可能遭到入侵。

- 要修复受损的 EKS 节点，请参阅修复受感染的 Kubernetes 节点 (p. 220)。
- 要修复受损的 EC2 实例，请参阅修复受感染的 EC2 实例 (p. 213)。

EKSCluster

如果查找结果详细信息中的资源类型为 eksClust er，则表示 EKS 集群内的容器或容器可能受到威胁。

- 要修复受损的 pod，请参阅修复受感染的 Kubernetes 容器 (p. 219)。
- 要修复受损的容器镜像，请参阅修复泄露的容器映像 (p. 219)。

Container

如果查找结果详细信息中的资源类型为 Container，则表明独立容器可能遭到破坏。

- 要进行修复，请参见修复受感染的独立容器 (p. 216)。
- 如果发现结果是使用同一个容器镜像跨多个容器生成的，请参阅修复泄露的容器映像 (p. 219)。
- 如果容器访问了底层 EC2 主机，则其关联的实例证书可能已被泄露。有关更多信息，请参阅修复被盗的凭证 Amazon (p. 215)：
- 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 Inst ance 选项卡下的建议补救措施。

修复受损的数据库

GuardDuty 生成的结果RDS 保护查找类型 (p. 153)表明在您启用支持的数据库 (p. 68)后您的登录行为可能存在可疑和异常GuardDutyRDS 防护 (p. 68)。使用 RDS 登录活动，通过识别登录尝试中的异常模式来 GuardDuty 分析和分析威胁。

Note

您可以通过从中选择查找结果类型来访问该查找结果的完整信息调查结果表 (p. 174)。

按照这些建议的步骤修复Amazon环境中可能受损的 Amazon Aurora 数据库。

主题

- 使用成功的登录事件修复可能受损的数据库 (p. 221)
- 修复带有失败登录事件的潜在受损数据库 (p. 222)
- 修复可能受损的凭证 (p. 222)
- 限制网络访问 (p. 223)

使用成功的登录事件修复可能受损的数据库

以下推荐步骤可以帮助您修复可能被入侵的 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 调查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，请参阅正在寻找细节 (p. 78)：
2. 确认此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 的潜在情况：
   - 在很长一段时间之后登录数据库的用户。
   - 偶尔登录数据库的用户，例如，每个季度登录的财务分析师。
   - 参与成功登录尝试的潜在可疑行为者可能会破坏数据库。
3. 如果行为出乎意料，请开始此步骤。

   1. 限制数据库访问权限

      限制可疑账户的数据库访问权限以及此登录活动的来源。有关更多信息，请参阅 修复可能受损的凭证 (p. 222) 和 限制网络访问 (p. 223)。
   2. 评估影响并确定访问了哪些信息。
      - 查看审核日志（如果有）以确定可能已访问的信息。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的信息。

修复带有失败登录事件的潜在受损数据库

以下推荐的步骤可以帮助您修复可能被入侵的 Aurora 数据库，该数据库表现出与登录失败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 调查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，请参阅正在寻找细节 (p. 78)：

2. 确定登录尝试失败的来源。

   生成的 GuardDuty 查找结果在查找结果面板的 Acto r 部分下提供 IP 地址和 ASN 组织（如果是公共连接）。

   自治系统 (AS) 是一组由一个或多个 IP 前缀（网络上可访问的 IP 地址列表）组成，由一个或多个网络运营商运行，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) 来控制其网络内的路由，并与其他互联网服务提供商 (ISP) 交换路由信息。

3. 确认此行为是意外的。

   检查此活动是否代表企图获得更多未经授权的数据库访问权限，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反复尝试连接。
   - 如果这是外部行为者，请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. 限制数据库访问权限

      限制可疑账户的数据库访问权限以及此登录活动的来源。有关更多信息，请参阅 修复可能受损的凭证 (p. 222) 和 限制网络访问 (p. 223)。

   2. 进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创建不安全状态时收到通知。有关更多信息，请参阅Amazon Network Firewall开发者指南Amazon Network Firewall中的防火墙策略。

修复可能受损的凭证

GuardDuty 发现结果可能表明，当发现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。您可以在控制台的查找结果面板的 RDS 数据库用户详细信息部分中识别用户，也可以在发现 JSON 中识别用户。`resource.rdsDbUserDetails`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。

- 要撤消参与调查的特定用户的访问权限或轮换密码，请参阅《亚马逊 Aurora 用户指南》中的 Amazon Aurora MySQ L 安全性或 Amazon Aurora PostgreSQL 的安全性。
- Amazon Secrets Manager用于安全存储箱和自动轮换 Amazon Relational Database Service（RDS）数据库的密钥。有关更多信息，请参阅Amazon Secrets Manager用户指南中的Amazon Secrets Manager教程。
- 使用 IAM 数据库身份验证无需密码即可管理数据库用户的访问权限。有关更多信息，请参阅 A mazon 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 RDDS 用户指南中的亚马逊Relational DS 用户指南中的亚马逊Relational DS 用户指南。

限制网络访问

GuardDuty 调查结果可能表明，除了您的应用程序或Virtual Private Cloud (VPC) 之外，还可以访问数据库。如果调查结果中的远程 IP 地址是意外的连接来源，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/ 控制台的安全组下找到，也可以在调查结果 JSON 中`resource.rdsDbInstanceDetails.dbSecurityGroups`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。

如果您使用防火墙，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Amazon Network Firewall开发者指南Amazon Network Firewall中的防火墙。

修复受损的 Lambda 函数

当 GuardDuty 生成 Lambda Protection 调查结果且该活动出乎意料时，您的 Lambda 函数可能会受到攻击。我们建议完成以下步骤来修复受损的 Lambda 函数。

修复 Lambda 保护发现的结果

1. 确定受影响的 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. 确定可疑活动的来源。

   a. 查看与调查结果中涉及的 Lambda 函数版本相关的代码。
   b. 查看调查结果所涉及的 Lambda 函数版本的导入库和层。
   c. 如果您已使用 Amazon Inspector 启用了扫描Amazon Lambda功能，请查看与调查结果所涉及的 Lambda 函数相关的Amazon Inspec tor 调查结果。
   d. 查看Amazon CloudTrail日志以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. 修复受影响的 Lambda 函数。

   a. 禁用调查结果中涉及的 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，以移除潜在的可疑库和层。
   c. 缓解与调查结果中涉及的 Lambda 函数相关的Amazon Inspector tor 调查结果。

在亚马逊管理多个账户 GuardDuty

要在亚马逊管理多个账户 GuardDuty，您必须选择一个Amazon账户作为管理员账户 GuardDuty。然后，您可以将其他Amazon账户与管理员账户关联为成员账户。有两种方法可以将帐户与 GuardDuty 管理员帐户关联：通过两个帐户均为成员的Amazon Organizations组织，或者通过发送邀请 GuardDuty。

GuardDuty 建议使用该Amazon Organizations方法。有关设置组织的更多信息，请参阅Amazon Organizations用户指南中的创建组织。

通过以下方式管理多个账户Amazon Organizations

如果您要指定为 GuardDuty 管理员帐户的帐户是其中的组织的一部分Amazon Organizations，则可以将该帐户指定为该组织的委托管理员 GuardDuty。注册为委托管理员的账户自动成为 GuardDuty 管理员账户。

将组织中的任何帐户添加 GuardDuty 为成员帐户时，您可以使用该管理员帐户启用和管理该帐户。

如果您已经拥有 GuardDuty 管理员帐户和通过邀请关联的成员帐户，则可以将该帐户注册为组织的 GuardDuty 委托管理员。当您执行此操作时，所有当前关联的成员账户仍保留为成员，这样您就可以充分利用所添加的通过 Amazon Organizations 管理 GuardDuty 账户的功能。

有关 GuardDuty 通过组织支持多个账户的更多信息，请参阅使用以下GuardDuty方式管理账户 Amazon Organizations (p. 225)。

通过邀请管理多个账户

如果您要关联的帐户不属于您的Amazon Organizations组织，则可以在中指定管理员帐户， GuardDuty 然后使用管理员帐户邀请其他Amazon帐户成为成员帐户。当受邀账户接受邀请时，该账户将成为与管理员账户关联的 GuardDuty 成员账户。

有关通过邀请支持多个账户的更多信息， GuardDuty 请参阅通过的成员 GuardDuty 账户 (p. 231)。

了解 GuardDuty 管理员账户和成员账户之间的关系

当您在多账户环境 GuardDuty 中使用时，管理员帐户可以代表成员账户管理某些方面。 GuardDuty 管理员帐户可以执行的主要功能如下：

- 添加和删除关联的成员账户。执行此操作的过程取决于账户是通过组织关联的还是通过邀请关联的。
- 管理关联成员账户 GuardDuty 内的状态，包括启用和暂停 GuardDuty。

  Note

  使用Amazon Organizations自动启用 GuardDuty 管理的委托管理员帐户添加为成员的帐户。
- 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 网络内的发现结果。成员账户在多账户环境中会失去对这些功能的访问权限。

下表详细说明了 GuardDuty 管理员帐户和成员帐户之间的关系。

对于指定为自身的账户，只能在自己的账户中执行列出的操作。指定任意表示账户可以为任何关联账户执行所述的操作；而指定所有表示操作在由指定账户执行时，将会应用于所有关联账户。带有短划线 (—) 的表格单元格表示该名称的账户无法执行列出的操作。

Action	Designation		
	管理员（组织）	管理员（通过邀请）	成员
查看所有Amazon Organizations成员账户，无论 GuardDuty 状态如何	任何	—	—
自动为新账户启用 S3 保护	全部		
为新账户自动启用 EKS 保护	全部		
自动为新账户启用恶意软件防护	全部		
启用 GuardDuty	任何	自身	—
查看 GuardDuty 结果	任何	任何	自身
归档发现结果	任何	任何	—
应用禁止规则	全部	全部	—
生成示例发现结果	自身	自身	自身
创建可信或威胁 IP 列表	全部	全部	—
更新可信或威胁 IP 列表	全部	全部	—
删除可信或威胁 IP 列表	全部	全部	—
设置 EventBridge 通知频率	全部	全部	自身
为 Amazon S3 位置	全部	全部	自身
暂停 GuardDuty	任何*	任何*	—

* 表示必须先对所有关联账户执行该操作，然后才能在指定账户中执行。

使用以下GuardDuty方式管理账户 Amazon Organizations

当您将 GuardDuty 与 Amazon Organizations 组织一起使用时，您可以委派组织内的任意账户作为 GuardDuty 委派管理员。只有组织管理账户可以指定GuardDuty委派管理员。

被指定为委派管理员的账户将成为GuardDuty管理员帐户，在指定区域中GuardDuty自动启用，并被授予启用和管理GuardDuty该区域内组织中所有账户的权限。可以查看组织中的其他帐户，并将其添加为与委托管理员帐户关联的GuardDuty成员帐户。

如果您已经通过邀请设置了具有关联成员帐户的GuardDuty管理员，并且这些成员帐户属于同一个组织，则在您为组织设置GuardDuty委派管理员时，其类型将从 “受邀者” 更改为 “通过组织”。如果新的委派管理员之前通过邀请添加了不属于同一组织的成员，则他们的类型为通过邀请。在这两种情况下，先前添加的这些账户都是组织GuardDuty委派管理员的成员账户。

您可以继续将账户添加为成员，即使账户位于组织之外也是如此。要了解更多信息，请参阅通过邀请指定管理员和成员账户（控制台）(p. 231)和通过邀请指定 GuardDuty 管理员和成员账户 (API) (p. 232)。

GuardDuty委派管理员的重要注意事项

请注意以下因素，这些因素定义了委派管理员的操作方式GuardDuty：

委派管理员最多可以管理 10,000 名成员。

每个GuardDuty委派管理员的成员账户上限为 10,000 个。这包括通过添加的成员帐户Amazon Organizations或接受GuardDuty管理员邀请加入其组织的成员帐户。但是，您的组织中可能有超过 10,000 个帐户。您的组织中所有账户的数量显示在GuardDuty控制台的 “帐户” 页面上。

如果您超过 10,000 个成员帐户的限制，您将通过CloudWatchAmazon Health Dashboard、收到通知，并且还会向委托管理员账户发送一封电子邮件。

委派管理员为区域管理员。

不同的是Amazon Organizations，GuardDuty是一项区域服务。这意味着必须在每个所需的区域中添加GuardDuty委托管理员及其成员帐户Amazon Organizations以进行帐户管理，才能在每个区域中处于活动状态。换句话说，如果组织管理账户仅为GuardDuty美国东部（弗吉尼亚北部）指定委托管理员，则该委派管理员将仅管理在该地区添加的成员账户。有关区域的更多信息，GuardDuty请参阅区域和终端节点 (p. 292)。

