



用户指南

Amazon Detective



Amazon Detective: 用户指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 Detective ?	1
Amazon Detective 的特点	1
访问 Amazon Detective	3
Amazon Detective 的定价	4
Detective 是如何运作的 ?	4
谁在用 Detective ?	5
相关服务	5
概念和术语	7
入门	11
设置	11
注册获取 AWS 账户	11
创建具有管理访问权限的用户	12
先决条件	13
授予所需的 Detective 权限	13
支持的 AWS Command Line Interface 版本	13
建议	13
建议与 GuardDuty 和对齐 AWS Security Hub	14
GuardDuty CloudWatch通知频率的建议更新	14
启用 Detective	15
检查 Detective 是否正在摄取数据	16
行为图中的数据	18
Detective 如何填充行为图	18
Detective 如何处理源数据	19
Detective 提取	19
Detective 分析	19
新行为图的训练期	20
行为图数据结构概述	20
行为图数据结构中的元素类型	20
行为图数据结构中的实体类型	21
行为图中使用的源数据	26
Detective 中的核心数据来源类型	27
Detective 中可选数据来源的类型	27
亚马逊EKS审核日志	28
AWS 安全调查结果	29

Detective 如何摄取和存储源数据	30
Detective 如何执行行为图的数据量配额	30
摘要控制面板	32
调查	32
观察到新的地理位置	33
过去 7 天内活跃的调查发现群组	33
API通话量最大的角色和用户	33
EC2流量最大的实例	34
拥有最多 Kubernetes 容器组 (pod) 的容器集群	34
近似值通知	35
如何使用 Detective 进行调查	36
调查阶段	36
侦探调查的起点	36
检测到的结果 GuardDuty	37
AWS 由 Security Hub 汇总的安全调查结果	37
从 Detective 源数据中提取的实体	37
Detective 调查流程	37
Detective 调查	39
进行侦探调查	39
查看 Detective 调查报告	42
了解 Detective 调查报告	42
Detective 调查报告摘要	43
下载 Detective 调查报告	44
存档 Detective 调查报告	45
分析调查发现	46
调查发现概述	46
用于调查发现概述的范围时间	46
调查发现详细信息	47
相关实体	47
排查“找不到页面”问题	47
寻找群组	48
了解调查发现群组页面	49
调查发现群组的信息调查发现	50
调查发现群组配置文件	51
调查发现群组可视化	52
调查发现组摘要	54

查看调查发现组摘要	55
禁用调查发现组摘要	56
启用调查发现组摘要	57
支持的区域	57
存档 GuardDuty 调查结果	57
分析实体	59
使用实体配置文件	59
实体配置文件的范围时间	59
实体的标识符和类型	60
涉及的调查发现	60
涉及该实体的调查发现群组	60
包含实体详细信息和分析结果的配置文件面板	60
在实体配置文件中导航	61
型材面板	61
配置文件面板上