一个组织只能指定一个GuardDuty委派管理员。

您只能为您的组织指定一名GuardDuty委派管理员。如果您已将某个账户指定为某个区域的委派管理员，则该账户必须是所有其他区域的委派管理员。您可以随时指定新的委派管理员。有关更多信息，请参阅注销GuardDuty委派管理员 (p. 230)。

不建议将您组织的管理帐户设置为委派管理员。

贵组织的管理帐户可以是委派管理员，但根据遵循最小权限原则Amazon的安全最佳实践，不建议这样做。

更改委派管理员并不会GuardDuty对成员帐户禁用。

如果您删除委派管理员，则取消所有关联的成员账户作为 GuardDuty 成员，但不会在这些账户中禁用 GuardDuty。

指定委派管理员所需的权限

GuardDuty委托委派管理员时，您必须具有启用权限GuardDuty以及以下政策声明中列出的某些 Amazon Organizations API 操作。

您可以将以下声明添加到 IAM policy 的末尾以授予这些权限：

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

此外，如果您希望将您的Amazon Organizations管理账户指定为GuardDuty委托管理员，则该实体将需要`CreateServiceLinkedRole`权限才能进行初始化GuardDuty。可以使用以下语句将其添加到 IAM 策略中，将账户 ID 替换为您的组织管理账户的 ID：

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Note

如果您在手动启用的区域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）区域使用，请替换为`"Service": "guardduty.amazonaws.com"`。`"Service": "guardduty.me-south-1.amazonaws.com"`

指定GuardDuty委派管理员

选择您的访问方式，为您的Amazon组织指定委派管理员并添加成员帐户。

Console

步骤 1-为您的组织注册GuardDuty委派管理员

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   要登录，请使用您所在Amazon Organizations组织的管理帐户。
2. 是否已在您的账户中启用 GuardDuty？
   - 如果GuardDuty尚未启用，请选择 “开始”，然后在 “欢迎使用” GuardDuty 页面上指定GuardDuty委派管理员。

     Note

     管理帐户必须具有GuardDuty服务相关角色，委托管理员才能在该帐户GuardDuty中启用和管理。您可以在管理账户的任何区域启用GuardDuty自动创建此角色。
   - 如果GuardDuty已启用，则可以在 “设置” 页面上指定GuardDuty委派管理员。
3. 输入您要指定Amazon**`account ID`**为组织GuardDuty委派管理员的帐户的 12 位数字。
4. 选择 Delegate (委派)。如果尚未启用 GuardDuty，则在指定委派管理员时，将在您当前的区域中为该账户启用 GuardDuty。
5. 如果您想允许委派管理员向成员帐户附加相关权限以启用恶意软件防护，请打开权限设置。
6. （推荐）在每个Amazon区域重复前面的步骤。

指定委派管理员后，您只需要使用组织管理帐户来更改或删除委派管理员帐户。

Important

当您添加账户作为成员时，GuardDuty 会在当前区域中为该账户自动启用。此行为不同于邀请方法，在将帐户添加为成员之前，GuardDuty必须先启用邀请方法。

您必须在每个区域中添加您的组织成员，才能为这些区域启用 GuardDuty。

步骤 2 - 将现有组织账户添加为成员

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 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。这些账户的 Type (类型) 是 via organizations (通过组织)。与组织的GuardDuty委托管理员关联的非成员账户的状态为 “非成员”。
3. 选中账户 ID 旁边的复选框，选择要添加为成员的一个或多个帐户。

   Note

   通过GuardDuty在页面顶部的横幅中选择 “启用”，可以在当前区域为所有组织账户启用功能。此操作还会启用 “自动启用” 功能，该功能可在将来添加到组织GuardDuty中的任何帐户中启用。
   或者，您可以使用筛选字段按关系状态进行筛选：非会员，然后选择当前区域中未GuardDuty启用的每个账户。
4. 选择 “操作”，然后选择 “添加成员”。
5. 确认您要将所选帐户添加为成员。账户的状态将更改为 “已启用”。
6. （推荐）在每个Amazon区域重复这些步骤，以确保您的委托管理员可以管理所有区域中成员账户的调查结果。

步骤 3 - 自动将新组织账户添加为成员

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。

   使用委派的管理员凭据登录。
2. 在导航窗格的 “设置” 下，选择 “帐户”，然后打开 “自动启用”。
3. 此外GuardDuty，如果您想为新账户启用可选检测功能，请选择操作，然后选择启用 S3 保护、启用 Kubernetes 审核日志监控或启用恶意软件保护。有关这些功能的更多信息，请参阅在多账户环境中配置 S3 保护 (p. 75)在多账户环境中配置 EKS 审核日志监控 (p. 17)、或在多GuardDuty账户环境中配置启动的恶意软件扫描 (p. 58)。
4. （推荐）在每个Amazon区域重复这些步骤，以确保GuardDuty在每个区域的任何新账户上自动启用该功能。

自动启用功能GuardDuty适用于您组织的所有未来成员。这允许您的GuardDuty委派管理员管理在组织内创建或添加到组织中的任何新成员。当成员帐户数量达到 10,000 的限制时，自动启用功能将自动关闭。如果您移除成员帐户且成员总数减少到少于 10,000，则自动启用功能将重新开启。

API

指定委派管理员并添加成员账户 (API)

1. 使用组织管理账户Amazon Web Services 账户的证书运行 enableOrganizationAdminAccountAPI 操作。

   您也可以使用Amazon命令行通过运行以下 CLI 命令来执行此操作。请务必指定要设置为GuardDuty委派管理员的账户的账户 ID。

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 11111111111
   ```

   此命令仅为您的当前区域设置委派管理员。如果尚未在当前区域中为该账户启用 GuardDuty，则会自动启用。

要为其他区域设置委派管理员，您必须指定您希望授权管理员管理的区域。有关更多信息，请参阅 GuardDuty 终端节点和配额。以下示例演示了如何在美国西部（俄勒冈）启用委托管理员。

```
aws guardduty enable-organization-admin-account --admin-account-id 11111111111 --
region us-west-2
```

2. 使用Amazon Web Services 账户您在上一步中指定为GuardDuty委派管理员的证书运行 CreateMembersAPI 操作。

   您必须指定委托管理员Amazon帐户的区域探测器 ID 以及要成为GuardDuty成员的帐户的帐户详细信息，包括帐户 ID 和电子邮件地址。可以使用此 API 操作创建一个或多个成员。

   > **Important**
   >
   > 添加为成员的账户将在该区域GuardDuty启用，但组织管理账户除外，必须先启用该账户，GuardDuty然后才能将其添加为成员账户。

   您也可以使用Amazon命令行工具运行以下 CLI 命令来执行此操作。务必使用您自己的有效探测器 ID、账户 ID 和电子邮件。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=123456789012,Email=guarddutymember@amazon.com
   ```

   您可以使用 ListAccountsAPI 操作或运行以下 CLI 命令来查看所有组织成员的列表。

   ```
   aws organizations list-accounts
   ```

3. 使用GuardDuty委托管理员账户的证书运行 updateOrganizationConfigurationAPI 操作，以便GuardDuty在该区域自动为新成员账户启用。

   您必须指定委托管理员Amazon帐户的探测器 ID。

   您也可以使用Amazon命令行工具运行以下 CLI 命令来执行此操作。务必使用您自己的有效探测器 ID。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

   ```
   aws guardduty update-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable
   ```

   您可以通过运行 describeOrganizationConfigurationAPI 操作或使用所需区域中委托管理员的检测器 ID 运行以下 CLI 命令来确认您已在某个区域中开启自动启用GuardDuty功能。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到当前区域的 detectorID，也可以使用 API。ListDetectors

   ```
   aws guardduty describe-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0
   ```

4. （推荐）使用该区域的唯一探测器 ID 在每个区域重复这些步骤，以启用对所有成员的GuardDuty监控覆盖范围Amazon Web Services 区域。

将GuardDuty管理员帐户合并到单个组织委派管理员下

GuardDuty建议使用关联Amazon Organizations来管理委托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的管理员和通过邀请关联的成员合并到单个GuardDuty委派管理员之下。

> Note
>
> 已经由GuardDuty委派管理员管理的帐户或具有活跃成员的委托管理员帐户无法添加到其他GuardDuty委托管理员帐户。每个组织在每个区域只能有一个GuardDuty委派管理员账户，每个成员账户只能有一个委派管理员。

1. 确保您要为 GuardDuty 管理的所有账户都是您组织的一部分。有关向您的组织添加帐户的信息，请参阅邀请Amazon Web Services 账户加入您的组织。
2. 取消所有成员帐户与先前存在的管理员帐户的关联，但您希望指定为组织GuardDuty委派管理员的帐户下的成员帐户除外。
3. 从 “设置” 页面为组织指定GuardDuty委派管理员。
4. 登录到指定的委派管理员账户。
5. 继续向您的Amazon组织添加成员。

> Important
>
> GuardDuty是一项区域服务。在合并GuardDuty管理员帐户之前，请指定并启用您的委托管理员帐户，并将所有成员帐户添加到组织中。建议您在每个地区都这样做，以最大限度地提高其有效性GuardDuty。

注销GuardDuty委派管理员

> Note
>
> 只有组织管理帐户可以注销委托管理员。

选择控制台或 API，然后按照提供的步骤注销您的委托管理员。取消注册完成后，您可以指定新的委派管理员。

Console

当您从控制台注销委派管理员时，如果您的账户也是组织管理账户，则必须在您的账户被指定为委托管理员的每个区域重复此过程。

> Important
>
> 如果您是组织管理账户，并且已将其他账户指定为委派管理员，则将在每个区域注销他们的注册。

1. 通过 https://console.aws.amazon.com/guardduty/ 打开GuardDuty主机。
2. 选择设置。
3. 在 “设置” 页面的 “委派管理员” 下，选择 “删除”。
4. 选择 “删除管理员” 确认更改。

API

从 API 中注销委派管理员时，必须先在每个区域注销委派管理员，然后才能指定新的委派管理员。

1. 使用组织管理账户的证书运行 DisableOrganizationAdminAccountAPI 操作。

```
aws guardduty disable-organization-admin-account --admin-account-id "123456789012"
```

2. 在由该委派管理员管理的每个区域中重复此操作。

通过的成员 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。当您使用此方法时，当另一个账户接受您成为成员账户的邀请时，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账户，则可以接受来自其他账户的邀请。接受邀请后，您的账户将成为成员账户。一个Amazon账户不能同时是 GuardDuty 管理员账户和成员账户。

通过邀请关联的账户与通过邀请关联的账户具有相同的总体 administrator-to-member 关系Amazon Organizations，如中所述了解 GuardDuty 管理员账户和成员账户之间的关系 (p. 224)。但是，邀请管理员账户用户无法 GuardDuty 代表关联成员账户启用，也不能查看其Amazon Organizations组织内的其他非成员账户。

Important

使用此方法 GuardDuty 创建成员帐户时，可能会发生跨区域数据传输。为了验证成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户的成员账户。 GuardDuty

通过邀请指定管理员和成员账户（控制台）

可使用以下过程添加账户，邀请账户，或者接受来自其他账户的邀请。

步骤 1 – 添加账户

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中，选择 Accounts (账户)。
3. 在顶部面板中选择 Add accounts by invitation (通过邀请添加账户)。
4. 在添加成员账户页面的输入账户下，Amazon输入要添加的账户的账户 ID 和电子邮件地址。然后，选择 Add (添加)。

   Important

   您在此步骤中指定的电子邮件地址必须与与要添加为 GuardDuty 成员Amazon帐户的帐户关联的电子邮件地址相同。

   您可以通过一次指定一个账户的 ID 和电子邮件地址来添加多个账户。您还可以选择 Upload list (.csv) 来批量添加账户。如果你想邀请其中一些账户 GuardDuty 立即启用，但又想延迟启用其他账户，这可能很有用。

   Important

   您的 .CSV 文件的第一行必须包含以下标题，如下面的示例中所示：**`Account ID,Email`**。后面的每一行必须包含您要添加账户的单个有效账户 ID 和单个有效电子邮件地址。每行必须显示一个账户，账户 ID 和电子邮件地址必须使用逗号分隔。

   ```
   Account ID,Email
   111111111111,user@example.com
   ```

5. 账户添加完毕后，选择 Next (下一步)。

   添加的账户显示在 Accounts 页面上的列表中。此列表中添加的每个账户在 Status 列中具有 Invite 链接。

步骤 2 – 邀请账户

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 在导航窗格中，选择 Accounts (账户)。
3. 选择一个或多个需要启用的帐户 GuardDuty。
4. 选择 “操作” 下拉菜单，然后选择 “邀请”。
5. 在 “邀请到 GuardDuty” 对话框中，提供邀请消息（可选），然后选择 “发送邀请”。

   Note

   如果受邀账户无权访问电子邮件，请选择同时向受邀者的 root 用户发送电子邮件通知，Amazon Web Services 账户并在受邀者的 Personal Health Dashboard 中生成提醒。

   受邀账户的 “状态” 列中的值更改为 “已邀请”。

步骤 3 – 接受邀请

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。
2. 如果您尚未启用 GuardDuty，请在 “启用” GuardDuty 页面 GuardDuty上选择 “启用”。

   Important

   必须 GuardDuty 先启用，然后才能接受成员资格邀请。
3. 如果您已启用 GuardDuty，请执行以下步骤：

   a. 在导航窗格中，选择 Settings (设置)。
   b. 选择 账户。
   c. 确保验证您接受的账户的所有者。选择 “接受” 接受成员资格邀请。
4. 接受邀请后，您的账户将成为 GuardDuty 会员账户。所有者发送邀请的账户成为 GuardDuty管理员账户。管理员账户的状态列中的值何时更改为已监控，管理员账户所有者就会知道。管理员账户所有者现在可以查看和管理您的成员账户的 GuardDuty 调查结果。

通过邀请指定 GuardDuty 管理员和成员账户 (API)

您可以通过 API 操作通过邀请指定管理员和成员 GuardDuty 账户。运行以下 GuardDuty API 操作以在中指定管理员和成员账户 GuardDuty。

使用要指定为 GuardDuty 管理员Amazon帐户的帐户的凭据完成以下步骤。

1. 使用已 GuardDuty 启用的Amazon账户的证书运行 CreateMembersAPI 操作。这是您要用作作管理员 GuardDuty 账户。

   您必须指定当前Amazon账户的检测器 ID 以及要成为 GuardDuty 成员的账户的账户 ID 和电子邮件地址。可以使用此 API 操作创建一个或多个成员。

   您也可以使用Amazon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。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. 使用已 GuardDuty 启用的Amazon账户的证书运行 InviteMembersAPI 操作。这是您要用作作管理员 GuardDuty 账户。

   您必须指定当前Amazon账户的检测器 ID 和要成为 GuardDuty 成员的账户的账户 ID。可以使用此 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。

   您也可以使用Amazon命令行工具通过运行以下 CLI 命令来指定成员帐户。务必使用您自己的有效探测器 ID，以及您要邀请的账户的有效账户 ID。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-
ids 111122223333
```

使用要指定为 GuardDuty 成员账户的每个Amazon账户的凭据完成以下程序。

1. 为每个受邀成为 GuardDuty 成员Amazon账户且您想要接受邀请的账户运行 CreateDetectorAPI 操作。

   您必须指定是否使用 GuardDuty 服务启用探测器资源。必须创建并启用探测器 GuardDuty 才能运行。GuardDuty 在接受邀请之前，必须先启用。

   您也可以使用Amazon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Amazon账户的证书，为每个要接受成员资格邀请的账户运行 AcceptAdministratorInvitationAPI 操作。

   您必须为成员账户指定此Amazon账户的检测器 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。你可以在邀请电子邮件中找到管理员账户的账户 ID，也可以使用 API 的ListInvitations操作。

   您也可以使用Amazon命令行工具通过运行以下 CLI 命令来接受邀请。确保使用有效的探测器 ID、管理员账户 ID 和邀请 ID。

   你可以在 https://console.aws.amazon.com/guardduty/ 控制台的 “设置” 页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
administrator-id 444455556666 --invitation-id 84b097800250d17d1872b34c4daadcf5
```

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 https://github.com/aws-samples/ GuardDuty 上示例存储库中的脚本在多个账户上 GitHub 自动启用或禁用amazon-guardduty-multiaccount-scripts。使用本节中的流程启用 GuardDuty 使用 Amazon EC2 的成员账户列表。有关使用禁用脚本或在本地设置脚本的信息，请参阅 GitHub 说明。

该enableguardduty.py脚本启用 GuardDuty、发送来自管理员帐户的邀请，并接受所有成员帐户中的邀请。结果是一个包含所有成员 GuardDuty 帐户的所有安全发现的管理员帐户。由于 GuardDuty 是按区域隔离的，因此每个成员账户的发现都会汇总到管理员账户中的相应区域。例如，您的 GuardDuty 管理员账户的 us-east-1 区域包含所有相关成员账户的 us-east-1 区域的 us-east-1 区域。

这些脚本依赖于具有托管策略的共享 IAM 角色—Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)。此政策为实体提供访问权限， GuardDuty 并且必须存在于管理员账户和您要启用的每个账户中 GuardDuty。

默认情况下， GuardDuty 在所有可用区域中启用以下流程。您只能通过使用可选--enabled_regions参数并提供以逗号分隔的区域列表 GuardDuty 在指定区域中启用。您还可以选择通过打开 enableguardduty.py 并编辑 gd_invite_message 字符串，自定义发送给成员账户的邀请消息。

1. 在 GuardDuty 管理员账户中创建 IAM 角色并附加要启用的Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)策略 GuardDuty。
2. 在您希望由 GuardDuty 管理员账户管理的每个成员账户中创建 IAM 角色。此角色必须与步骤 1 中创建的角色同名，应允许管理员账户作为可信实体，并且应具有前面描述的相同 AmazonGuardDutyFullAccess 管理策略。
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 中将角色添加到的成员账户的账户 ID 和电子邮件的列表。帐户必须每行显示一个，并且帐户 ID 和电子邮件地址必须用逗号分隔，如以下示例所示。

```
111122223333,guardduty-member@organization.com
```

   Note

   CSV 文件必须与 enableguardduty.py 脚本的位置相同。您可以使用以下方法将现有 CSV 文件从 Amazon S3 复制到您的当前目录。

```
aws s3 cp s3://my-bucket/my_key_name example.csv
```

6. 运行 Python 脚本。确保提供您的 GuardDuty 管理员账户 ID、在第一步中创建的角色名称以及 CSV 文件的名称作为参数。

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

估算 GuardDuty 成本

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。在 30 天的免费试用期内，成本估算可以预测试用期结束后的预计成本。如果您在多账户环境中运营，您的 GuardDuty 管理员账户可以监控所有成员账户的成本指标。

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-列出以下 GuardDuty 数据源类型的指定数据源的估计成本：VPC 流日志、 CloudTrail 管理日志、CloudTrail 数据事件或 DNS 日志。
- 功能 — 列出以下 GuardDuty 功能在指定数据源上的预估成本：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或 Lambda 网络活动监控。
- S3 存储桶 — 列出指定存储桶上的 S3 数据事件的估计成本，或环境中账户最昂贵的存储桶。

  Note

  只有在为账户启用 S3 保护后，S3 存储桶统计数据才可用。有关更多信息，请参阅亚马逊的 Amazon S3 保护 GuardDuty (p. 74)：

了解使用成本是如何计算的

使用的成本监控功能时 GuardDuty，了解估算值的计算方式非常重要。中显示的估算值 GuardDuty 可能与您的 Billinemanagemenemenemenemenemenemenmen 请注意以下有关如何计算 GuardDuty 成本估算的内容。

- GuardDuty 使用量估计值仅适用于当前区域。
- GuardDuty 使用量估算值是根据过去 7 到 30 天的使用量得出的平均每日成本。

  Note

  对于新启用的探测器 ID 或使用时间少于七天的数据源，费用列为 “待定”。
- 试验估计值反映了目前处于试用期的数据源。
- GuardDuty 使用量估算包括每个地区的 GuardDuty 批量定价折扣，详见亚马逊 GuardDuty 定价页面，但仅适用于符合批量定价等级的个人账户。批量定价折扣不包含在组织内账户之间合并总使用量的估算值中。有关合并使用量discount 定价的信息，请参阅Amazon账单：批量折扣。

当您为账户启用 EKS 运行时监控时，会根据账户VPC 流日志 (p. 15)中的 EKS EC2 节点 GuardDuty 继续分析和生成安全调查结果。这 GuardDuty 有助于基于 VPC Flow Log 覆盖范围所特有的威胁检测功能继续提供安全覆盖范围。这还有 GuardDuty 助于在 EKS 运行时监控覆盖范围差距的情况下继续提供覆盖范围。但是，您无需为 EKS EC2 节点的 EKS 运行时监控和 VPC 流日志监控付费。

GuardDuty 如果从 EKS EC2 节点接收运行时事件，则无需为分析来自该实例的 VPC 流日志付费。或者，GuardDuty 如果未从 EKS EC2 节点接收运行时事件，则无需为分析来自实例的运行时事件付费。

查看 GuardDuty 使用情况统计信息

选择一种访问方法来查看您的 GuardDuty账户的使用情况统计信息。如果您是 GuardDuty 管理员，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. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 主机。

   确保使用 GuardDuty 管理员帐户。
2. 在导航窗格中，选择 Usagemen ag emen
3. GuardDuty 拥有成员的管理员帐户会看到所有托管帐户的列表。单一账户查看按数据源划分的明细。

   如果您有成员账户，则可以通过在账户表中选择个人账户来查看该账户的统计信息。如果为所选账户启用了 S3 保护，则按使用成本排列的前 S3 存储段将显示在“按数据源”面板中。

   Note

   绿点表示免费试用期已启动。

API

使用 GuardDuty 管理员帐户的凭据调用 GetUsageStatisticsAPI 操作。提供以下信息以运行该命令：

- （必选）提供要为其检索统计数据的账户的区域 GuardDuty 探测器 ID。
- （必需）提供要检索的统计信息类型之一：SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | TOP_RESOURCES。
- （必需）通过以下选项提供至少一个数据源进行查询：FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_LOGS | KUBERNETES_AUDIT_LOGS | EC2_MALWARE_SCAN | RDS_LOGIN_EVENTS | EKS_RUNTIME_MONITORING | LAMBDA_NETWORK_LOGS。
- （可选）提供您要检索其使用情况统计信息的账户 ID 列表。

您也可以使用 Amazon Command Line Interface。以下命令是一个获取示例，用于检索所有数据源和功能的使用总和。请务必detector-id用您自己的有效探测器 ID 替换。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，则会看到所有成员按账户列出的费用。

你可以在 https://console.aws.amazon.com/guardduty/ 控制台的设置页面上找到你当前区域的 detectorId，也可以使用 ListDetectorsAPI。

```
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",
 "RDS_LOGIN_EVENTS", "EKS_RUNTIME_MONITORING", "LAMBDA_NETWORK_LOGS"]}'
```

亚马逊的安全 GuardDuty

Amazon 十分重视云安全性。作为 Amazon 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Amazon和您的共同责任。责任共将其描述为云的安全性和云中的安全性。

- 云的安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为 Amazon 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。要了解适用于的合规性计划 GuardDuty，请参阅范围内的Amazon服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 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型 GuardDuty。它说明了如何配置 GuardDuty 以实现您的安全性和合规性目标。您还将了解如何使用其他Amazon服务来帮助您监控和保护 GuardDuty 资源。

目录

- Amazon 数据保护 GuardDuty (p. 238)
- 使用以下命令记录亚马逊 GuardDuty API 调用Amazon CloudTrail (p. 240)
- 适用于 Amazon 的Identity and Access Management GuardDuty (p. 243)
- Amazon Amazon 的 GuardDuty (p. 269)
- Amazon 中的恢复能力 GuardDuty (p. 269)
- Amazon 中的基础设施安全性 GuardDuty (p. 269)

Amazon 数据保护 GuardDuty

共担担担担担 GuardDuty 如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置单个用户。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您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon Web Services 中的所有默认安全控制。
- 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。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

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 Name（名称）字段）。这包括使用控制台、API、Amazon CLI 或 Amazon SDK 处理 GuardDuty 或其他

Amazon Web Services时。您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。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

静态加密

所有GuardDuty客户数据均使用加密解决方案进行静Amazon态加密。

GuardDuty使用Amazon自有客户管理的密钥使用 Amazon Key Management Service (Amazon KMS) 对发现等数据进行静态加密。

传输中加密

GuardDuty分析来自其他服务的日志数据。它使用 HTTPS 和 KMS 对从这些服务传输的所有数据进行加密。一旦从日志中GuardDuty提取了所需的信息，它们就会被丢弃。有关如何GuardDuty使用其他服务信息的更多信息，请参阅GuardDuty数据源 (p. 14)。

GuardDuty数据在服务之间传输时进行加密。

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，选择Amazon Organizations不将您的数据用于开发GuardDuty和改进以及其他Amazon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《Amazon Organizations用户指南》中的 AI 服务退出政策。

> Note
>
> 要使用选择退出政策，您的Amazon账户必须由集中管理Amazon Organizations。如果您尚未为Amazon账户创建组织，请参阅Amazon Organizations用户指南中的创建和管理组织。

选择退出具有以下效果：

- GuardDuty将删除它在您选择退出之前收集和存储的数据（如果有）。
- 在您选择退出后，GuardDuty将不再收集或存储这些数据。

EKS 运行时监控

EKS Elastic Kubernetes Service（Amazon EKS EKS）集群具有运行时威胁检测功能（Amazon EKS EKS）集群 启用 EKS 运行时监控并在 EKS 集群上部署 EKS 附加安全代理后，GuardDuty监控和分析 EKS 容器工作负载运行时事件，例如文件访问、流程执行和网络连接。

虽然目前GuardDuty不收集您可能定向到 EKS 集群的命令行参数、模块参数和程序参数，但安全代理的 future 版本可能会这样做，以开发和改进其 EKS 运行时监控威胁检测和服务。GuardDuty收集的数据也可用于开发和改进其他Amazon安全服务。您的信任、隐私和内容安全是我们的重中之重，并确保我们的使用符合我们对您的承诺。有关更多信息，请参阅数据隐私常见问题。

GuardDuty恶意软件防护

GuardDuty恶意软件保护会扫描并检测与可能受感染的 Amazon EC2 实例和容器工作负载相关的 EBS 卷中包含的恶意软件。当 M GuardDuty alware Protection 将 EBS 卷文件识别为恶意或有害文件时，GuardDuty恶意软件保护会收集并存储该文件，以开发和改进其恶意软件检测和服务。GuardDuty此文件也可用于开发和改进其他Amazon安全服务。您的信任、隐私和内容安全是我们的重中之重，并确保我们的使用符合我们对您的承诺。有关更多信息，请参阅数据隐私常见问题。

使用以下命令记录亚马逊 GuardDuty API 调用 Amazon CloudTrail

GuardDuty Amazon 已与Amazon CloudTrail服务集成，后者提供了中由用户、角色或Amazon服务所采取操作的记录 GuardDuty。 CloudTrail 将对的所有 API 调用均 GuardDuty 作为事件捕获，包括来自 GuardDuty 控制台的调用和对 GuardDuty API 的代码调用。如果您创建跟踪记录，则可以使 Amazon Simple Storage Service (Amazon S3) 存储桶（包括的事件） GuardDuty。 CloudTrail 如果您不配置跟踪记录，则仍可在 Event history（事件历史记录）中查看 CloudTrail 控制台中的最新事件。通过使用收集的信息 CloudTrail，您可以确定向发出了什么请求 GuardDuty、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其它详细信息。

有关 CloudTrail更多信息（包括如何对其进行配置和启用），请参阅Amazon CloudTrail用户指南。

GuardDuty 中的信息 CloudTrail

CloudTrail 在您创建Amazon账户时，即针对该账户启用了。当中发生受支持的事件活动时，该活动将记录在 GuardDuty事件历史记录中，并与其他Amazon服务 CloudTrail 事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 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记录查看 CloudTrail 事件。

要持续记录Amazon账户中的事件（包括的事件） GuardDuty，请创建跟踪。通过跟踪 CloudTrail ，可以将日志文件传送至 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 Amazon 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）桶。此外，您可以配置其他Amazon服务，进一步分析在 CloudTrail 日志文件中收集的事件数据并采取操作。有关更多信息，请参阅：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为配置 Amazon SNS 通知 CloudTrail
- 从多个区域接收 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件文件

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还是 IAM 用户的登录凭证发出的
- 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 Amazon 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

GuardDuty 控制层事件 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

EKS 运行时监控 (p. 21)使用 GuardDuty 安全代理 Amazon EKS 附加组件 (`aws-guardduty-agent`)，它运行时事件类型 (p. 37)为您的 Amazon Elastic Kubernetes Service (Amazon EKS) 节点和工作负载收集并将其发送到 GuardDuty 进行威胁检测和分析。有关 GuardDuty 调查结果的更多信息，请参阅了解亚马逊的 GuardDuty调查结果 (p. 78)。

记录和监控数据事件

您可以选择配置Amazon CloudTrail日志以查看 GuardDuty 安全代理的数据事件。

要创建和配置 CloudTrail，请参阅Amazon 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Amazon Web Services Management Console。记录文件时，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，选择记录所有事件。
- 展开配置的 JSON 视图。它应该类似于以下 JSON：

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

启用跟踪选择器后，导航到 S3 控制台，网址为 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

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含日志文件 一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公有 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 演示数据层面事件。

```
{
        "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-EXAMPLEbbbbb",
        "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"
        }
    }
```

下面的示例显示了一个说明CreateIPThreatIntelSet操作 CloudTrail 的日日志文件的日志文件的日志文件的日志文件事件。

```
{
    "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 发出的。

适用于 Amazon 的Identity and Access Management GuardDuty

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用 GuardDuty 资源的人员。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- 受众 (p. 243)
- 使用身份进行身份验证 (p. 244)
- 使用策略管理访问 (p. 245)
- 亚马逊如何与 IAM 协同 GuardDuty 工作 (p. 246)
- 适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)
- 对 Amazon 使用服务相关角色 GuardDuty (p. 256)
- Amazon GuardDuty 身份和访问疑难解答 (p. 264)
- Amazon亚马逊的托管政策 GuardDuty (p. 265)

受众

使用 Amazon Identity and Access Management (IAM) 的方式因您可以在 GuardDuty 中执行的操作而异。

服务用户-如果您使用 GuardDuty 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 GuardDuty 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 GuardDuty 中的功能，请参阅 Amazon GuardDuty 身份和访问疑难解答 (p. 264)。

服务管理员 — 如果您在公司负责 GuardDuty 管理，您可能具有的完全访问权限 GuardDuty。您有责任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 管理员提交请求以更改服务用

户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何使用 IAM 的更多信息 GuardDuty，请参阅亚马逊如何与 IAM 协同 GuardDuty 工作 (p. 246)。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 GuardDuty 的访问权限的详细信息。要查看您可在 IAM 中使用的 GuardDuty 基于身份的策略示例，请参阅适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包 (SDK) 和命令行界面（CLI），以便使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅《Amazon Web Services 一般参考》中的 签名版本 4 签名流程。

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，Amazon 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《IAM 用户指南》中的在 Amazon 中使用多重身份验证 (MFA)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。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。有关要求您以根用户身份登录的任务的完整列表，请参阅 Amazon Account Management 参考指南 中的需要根用户凭证的任务。

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）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

IAM 用户和组

IAM 用户是Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，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 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。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，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以担任角色。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。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（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。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 Amazon Web Services使用其它 Amazon Web Services中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（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。
  - 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅《服务授权参考》 GuardDuty中的 Amazon 的操作、资源和条件键。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 创建向 Amazon Web Service 委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 Amazon Web Service关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户 中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 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 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南 中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（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 policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（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。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

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中使用来自 IAM 的 Amazon 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Simple Storage Service（Amazon S3）、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表 (ACL) 概览。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。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 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 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 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 Amazon Web Services 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份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 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊如何与 IAM 协同 GuardDuty 工作

在使用 IAM 管理对的访问之前 GuardDuty，您应该了解哪些 IAM 功能可用于 GuardDuty。

可与 Amazon 结合使用的 IAM 功能 GuardDuty

IAM 功能	GuardDuty 支持
基于身份的策略 (p. 247)	是
基于资源的策略 (p. 247)	否
策略操作 (p. 248)	是
策略资源 (p. 248)	是
策略条件键 (p. 249)	是
ACL (p. 249)	否
ABAC（策略中的标签） (p. 249)	部分
临时凭证 (p. 250)	是
委托人权限 (p. 250)	是
服务角色 (p. 250)	是
服务相关角色 (p. 250)	是

要大致了解 GuardDuty 和其他Amazon服务如何与大多数 IAM 功能结合使用，请参阅《IAM 用户指南》中的与 IAM 结合使用的Amazon服务。

的基于身份的策略 GuardDuty

支持基于身份的策略	是

基于身份的策略是可附加到身份（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 policy。

通过使用 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。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

的基于身份的策略示例 GuardDuty

要查看 GuardDuty 基于身份的策略示例，请参阅适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)。

内内内内内基于资源的策略 GuardDuty

支持基于资源的策略。	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（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。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。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。当主体和资源处于不同的Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。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》中的 IAM 角色与基于资源的策略有何不同。

适用于的策略操作 GuardDuty

支持策略操作	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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 策略的 `Action` 元素描述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 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 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相关操作的权限。

要查看 GuardDuty 操作的列表，请参阅《服务授权参考》 GuardDuty中的 Amazon 定义的操作。

中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 基于身份的策略示例，请参阅适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)。

的政策资源 GuardDuty

支持策略资源	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）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 ARN 的列表，请参阅《服务授权参考》 GuardDuty中的 Amazon 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon 定义的操作 GuardDuty。

要查看 GuardDuty 基于身份的策略示例，请参阅适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)。

的策略条件键 GuardDuty

支持特定于服务的策略条件键	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。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 Amazon 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 Amazon 使用逻辑 OR 运算来评估条件。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，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

Amazon支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 Amazon 全局条件上下文键。

要查看 GuardDuty 条件键的列表，请参阅《服务授权参考》 GuardDuty中的 Amazon 的条件键。要了解您可以在哪些操作和资源中使用条件键，请参阅 Amazon 定义的操作 GuardDuty。

要查看 GuardDuty 基于身份的策略示例，请参阅适用于 Amazon 的基于身份的策略示例 GuardDuty (p. 251)。

中的访问控制列表（ACL） GuardDuty

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 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) 是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及Amazon资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

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 Yes（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 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问控制（ABAC）。

将临时凭证用于的使用 GuardDuty

支持临时凭证	是

某些 Amazon Web Services在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon Web Services与临时凭证配合使用，请参阅 IAM 用户指南中的使用 IAM 的 Amazon Web Services。

如果您不使用用户名和密码而用其它方法登录到Amazon Web Services Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问Amazon时，该过程将自动创建临时凭证。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 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

的跨服务主体权限 GuardDuty

支持委托人权限	是

当您使用 IAM 用户或角色在Amazon中执行操作时，您将被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅《服务授权参考》 GuardDuty 中的 Amazon 的操作、资源和条件键。

GuardDuty 的服务角色

支持服务角色	是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 创建向 Amazon Web Service 委派权限的角色。

> Warning
>
> 更改服务角色的权限可能会破坏 GuardDuty 功能。仅当 GuardDuty 提供相关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 Amazon Web Service相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户 中，并由该服务拥有。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，请参阅对 Amazon 使用服务相关角色 GuardDuty (p. 256)。

有关创建或管理服务相关角色的详细信息，请参阅使用 IAM 的Amazon服务。在表中查找服务相关角色列中包含 Yes 额表。选择 Yes 链接以查看该服务的服务相关角色文档。

适用于 Amazon 的基于身份的策略示例 GuardDuty

默认情况下，用户和角色没有创建或修改 GuardDuty 资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface（Amazon CLI）或 Amazon API 执行任务。要用户用户在其需要的资源上执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 创建 IAM policy。

有关定义的操作和资源类型的详细信息 GuardDuty，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》 GuardDuty中的 Amazon 的操作、资源和条件键。

主题

- 策略最佳实践 (p. 251)
- 使用 GuardDuty 控制台 (p. 252)
- 启用 GuardDuty 所需的权限 (p. 252)
- 允许用户查看他们自己的权限 (p. 252)
- 用于的自定义 IAM 策略 GuardDuty (p. 253)
- 拒绝访问 GuardDuty 调查结果 (p. 253)
- 使用自定义 IAM 策略来限制对 GuardDuty 资源的访问 (p. 254)

策略最佳实践

基于身份的策略确定某个用户是否可以创建、访问或删除您账户中的 GuardDuty 资源。这些操作可能会使 Amazon Web Services 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户管理型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 Amazon 托管策略或工作职能的 Amazon 托管策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请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 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- Require multi-factor authentication（MFA）[需要多重身份验证（MFA）] – 如果您所处的场景要求您的 Amazon Web Services 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作

时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 GuardDuty 控制台

要访问 Amazon GuardDuty 控制台，您必须具有一组最低的权限。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Amazon Web Services 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。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 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，还要将 GuardDuty `ConsoleAccess`或`ReadOnly`Amazon托管策略附加到实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限。

启用 GuardDuty 所需的权限

要授予各种 IAM 身份（用户、组和角色）必须具有的权限，请附加要启用的Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)策略 GuardDuty。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "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": "*"
        }
    ]
```

```
}
```

用于的自定义 IAM 策略 GuardDuty

要向 GuardDuty 您授予只读访问权限，可以使用AmazonGuardDutyReadOnlyAccess托管策略。

要创建向 IAM 角色、用户或群组授予只读访问权限的自定义策略 GuardDuty，您可以使用以下语句：

```
{
    "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来拒绝 IAM 角色、用户或组访问 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 策略来限制对 GuardDuty 资源的访问

要 GuardDuty 根据检测器 ID 定义用户的访问权限，您可以在自定义 IAM 策略中使用所有 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 定义用户对的访问权限：

- 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 1234567 的检测器 ID 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 1234567 的检测器 ID 和 000000 的 IPset ID 来运行该guardduty:UpdateIPSet操作：

  Note

  确保用户具有访问中的可信 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 (p. 194)：

```
{
    "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 区域使用任何探测器 ID 和 000000 的 IPset ID 来运行guardduty:UpdateIPSet操作：

  Note

  确保用户具有访问中的可信 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 (p. 194)：

```
{
    "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 来运行`guardduty:UpdateIPSet`操作：

  Note

  确保用户具有访问中的可信 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 (p. 194)：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

对 Amazon 使用服务相关角色 GuardDuty

亚马逊 GuardDuty 使用Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色 (SLR) 是一种与直接关联的独特类型的 IAM 角色 GuardDuty。服务相关角色由预定义， GuardDuty 并包含代表您调用其他Amazon服务 GuardDuty 所需的一切权限。

使用服务关联角色， 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，除非另有定义，否则只有 GuardDuty 可以承担该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

GuardDuty 支持在所有可用区域中使用服务相关角色。 GuardDuty 有关更多信息，请参阅区域和终端节点 (p. 292)：

只有在启用 GuardDuty 服务相关角色的所有区域 GuardDuty 中先禁用服务相关角色之后，您才可以删除服务相关角色。这将保护您的 GuardDuty 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅 IA M 用户指南中显示为 Yes（是）的Amazon服务，并查找 Service-linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

的服务相关角色权限 GuardDuty

GuardDuty 使用名为 Service-linked Role（服务相关角色）`AWSServiceRoleForAmazonGuardDuty`。SLR GuardDuty 允许执行以下任务。它还允许 GuardDuty 将检索到的属于 EC2 实例的元数据包含在 GuardDuty 可能生成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。

使用此权限策略 GuardDuty 可以执行以下任务：

- 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 VPC、子网、传输网关和安全组）的信息。
- 使用Amazon Organizations操作来描述关联账户。
- 使用 Amazon S3 操作检索有关 S3 存储桶和对象的信息。
- 启用恶意软件保护恶意软件保护的服务相关角色权限 (p. 259)后，使用 IAM 创建。

该角色使用以下名为的Amazon托管策略进行配置AmazonGuardDutyServiceRolePolicy。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments"
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
      ],
        "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

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"
    }
  ]
```

```
}
```

创建服务相关角色 GuardDuty

AWSServiceRoleForAmazonGuardDuty服务关联角色是在您首次启用时自动创建 GuardDuty 的，或者 GuardDuty 在之前未启用该角色的受支持区域启用该角色时自动创建的。您还可以使用 IAM 控制台、或 IAM API 手动创建服务相关角色。Amazon CLI

> **Important**
>
> 为 GuardDuty 委托管理员账户创建的服务关联角色不适用于成员 GuardDuty 账户。

您必须配置权限以允许 IAM 委托人 (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**
>
> 将以下示例中的示例*## ID* 替换为您的实际Amazon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。

为编辑服务相关角色 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。不过，您可以使用 IAM 编辑角色的说明。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

如果您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
>
> 如果您启用了恶意软件防护，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保护的服务相关角色。

您必须先 GuardDuty 在所有启用该功能的区域中禁用，才能删除AWSServiceRoleForAmazonGuardDuty。如果您尝试删除 GuardDuty 服务相关角色时未禁用该服务，删除服务相关角色将失败。有关更多信息，请参阅暂停或禁用 GuardDuty (p. 282)：

禁用时 GuardDuty，AWSServiceRoleForAmazonGuardDuty不会自动删除。如果你 GuardDuty 再次启用，它将开始使用现有的AWSServiceRoleForAmazonGuardDuty。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、Amazon CLI 或 IAM API 删除 AWSServiceRoleForAmazonGuardDuty 服务相关角色。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 Amazon Web Services 区域

亚马逊 GuardDuty 支持在所有可用Amazon Web Services 区域的地 GuardDuty 方使用AWSServiceRoleForAmazonGuardDuty服务相关角色。有关当前可用的区域列表 GuardDuty ，请参阅中的 Amazon GuardDuty 终端节点和配额Amazon Web Services 一般参考。

恶意软件保护的服务相关角色权限

恶意软件保护使用名为 Service-linked Role（服务相关角色）AWSServiceRoleForAmazonGuardDutyMalwareProtection。此 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。它 GuardDuty 允许在您的账户中创建 EBS 卷快照，并与 GuardDuty 服务账户共享该快照。 GuardDuty 评估快照后，它会在恶意软件保护调查结果中包含检索到的 EC2 实例和容器工作负载元数据。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服务相关角色信任 malware-protection.guardduty.amazonaws.com 服务来代入角色。

该角色的权限策略允许恶意软件保护执行以下任务：

- 使用 Amazon EC2 操作检索有关您的 EC2 实例、卷和快照的信息。恶意软件保护还提供访问亚马逊 EKS 和 Amazon 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，使用GuardDutyScanId标签创建快照。请勿删除此标签，否则恶意软件保护将无法访问快照。

  > Important
  >
  > 当您将设置GuardDutyExcluded为时true，该 GuardDuty服务将来将无法访问这些快照。这是因为此服务相关角色中的其他语句 GuardDuty 阻止对GuardDutyExcluded设置为的快照执行任何操作true。

- 仅当GuardDutyScanId标签存在且标签未设置为时，才允许共享和GuardDutyExcluded删除快照true。

  > Note
  >
  > 不允许恶意软件保护将快照公开。

- 访问客户管理的密钥（GuardDutyExcluded标签设置为true的密钥除外），通过调CreateGrant用创建和访问与 GuardDuty 服务帐户共享的加密快照创建和访问加密 EBS 卷。有关每个区域的 GuardDuty 服务帐号列表，请参阅GuardDuty服务账户由 Amazon Web Services 区域 (p. 50)。
- 访问客户 CloudWatch 日志以创建恶意软件保护日志组，并将恶意软件扫描事件日志放在/aws/guardduty/malware-scan-events日志组下。
- 允许客户决定是否要在自己的账户中保留检测到的恶意软件的快照。如果扫描检测到恶意软件，则服务关联角色允许 GuardDuty 向快照添加两个标签-GuardDutyFindingDetected 和GuardDutyExcluded。

  Note

  该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 EBS 管理的密钥。key Id

  GuardDuty 支持未加密和使用客户管理的密钥加密的卷。但是， GuardDuty 不支持使用 EBS 托管密钥加密的卷。有关更多信息，请参阅恶意软件防护中支持的容量 (p. 49)：
- 允许 Amazon EC2 代表恶意软件保护调用Amazon KMS，对客户管理的密钥执行多项加密操作。需要执行诸如kms:ReEncryptTo和kms:ReEncryptFrom之类的操作才能共享使用客户管理的密钥加密的快照。只有那些GuardDutyExcluded标签未设置为的密钥才可访问true。

该角色使用以下名为的Amazon托管策略进行配置AmazonGuardDutyMalwareProtectionServiceRolePolicy。

```
{
    "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTasks",
    "ecs:DescribeTasks",
    "eks:DescribeCluster"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshot",
   "Resource": "arn:aws:ec2:*:*:volume/*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/GuardDutyExcluded": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshot",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": "GuardDutyScanId"
    }
   }
  },
  {
```

```
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:*:*:*/*",
  "Condition": {
   "StringEquals": {
    "ec2:CreateAction": "CreateSnapshot"
   }
  }
 },
 {
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
   "StringLike": {
    "ec2:ResourceTag/GuardDutyScanId": "*"
   },
   "ForAllValues:StringEquals": {
    "aws:TagKeys": [
     "GuardDutyExcluded",
     "GuardDutyFindingDetected"
    ]
   }
  }
 },
 {
  "Effect": "Allow",
  "Action": [
   "ec2:DeleteSnapshot",
   "ec2:ModifySnapshotAttribute"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
   "StringLike": {
    "ec2:ResourceTag/GuardDutyScanId": "*"
   },
   "Null": {
    "aws:ResourceTag/GuardDutyExcluded": "true"
   }
  }
 },
 {
  "Effect": "Deny",
  "Action": [
   "ec2:ModifySnapshotAttribute"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
   "StringEquals": {
    "ec2:Add/group": "all"
   }
  }
 },
 {
  "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"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom"
   ],
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com"
    },
    "Null": {
     "aws:ResourceTag/GuardDutyExcluded": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "kms:DescribeKey",
   "Resource": "arn:aws:kms:*:*:key/*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "logs:DescribeLogGroups",
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
  }
 ]
}
```

以下信任策略附加至AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

创建服务相关角色

当您首次启用恶意软件保护或在之前未启用恶意软件保护的支持区域中启用恶意软件保护时，将自动创建AWSServiceRoleForAmazonGuardDutyMalwareProtection服务关联角色。您还可以使用 IAM 控制台、IAM CLI 或 IAM API 手动创建AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色。

Note

默认情况下，如果您是亚马逊 GuardDuty的新手，则会自动启用恶意软件防护。

Important

为 GuardDuty 委托管理员账户创建的服务关联角色不适用于成员 GuardDuty 账户。

您必须配置权限以允许 IAM 委托人 (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。

编辑服务相关角色

恶意软件保护不允许您编辑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。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

删除服务相关角色

如果您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，必须先在启用恶意软件保护的所有区域中禁用恶意软件防护。AWSServiceRoleForAmazonGuardDutyMalwareProtection
> 如果您尝试删除服务相关角色时未禁用恶意软件防护，删除服务相关角色将失败。有关更多信息，请参阅启用或禁用GuardDuty启动的恶意软件扫描 (p. 57)：

当您选择 “禁用” 来停止恶意软件保护服务AWSServiceRoleForAmazonGuardDutyMalwareProtection时，不会自动删除。如果您随后选择 “启用” 再次启动恶意软件保护服务，则 GuardDuty 将开始使用现有的AWSServiceRoleForAmazonGuardDutyMalwareProtection。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、Amazon CLI 或 IAM API 删除AWSServiceRoleForAmazonGuardDutyMalwareProtection服务相关角色。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 Amazon Web Services 区域

亚马逊 GuardDuty 支持在所有提供恶意软件保护Amazon Web Services 区域的地方使用AWSServiceRoleForAmazonGuardDutyMalwareProtection服务关联角色。

有关当前可用的区域列表 GuardDuty ，请参阅中的 Amazon GuardDuty 终端节点和配额Amazon Web Services 一般参考。

> **Note**
>
> 恶意软件防护目前在Amazon GovCloud （美国东部）和Amazon GovCloud （美国西部）不可用。

Amazon GuardDuty 身份和访问疑难解答

使用以下信息可帮助您诊断和修复在使用 GuardDuty 和 IAM 时可能遇到的常见问题。

主题

- 我无权在中执行操作 GuardDuty (p. 264)
- 我没有执行 iam 的权限：PassRole。 (p. 265)
- 我希望允许我的以外的人访问我的 GuardDuty 资源。Amazon Web Services 账户 (p. 265)

我无权在中执行操作 GuardDuty

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 guardduty:*GetWidget* 权限时，会发生以下示例错误。

```
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 Amazon 管理员。管理员是向您提供登录凭证的人。

我没有执行 iam 的权限：PassRole。

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 GuardDuty。

有些 Amazon Web Services允许您将现有角色传递到该服务，而不是创建新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 marymajor 的 IAM 用户尝试使用控制台在 GuardDuty 中执行操作时，会发生以下示例错误。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 Amazon 管理员。管理员是向您提供登录凭证的人。

我希望允许我的以外的人访问我的 GuardDuty 资源。Amazon Web Services 账户

您可以创建一个角色，以便其它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 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

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，请参阅亚马逊如何与 IAM 协同 GuardDuty 工作 (p. 246)。
- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的Amazon Web Services 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Amazon亚马逊的托管政策 GuardDuty

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管式策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户 中使用。有关 Amazon 托管策略的更多信息，请参阅 IAM 用户指南中的Amazon 托管策略。

Amazon 服务负责维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管式策略。例如，ReadOnlyAccessAmazon托管策略提供对所有Amazon服务和资源的只读访问权限。当服务启动新功能时，Amazon 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 用户指南中的适用于工作职能的 Amazon 托管策略。

Amazon 托管策略：AmazonGuardDutyFullAccess

您可以将 AmazonGuardDutyFullAccess 策略附加得到 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

此策略包含以下权限。

- 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。这允许GuardDuty管理员启用GuardDuty成员帐户。
- Organizations— 允许用户指定委派管理员和管理GuardDuty组织的成员。

执行iam:GetRole操作的权限AWSServiceRoleForAmazonGuardDutyMalwareProtection确定了账户中是否存在恶意软件防护的服务相关角色 (SLR)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "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"
        }
    ]
}
```

Amazon托管策略：AmazonGuardDutyReadOnlyAccess

您可以将 AmazonGuardDutyReadOnlyAccess 策略附加得到 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

此策略包含以下权限。

- GuardDuty— 允许用户查看GuardDuty发现结果并执行以Get、List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"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon托管策略：AmazonGuardDutyServiceRolePolicy

您不能将 AmazonGuardDutyServiceRolePolicy 附加到自己的 IAM 实体。此Amazon托管策略附加到服务相关角色，GuardDuty允许您代表执行操作。有关更多信息，请参阅的服务相关角色权限GuardDuty (p. 256)：

对 Amazon 托管式策略的 GuardDuty 更新

查看有关 GuardDuty 的 Amazon 托管式策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 GuardDuty 文档历史记录页面上的 RSS 源。

更改	说明	日期
AmazonGuardDutyServiceRolePolicy (p. 257) – 对现有策略的更新	GuardDuty添加了新权限，允许GuardDuty为恶意软件保护创建服务相关角色 (p. 259)。这将有助于GuardDuty简化启用恶意软件保护的过程。 GuardDuty现在可以执行以下 IAM 操作： `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	2023年2月21日
AmazonGuardDutyFullAccess (p. 260) – 对现有策略的更新	GuardDuty已`iam:GetRole`将的 ARN 更新为`*AWSServiceRoleForAmazonGuardDutyMalwareProtection`。	2022年7月26日
AmazonGuardDutyFullAccess (p. 260) – 对现有策略的更新	GuardDuty添加了一个新`AWSServiceName`内容，允许使用`iam:CreateServiceLinkedRole`GuardDuty恶意软件保护服务创建服务相关角色。 GuardDuty现在可以执行`iam:GetRole`操作以获取信息`AWSServiceRole`。	2022年7月26日
AmazonGuardDutyServiceRolePolicy (p. 257) – 对现有策略的更新	GuardDuty添加了新权限，GuardDuty允许使用 Amazon EC2 联网操作来改进调查结果。 GuardDuty现在可以执行以下 EC2 操作以获取有关您的 EC2 实例通信方式的信息。此信息用于提高查找准确性。 • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	2021年8月3日

更改	说明	日期
GuardDuty 已开启跟踪更改	GuardDuty 为其 Amazon 托管式策略开启了跟踪更改。	2021年8月3日

Amazon Amazon 的 GuardDuty

要了解某个 Amazon Web Service 是否在特定合规性计划范围内，请参阅 合规性计划范围内的 Amazon Web Services，然后选择您感兴趣的合规性计划。有关常规信息，请参阅Amazon Web Services合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

您使用 Amazon Web Services 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。Amazon 提供以下资源来帮助满足合规性：

- 安全性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 Amazon 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub – 此 Amazon Web Service 向您提供 Amazon 中安全状态的全面视图。Security Hub 通过安全控件评估您的 Amazon 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 中的恢复能力 GuardDuty

Amazon全球基础设施围绕Amazon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 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

Amazon 中的基础设施安全性 GuardDuty

作为一项托管式服务，A GuardDuty mazon 受Amazon全球网络安全保护。有关 Amazon 安全服务以及 Amazon 如何保护基础架构的信息，请参阅 Amazon 云安全。要按照基础设施安全最佳实践设计您的 Amazon 环境，请参阅《安全性支柱 Amazon Well-Architected Framework》中的 基础设施保护。

您可以使用 Amazon 发布的 API 调用通过网络访问 GuardDuty。客户端必须支持以下内容：

- 传输层安全性协议（TLS）我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（Ephemeral Diffie-Hellman）或 ECDHE（Elliptic Curve Ephemeral Diffie-Hellman）。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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon与... 的服务集成 GuardDuty

GuardDuty 可以与其他Amazon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调查结果。查看下面的集成选项，以详细了解如何设置该服务以配合使用 GuardDuty。

与... 集 GuardDuty 成Amazon Security Hub

Amazon Security Hub跨越Amazon账户、服务和受支持的第三方合作伙伴产品收集安全数据，以根据行业标准和最佳实践评估环境的安全状态。除了评估您的安全态势外，Security Hub 还会创建一个中心位置，用于存放所有集成Amazon服务和Amazon合作伙伴产品的调查结果。启用 Securit GuardDuty y Hub 将自动允许 Security Hub 提取 GuardDuty 发现数据。

有关使用 Security Hub 的更多信息， GuardDuty 请参阅与 Amazon Security Hub 集成 (p. 270)。

GuardDuty 与亚马逊Detective 集成

Amazon Detective 使用来自您Amazon账户的日志数据，为您的资源和与环境交互的 IP 地址创建数据可视化效果。侦探的可视化可帮助您快速轻松地调查安全问题。启用这两项服务后，您可以从 GuardDuty 查找详细信息转向在 Detective 控制台中查找信息。

有关使用 Detective 的更多信息， GuardDuty 请参阅与 Amazon DetDetective (p. 280)。

与 Amazon Security Hub 集成

Amazon Security Hub 提供了您在 Amazon 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 跨各 Amazon 账户、服务和受支持的第三方合作伙伴产品收集安全数据，帮助您分析安全趋势并确定最高优先级的安全问题。

亚马逊与 Sec GuardDuty urity Hub 的集成使您能够将调查结果发送GuardDuty到 Security Hub。Security Hub 可以在其对您的安保状况分析中包含这些结果。

目录

- 亚马逊如何GuardDuty将调查结果发送给 Amazon Security Hub (p. 271)
  - GuardDuty发送到 Security Hub 的结果类型 (p. 271)
    - 发送结果的延迟 (p. 271)
    - Security Hub 不可用时重试 (p. 271)
    - 更新 Security Hub 中的现有结果 (p. 271)
- 在 Amazon Security Hub 中查看 GuardDuty 结果 (p. 271)
  - 解释 Amazon Security Hub 中的 GuardDuty 结果名称 (p. 271)
  - 来自 GuardDuty 的典型结果 (p. 278)
- 启用和配置集成 (p. 280)
- 停止向 Security Hub 发布结果 (p. 280)

亚马逊如何GuardDuty将调查结果发送给 Amazon Security Hub

在 Amazon Security Hub 中，安全问题按结果进行跟踪。一些发现结果来自其他 Amazon 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。请参阅 Amazon Security Hub 用户指南中的查看结果。您还可以跟踪结果的调查状态。请参阅 Amazon Security Hub 用户指南中的对结果采取措施。

Security Hub 中的所有结果都使用标准的 JSON 格式，称为 Amazon Security Finding 格式 (ASFF)。ASFF 包括有关问题根源、受影响资源以及结果当前状态的详细信息。请参阅 Amazon Security Hub 用户指南中的 Amazon Security Finding 格式 (ASFF) 。

亚马逊GuardDuty是将调查结果发送到 Security Hub 的Amazon服务之一

GuardDuty发送到 Security Hub 的结果类型

启用集成后，将其生成的所有调查结果GuardDuty发送到 Security Hub。结果发送到 SSecurity Hub Amazonurity Finding。在 ASFF 中，Types 字段提供结果类型。

发送结果的延迟

GuardDuty创建新结果时。通常会在五分钟内将结果发送到 Security Hub。

Security Hub 不可用时重试

如果 Securit GuardDuty y Hub 不可用。

更新 Security Hub 中的现有结果

将结果发送到 Security Hub 之后。GuardDuty会发送反映对查找活动的其他观测结果到 Security Hub 中。汇总结果的更新速率基于导出更新频率 (p. 202)指定的值。

在 Security Hub 中的GuardDuty结果不会更新 Security Hub 中。这意味着手动取消存档的处于活动状态的发现GuardDuty将不会发送到 Security Hub

在 Amazon Security Hub 中查看 GuardDuty 结果

要在 Securit GuardDuty y Hub 中查看您的调查结果，请GuardDuty从摘要页面选择亚马逊下方的 “查看调查结果”。或者，您可以从导航面板中选择 “查找结果”，然后通过选择值为的 “产品名称:” 字段对GuardDuty查找结果进行筛选，使其仅显示搜索结果GuardDuty。

解释 Amazon Security Hub 中的 GuardDuty 结果名称

GuardDuty 使用 Amazon 安全结果格式 (ASFF) 将结果发送到 Security Hub。在 ASFF 中，Types 字段提供结果类型。ASFF 使用与不同的命名GuardDuty方案。下表详细列出了所有GuardDuty查找类型及其在 Security Hub 中出现的 ASFF 对应类型。

> Note
>
> 对于某些GuardDuty查找类型，Security Hub 会根据搜索结果细节的资源角色是 ACTOR 还是 TARGET 来分配不同的 ASFF 查找名称。有关更多信息，请参阅 正在寻找细节 (p. 78)。

GuardDuty结果类型	ASFF 结果类型
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
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: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

GuardDuty结果类型	ASFF 结果类型
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
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:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
发现:iamUser/ AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
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
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
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

GuardDuty结果类型	ASFF 结果类型
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/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
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
Impact: iamUser/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/ AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
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.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission

GuardDuty结果类型	ASFF 结果类型
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
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
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:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
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:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified

GuardDuty结果类型	ASFF 结果类型
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
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
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

GuardDuty结果类型	ASFF 结果类型
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
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结果类型	ASFF 结果类型
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/ UnauthorizedAccess: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
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 Amazon 安全结果格式 (ASFF)将结果发送到 Security Hub。

下面是 GuardDuty 典型结果的示例。

```
{
"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": "kubectl"
      },
      "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Amazon Security Hub，您必须启用 Security Hub。有关如何启用 Security Hub 的信息，请参阅 Amazon Security Hub 用户指南中的设置 Security Hub。

当您同时启用GuardDuty和 Security Hub 时。GuardDuty立即开始将结果发送到 Security Hub。

停止向 Security Hub 发布结果

要停止向 Security Hub 发送结果，您可以使用 Security Hub 控制台或 API。

请参阅Amazon Security Hub用户指南中的禁用和启用来自集成的结果流（控制台）或禁用来自集成的结果流（Security Hub AP Amazon I、CLI）。

与 Amazon DetDetective

Amazon Detecti ve 通过生成数据可视化来代表您的资源在一段时间内的行为和交互方式，帮助您快速分析和调查一个或多个Amazon账户的安全事件。Detective 创建 GuardDuty发现的可视化效果。

Detective 收集所有发现类型的发现细节，并提供对实体概况的访问权限，以调查参与发现的不同实体。实体可以是账户内的Amazon资源Amazon Web Services 账户，也可以是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：Amazon Web Services 账户、IAM 角色、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 (p. 281)
- 从 GuardDuty 发现转向亚马逊Detective (p. 281)
- 使用与 GuardDuty多账户环境的集成 (p. 281)

启用集成

要使用 Amazon Detective， GuardDuty 你必须先启用亚马逊Detective。有关如何启用 Detective 的信息，请参阅《亚马逊Detective 管理指南》中的 “设置 Amazon Detecti ve”。

当您同时启用 Amaz GuardDuty on Detective ve 时，集成将自动启用。启用后，Detective 将立即采集您的 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，现有调查结果更新的导出频率为 6 小时。为确保 Detective 收到调查结果的最新更新，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 设置导出更新的有效发现的频率 (p. 202)。

从 GuardDuty 发现转向亚马逊Detective

1. 登录 https://console.aws.amazon.com/guardduty/ 控制台。
2. 从发现表中选择一项发现。
3. 从查找结果详细信息窗格中选择 “与Detective 一起调查”。
4. 选择发现的某个方面与亚马逊Detective 一起进行调查。这将为该发现或实体打开Detective 控制台。

如果数据透视表未按预期运行，请参阅 Amazon Detective 用户指南中的数据透视问题排除。

> Note
>
> 如果你在 Detecti GuardDuty ve 控制台中存档发现结果，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 GuardDuty管理多账户环境，则必须将您的成员账户添加到 Amazon Detective，才能查看这些账户中调查结果和实体的Detective 数据可视化。

建议您使用与 Detecti GuardDuty ve 的管理员帐户相同的管理员帐户。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 是一项区域服务，这意味着您必须启用 Detective 并在要使用集成的每个区域添加您的成员账户。

暂停或禁用 GuardDuty

您可以使用 GuardDuty 控制台暂停或禁用该 GuardDuty 服务。服务暂停 GuardDuty 后，您无需支付使用费用。

- 必须先取消所有可选数据源与所有区域的所有探测器的关联，然后才能暂停或禁用 GuardDuty。
- 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Amazon环境安全或生成新的发现。您的现有发现完好无损，不受 GuardDuty 暂停的影响。您可以选择 GuardDuty 稍后重新启用。
- 如果您禁用 GuardDuty，则现有发现和 GuardDuty 配置将丢失且无法恢复。如果要保存现有发现，则必须先将其导出，然后才能停止 GuardDuty。有关如何导出结果的信息，请参见导出调查结果 (p. 196)。

暂停或禁用 GuardDuty

1. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 控制台。
2. 在导航窗格中，选择 Settings (设置)。
3. 在 “暂停” GuardDuty 部分中，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. 通过 https://console.aws.amazon.com/guardduty/ 打开 GuardDuty 控制台。
2. 在导航窗格中，选择 Settings (设置)。
3. 选择 “重新启用” GuardDuty。

订阅亚马逊 SNS 公告 GuardDuty

本部分提供有关订阅 Amazon SNS（简单通知服务）以接收有关新发布的查找结果类型、现有查找类型更新和其他功能变更的通知的GuardDuty公告的信息。通知以 Amazon SNS 支持的所有格式提供。

S GuardDuty NS 会向任何已订阅的账户Amazon发送有关GuardDuty服务更新的公告。要接收有关您账户内发现情况的通知，请参阅使用 Amazon Ev CloudWatch ents 创建对GuardDuty调查结果的自定义 (p. 202)。

Note

您的 IAM 用户必须拥有订阅 SNS 的`sns::subscribe`权限。

您可以为 Amazon SQS 队列订阅此通知主题，但必须使用同一区域中的主题 ARN。有关更多信息，请参阅亚马逊简单队列服务开发人员指南中的教程：订阅 Amazon SQS 队列至 Amazon SNS 主题。

您还可以使用Amazon 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人员指南中的使用 Amazon SNS 通知调用 Lambda 函数。

每个地区的 Amazon SNS 主题 ARN 如下所示。

Amazon 区域	亚马逊 SNS 主题 ARN
us-east-1	arn:aws:sns:us-east-1:242987662583:GuardDutyAnnounc
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnounc
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnounc
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnounc
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnc
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnour
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnounc
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnounc
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnounc
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnc
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnc
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnounc

Amazon 区域	亚马逊 SNS 主题 ARN
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAr
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAr
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAr
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAr
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnour
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnounc
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnounc
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnour
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAr
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnour
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnc
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnour
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnour
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnounc
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAr
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAr
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnour
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAr

在 Amazon Web Services Management Console中订阅 GuardDuty 更新通知电子邮件

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。
2. 在区域列表中，选择与要订阅的主题 ARN 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 Create Subscription (创建订阅) 对话框中，对于 Topic ARN (主题 ARN)，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 Create subscription（创建订阅）。
7. 在您的电子邮件应用程序中，打开Amazon通知中的消息，然后打开链接以确认您的订阅。

   您的 Web 浏览器将显示来自 Amazon SNS 的确认响应。

使用 Amazon CLI 订阅 GuardDuty 更新通知电子邮件

1. 使用 Amazon 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Amazon通知中的消息，然后打开链接以确认您的订阅。

   您的 Web 浏览器将显示来自 Amazon SNS 的确认响应。

亚马逊 SNS 消息格式

有关新调查结果的示例 GuardDuty 更新通知消息如下所示：


```
{
    "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 Amazon 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" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/
V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAgHfXsit
+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/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"
```

```
}
```

解析后的消息值（删除了转义引号）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 Amazon
 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 功能更新的示例 GuardDuty 更新通知消息如下所示：

```
{
    "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_cloudtrail
\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/
V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAgHfXsit
+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/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"
}
```

解析后的消息值（删除了转义引号）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_cloudtrail"
    }]
}
```

有关更新的调查结果的示例 GuardDuty 更新通知消息如下所示：

```
{
    "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": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/
V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAgHfXsit
+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/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"
}
```

解析后的消息值（删除了转义引号）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."
    }]
}
```

亚马逊的配额 GuardDuty

您的 Amazon 账户对于每项 Amazon 服务都具有默认配额（以前称为限制）。除非另有说明，否则，每个配额是区域特定的。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 GuardDuty 的限额，请打开服务限额控制台。在导航窗格中，选择Amazon服务并选择亚马逊 GuardDuty。

要请求提高配额，请参阅 Service Quotas 用户指南中的请求增加配额。

您的Amazon账户在GuardDuty每个地区的亚马逊配额如下。

Note

有关GuardDuty恶意软件防护的特定配额，请参阅恶意软件保护配额 (p. 66)。

资源	默认值	注释
探测器	1	您可以为每个区域的每个Amazon账户创建的最大探测器资源数。 您无法请求提高配额。
Filters	100	每个区域每个Amazon账户保存的最大筛选器数量。 您无法请求提高配额。
调查结果保留期	90 天	保留调查结果的最大天数。 您无法请求提高配额。
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。 您无法请求提高配额。
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。 您无法请求提高配额。
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 您无法请求提高配额。
成员账户（通过邀请）	5000	与管理员帐户关联的最大成员帐户数。

资源	默认值	注释
成员账户	10000	与管理员帐户关联的最大成员帐户数Amazon Organizations。这包括通过邀请添加到组织的成员账户。
威胁情报集	6	每个区域的每个Amazon账户可以添加的最大威胁情报集数。 您无法请求提高配额。
可信 IP 集	1	每个区域每个Amazon账户可以上传和激活的最大可信 IP 集数量。 您无法请求提高配额。

排查中的排查 GuardDuty

当您收到与执行中的相关主题 GuardDuty，请参阅本部分的主题。

主题

- 我正在启动按需恶意软件扫描，但它导致缺少所需权限错误。 (p. 290)
- 我在使用恶意软件防护时收到iam:GetRole错误。 (p. 290)
- 我想管理多个账户，但没有所需的Amazon Organizations管理权限。 (p. 290)
- 我是一名 GuardDuty 管理员，需要启用 GuardDuty启动的恶意软件扫描，但不使用Amazon托管策略 AmazonGuardDutyFullAccess 进行管理 GuardDuty。 (p. 291)
- 其他排查中的排查中的 (p. 291)

我正在启动按需恶意软件扫描，但它导致缺少所需权限错误。

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Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)策略附加到您的 IAM 角色。

如果你是Amazon组织的成员，但仍然收到同样的错误，请连接你的管理账户。有关更多信息，请参阅Amazon OrganizationsSCP-拒绝访问 (p. 63)：

我在使用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Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)策略附加到 IAM 角色的相关主题。

我想管理多个账户，但没有所需的Amazon 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.`，则表示您缺少对组织中的多个帐户启用 GuardDuty启动的恶意软件扫描的权限。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 (p. 58)。

我是一名 GuardDuty 管理员，需要启用 GuardDuty 启动的恶意软件扫描，但不使用Amazon托管策略 AmazonGuardDutyFullAccess 进行管理 GuardDuty。

- 将您使用的 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，请参阅为恶意软件防护创建服务关联角色。
- 将的附加Amazon 托管策略：AmazonGuardDutyFullAccess (p. 266)到 IAM 中的相关主题。这将帮助您对成员帐户 GuardDuty启用启动的恶意软件扫描。

其他排查中的排查中的

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：

- 有关您访问 https://console.aws.amazon.com/guardduty/ 时出现的一般 IAM 问题，请参阅Amazon GuardDuty 身份和访问疑难解答 (p. 264)。
- 有关访问时的身份验证和授权问题AmazonAmazon Web Services Console Home，请参阅 IAM 疑难解答。

区域和终端节点

要查看亚马逊的Amazon Web Services 区域可用GuardDuty区域，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的版本中启用Amazon Web Services 区域。这样，GuardDuty 就可以生成有关未授权或异常活动的结果，甚至在您未主动使用的区域中也是如此。这还GuardDuty允许监视受支持者Amazon CloudTrail的事件Amazon Web Services 区域，其检测涉及全球服务的活动的能力会降低。

特定区域功能的可用性

区域差异列表，用于指定GuardDuty功能的可用性。

Amazon EC2 查找类型—— DefenseEvasion:EC2/UnusualDoHActivity (p. 100) 以及 DefenseEvasion:EC2/UnusualDoTActivity (p. 101)

下表显示了Amazon Web Services 区域哪里GuardDuty可用，但尚不支持这两种 Amazon EC2 查找类型。

Amazon Web Services 区域	区域代码
亚太地区（首尔）	ap-northeast-2
亚太地区（大阪）	ap-northeast-3
亚太地区（雅加达）	ap-southeast-3

GuardDuty具有区域差异的特征

下表显示了指定的GuardDuty功能可能不可用Amazon Web Services 区域。

Amazon Web Services 区域	GuardDuty 功能			
亚太地区（墨尔本）	–	可用	–	
亚太地区（海得拉巴）	可用	–	–	
欧洲（西班牙）	可用	–	–	
欧洲（苏黎世）	可用	–	–	
中东（阿联酋）	可用	–	可用	

由于这些地区的某些数据源不可用，Amazon GuardDuty API 参考中的以下 API 可能存在区域差异：

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors

- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration
- DescribeMalwareScans
- UpdateMalwareScanSettings
- GetMalwareScanSettings

Amazon GovCloud (US) 地区

有关最新信息，请参阅Amazon GovCloud (US)用户指南GuardDuty中的亚马逊。

中国区域

有关最新信息，请参阅功能可用性和实现差异。

亚马逊的文档历史记录 GuardDuty

下表描述了每个版本的GuardDuty用户指南中的重要更改。

变更	说明	日期
GuardDuty通过以下方式支持 10,000 个会员账户 Amazon Organizations	现在，GuardDuty管理员可以通过管理最多 10,000 个成员帐户 Amazon Organizations。这还包括通过邀请与GuardDuty管理员关联的最多 5000 个成员帐户。	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进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 Protection 中的 EKS 运行时监控发布了新的代理版本 1.2.0，该版本还支持基于 ARM64 的实例。增加了对 Bottlerocket 的支持。有关更多信息，请参阅 EKS 附加代理发布历史记录。	2023 年 6 月 16 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 审核日志监控（在 EKS 保护中），以监控来自 Amazon EKS 集群的 Kubernetes 审核日志，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（阿联酋）上线	EKS 保护中的 EKS 审计日志监控现已在中东（阿联酋）推出。为您的账户启用 EKS 审核日志监控，以监控来自 Amazon EKS 集群的 Kubernetes 审核日志，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恶意软件保护宣布按需恶意软件扫描	恶意软件保护可帮助您检测连接到您的 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-启动的恶意软件扫描仅在GuardDuty生成调用启动的恶意软件扫描的结果之一时，才会自动在 Amazon EBS 卷中启动无代理扫描。GuardDuty通过提供与该 Amazon EC2 实例关联的亚马逊	2023 年 4 月 27 日

	资源名称 (ARN)，您可以对账户中的 Amazon EC2 实例启动按需恶意软件扫描。有关两种扫描类型有何不同之处的更多信息，请参阅恶意软件防护。 • GuardDuty-启动恶意软件扫描 • 按需恶意软件扫描	
GuardDuty宣布推出 Lambda 保护	Lambda 保护可帮助您识别Amazon Lambda函数中的潜在安全威胁。 • Lambda 保护查找类型 (p. 147) • 修复受损的 Lambda 函数 (p. 223)	2023 年 4 月 20 日
GuardDuty现已在亚太地区（墨尔本）区域推出	将亚太地区（墨尔本）添加到可用区域列表中。Amazon Web Services 区域 GuardDuty有关该区域提供哪些功能的信息，请参阅区域和终端节点。	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 DNS 解析器和加密 DNS 技术的使用。有关哪些 Amazon Web Services 区域支持这些查找类型的信息，请参阅区域和终端节点。 • DefenseEvasion:EC2/UnusualDNSResolver (p. 100) • DefenseEvasion:EC2/UnusualDoHActivity (p. 100) • DefenseEvasion:EC2/UnusualDoTActivity (p. 101)	2023 年 4 月 5 日
GuardDuty在 EKS 保护中宣布 EKS 运行时监控	EKS 保护中的 EKS 运行时监控为Amazon环境中的 Amazon EKS 集群提供运行时威胁检测。它使用 Amazon EKS 附加代理 (`aws-guardduty-agent`) 从您的 EKS 工作负载收集运行时事件。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	亚马逊GuardDuty添加了一个新的组织配置选项，可帮助GuardDuty管理员审核和强制执行（如果需要）为ALL其组织成员启用的组织配置选项。GuardDuty现在的最佳做法是使用autoEnableOrganizationMembers而不是autoEnable。autoEnable已弃用但仍受支持。以下 API 受此新功能的影响： • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	2023 年 3 月 23 日
亚马逊的 RDS 保护功能 GuardDuty现已正式上线	GuardDutyRDS 保护会监控和分析 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Amazon Web Services 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宣布激活功能	过去，GuardDutyAPI 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仍然通过 API 支持数据源，但不会添加新的 API。功能激活会影响用于启用的 API 的行为GuardDuty或其中的保护类型GuardDuty。如果您通过 API、SDK 或 CFN 模板管理GuardDuty账户，请参阅 2023 年 3 月GuardDuty的 API 变更。	2023 年 3 月 16 日
GuardDuty恶意软件防护现已在中东（UAE）地区提供	中东（U GuardDuty AE）区域支持中的恶意软件保护功能。有关更多信息，请参阅区域和终端节点。	2023 年 3 月 13 日
亚马逊更新GuardDuty了服务相关角色 (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。 • 使用 Amazon EKS 操作来管理和检索有关 EKS 集群的信息，并管理 EKS 集群上的 EKS 插件。EKS 操作还检索与关联的标签的相关信息GuardDuty。 `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	2023 年 3 月 8 日

亚马逊更新GuardDuty了服务相关角色 (SLR)	S GuardDuty LR 已更新，允许在启用恶意软件保护后创建恶意软件保护 SLR。	2023 年 2 月 21 日
GuardDuty需要 TLS 版本 1.2 或更高版本	要与Amazon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）区域添加到可用区域列表中。Amazon Web Services 区域 GuardDuty有关更多信息，请参阅区域和终端节点。	2023 年 2 月 14 日
亚马逊GuardDuty用户指南符合 IAM 最佳实践	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 10 日
GuardDuty现已在欧洲（西班牙）区域推出	将欧洲（西班牙）添加到可用 Amazon Web Services 区域 GuardDuty位置列表中。有关更多信息，请参阅区域和终端节点。	2023 年 2 月 8 日
GuardDuty现已在欧洲（苏黎世）地区推出	将欧洲（苏黎世）添加到可用 Amazon Web Services 区域区域 GuardDuty列表中。有关更多信息，请参阅区域和终端节点。	2022 年 12 月 12 日
一项新功能的预览版 — GuardDuty RDS 保护	GuardDutyRDS 保护会监控和分析 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，它可以在五个版本中发布预览版Amazon Web Services 区域。有关更多信息，请参阅区域和终端节点。	2022 年 11 月 30 日
GuardDuty现已在中东（UAE）地区推出	将中东（UAE）添加到可用 Amazon Web Services 区域 GuardDuty位置列表中。有关更多信息，请参阅区域和终端节点。	2022 年 10 月 6 日

为一项新功能（GuardDuty恶意软件防护）添加了内容	GuardDuty恶意软件保护是亚马逊的一项可选增强功能GuardDuty。在GuardDuty识别存在风险的资源的同时，恶意软件保护会检测可能是入侵来源的恶意软件。启用恶意软件保护后，每当GuardDuty检测到 Amazon EC2 实例上的可疑行为或表明存在恶意软件的容器工作负载时，GuardDuty恶意软件保护就会对连接到受影响的 EC2 实例或容器工作负载的 EBS 卷启动无代理扫描，以检测是否存在恶意软件。要了解恶意软件保护的工作原理以及如何配置此功能，请参阅GuardDuty恶意软件防护。 • 有关恶意软件防护发现的信息，请参阅查找详情。 • 有关修复受感染的 EC2 实例和独立容器的信息，请参阅修复发现的安全问题。GuardDuty • 有关审核恶意软件扫描CloudWatch日志以及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。	2022 年 7 月 26 日
已停用一种搜索类型	Exfiltration:S3/ObjectRead.Unusual已经退休。	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 查找类型。这些查找类型可识别 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。要了解有关这些新发现的更多信息，请参阅 S3 查找类型。 • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	2022 年 7 月 5 日

添加了 GuardDuty EKS 保护内容 GuardDuty	GuardDuty现在可以通过监控 Kubernetes 审核日志为您的亚马逊 EKS 资源生成调查结果。要了解如何配置此功能，请参阅亚马逊的 EKS 保护GuardDuty。有关GuardDuty可以为 Amazon EKS 资源生成的调查结果列表，请参阅 Kubernet es 的调查结果。在 Kubernetes 发现补救指南中添加了新的补救指南，以支持修复这些发现。	2022 年 1 月 25 日
添加了 1 个新发现	添加 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS 了一个新发现。当您的Amazon环境之外的Amazon账户访问您的实例证书时，这一发现会通知您。	2022 年 1 月 20 日
更新了查找类型以帮助识别与 log4j 相关的问题 (p. 94)	亚马逊更新GuardDuty了以下发现类型，以帮助识别和优先处理与 CVE-2021-44228 和 CVE-2021-45046 相关的问题：backdoor: ec2/c&cactivity.b; backdoor: ec2/c&cactivity.b！ DNS；行为：ec2/。NetworkPortUnusual	2021年12月22日
寻找变更	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration 已更改为 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS。该调查结果的改进版本可了解使用您的凭证的典型地点，以减少通过本地网络路由的流量发现的结果。UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	2021 年 9 月 7 日
更新到GuardDuty单反相机	S GuardDuty LR已更新，增加了新的动作，以提高发现的准确性。	2021 年 8 月 3 日
为每种查找类型添加了数据源信息。	查找描述现在包含有关GuardDuty使用哪个数据源生成该查找结果的信息。	2021 年 5 月 10 日

已退出 13 种搜索类型。	13 项调查结果已停用，取而代之的是新的AnomalousBehavoir调查结果。 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, 0, 1, 2。Discovery:S3/BucketEnumeration.UnusualImpact:S3/ObjectDelete.UnusualImpact:S3/PermissionsModification.Unusual	2021 年 3 月 12 日
为异常行为添加了 8 种新的发现类型。	基于 IAM 主体的异常行为，添加了 8 种新的IAMUser查找类型。 CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior,, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior。	2021 年 3 月 12 日
添加了基于域信誉的 EC2 调查结果。	添加了 4 种基于域名信誉的新影响力查找类型。Impact:EC2/AbusedDomainRequest.Reputation，Impact:EC2/BitcoinDomainRequest.Reputation，Impact:EC2/MaliciousDomainRequest.Reputation。还为 c&cActivity 添加了一项新的 EC2 调查结果。 Impact:EC2/SuspiciousDomainRequest.Reputation	2021 年 1 月 27 日

添加了 4 种新的查找类型。	添加了 3 个新的 S3 MaliciousIPcaller 发现结果。Discovery:S3/MaliciousIPCaller，Exfiltration:S3/MaliciousIPCaller，Impact:S3/MaliciousIPCaller。 还为 c&cActivity 添加了一项新的 EC2 调查结果。 Backdoor:EC2/C&CActivity.B	2020 年 12 月 21 日
已停用UnauthorizedAccess:EC2/TorIPCaller查找类型。	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查找类型。	添加了新的影响力发现,Impact:EC2/WinRmBruteForce. 了解更多。	2020 年 9 月 17 日
添加了Impact:EC2/PortSweep查找类型。	添加了新的影响力发现,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Amazon区域列表GuardDuty中。了解更多	2020 年 7 月 31 日
为监控GuardDuty成本添加了新的使用详情。	现在，您可以使用新指标来查询您的账户和所管理账户的GuardDuty使用成本数据。新的使用成本概览可在控制台中找到，网址为https://console.aws.amazon.com/guardduty/。可以通过 API 访问更多详细信息。	2020 年 7 月 31 日
在中添加了涵盖通过S3数据事件监控进行S3保护的内容GuardDuty。	GuardDuty现在，可以通过监控 S3 数据平面事件作为新数据源来获得 S3 保护。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帐户启用新的数据源。	2020 年 7 月 31 日
添加了 14 个新的 S3 调查结果。	为 S3 控制平面和数据平面源添加了 14 种新的 S3 查找类型。	2020 年 7 月 31 日
添加了对 S3 查找结果的额外支持，并更改了 2 个现有的查找类型名称。	GuardDuty 调查结果现在包含涉及 S3 存储桶的调查结果的更多详细信息。与 S3 活动相关的现有查找类型已重命名：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Amazon Organizations整合的内容。	GuardDuty 现在与 Amazon Organizations 委派管理员集成，可让您管理组织内的 GuardDuty 账户。当您将委派管理员设置GuardDuty为GuardDuty管理员时，可以自动允许任何组织成员由委派管理员帐户进行管理。您也可以在新的 Amazon Organizations 成员账户中自动启用 GuardDuty。了解更多。	2020 年 4 月 20 日
为导出发现功能添加了内容。	添加了描述的 “导出查找结果” 功能的内容GuardDuty。	2019 年 11 月 14 日
添加了UnauthorizedAccess:EC2/MetadataDNSRebind查找类型。	添加了一个新的未经授权的发现，UnauthorizedAccess:EC2/MetadataDNSRebind。了解更多。	2019 年 10 月 10 日
添加了Stealth:IAMUser/S3ServerAccessLoggingDisabled查找类型。	添加了新的隐身发现,Stealth:IAMUser/S3ServerAccessLoggingDisabled.了解更多。	2019 年 10 月 10 日
添加了Policy:IAMUser/S3BlockPublicAccessDisabled查找类型。	添加了新的政策调查结果Policy:IAMUser/S3BlockPublicAccessDisabled。了解更多。	2019 年 10 月 10 日
已停用Backdoor:EC2/XORDDOS查找类型。	Backdoor:EC2/XORDDOS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查找类型。	PrivilegeEscalation查找类型可检测用户何时尝试为其帐户分配更高的、更宽松的权限。了解更多	2019 年 5 月 14 日
GuardDuty现已在欧洲（斯德哥尔摩）区域推出。	将欧洲（斯德哥尔摩）添加到可用Amazon区域列表GuardDuty中。了解更多	2019 年 5 月 9 日
添加了新的查找类型Recon:EC2/PortProbeEMRUnprotectedPort。	此调查结果会通知您，某个 EC2 实例上与 EMR 相关的敏感端口未被阻止或正在被积极探测。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。	这些调查结果会通知您，您环境中的 EC2 实例的行为方式可能表明它们正被用于执行拒绝服务 (DoS) 攻击。了解更多	2019 年 3 月 8 日
添加了新的查找类型：Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsage查找类型通知您，您的根用户登录凭证 Amazon Web Services 账户正用于向Amazon服务发出编程请求。了解更多	2019 年 1 月 24 日

UnauthorizedAccess:IAMUser/UnusualASNCaller查找类型已停用	UnauthorizedAccess:IAMUser/UnusualASNCaller查找类型已停用。现在，您将收到有关通过其他主动GuardDuty查找类型从异常网络调用的活动的通知。生成的调查结果类型将基于已从异常网络调用的 API 的类别。了解更多	2018 年 12 月 21 日
添加了两种新的查找类型：PenTest:IAMUser/ParrotLinux和PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux查找类型会通知你运行 Parrot Security Linux 的计算机正在使用属于你Amazon账户的证书进行 API 调用。 PenTest:IAMUser/PentooLinux查找类型会通知你运行 Pentoo Linux 的计算机正在使用属于你Amazon账户的证书进行 API 调用。了解更多	2018 年 12 月 21 日
增加了对亚马逊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、现有查找结果类型的更新和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
添加了两种新的查找类型：UnauthorizedAccess:EC2/TorClient和UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClient查找类型会通知您Amazon环境中的 EC2 实例正在与 Tor Guard 或 Authority 节点建立连接。UnauthorizedAccess:EC2/TorRelay查找类型会通知您Amazon环境中的 EC2 实例正在与 Tor 网络建立连接，这表明它充当了 Tor 中继。了解更多	2018 年 11 月 16 日
添加了新的查找类型：CryptoCurrency:EC2/BitcoinTool.B	这一发现告诉您，您的Amazon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相关的域名。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 Ev CloudWatch ents 发送通知的频率，以备后续出现的现有发现结果。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
增加了区域支持	添加了 AmazonGovCloud（美国西部）的区域支持了解更多	2018 年 7 月 25 日
增加了对 in Amazon CloudFormation StackSets 的支持 GuardDuty	您可以使用 “启用亚马逊” GuardDuty 模板在多个账户中GuardDuty同时启用。了解更多	2018 年 25 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结果抑制构建精细的自动存档规则。对于匹配自动存档规则的调查结果，GuardDuty 会自动将其标记为已存档。这使客户能够进一步调整 GuardDuty，以便仅在当前调查结果表中保留相关调查结果。了解更多	2018 年 5 月 4 日
GuardDuty在欧洲（巴黎）区域可用	GuardDuty现已在欧洲（巴黎）上线，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Amazon CloudFormation创建GuardDuty管理员和成员帐户。	有关更多信息，请参阅 `AWS::GuardDuty::master` 和 `AWS::GuardDuty::member`。	2018 年 3 月 6 日
增加了九个新的CloudTrail基于异常的检测。	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
添加了三种新的威胁情报检测（查找类型）。	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
GuardDuty会员账户限额上限。	在此版本中，每个Amazon账户（GuardDuty管理员帐户）最多可以添加 1000 个GuardDuty成员帐户。了解更多	2018 年 1 月 25 日
更改GuardDuty管理员和成员帐户的可信 IP 列表和威胁列表的上传和进一步管理。	在此版本中，来自管理员GuardDuty帐户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列表。管理员帐户上传的可信 IP 列表和威胁列表是对其成员帐户的GuardDuty功能强加的。了解更多	2018 年 1 月 25 日

早期更新

更改	说明	日期
初次发布	《亚马逊GuardDuty用户指南》的首次出版。	2017 年 11 月 28 日

Amazon词汇表

有关最新 Amazon 术语，请参阅《Amazon Web Services 一般参考》中的 Amazon 术语表。

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。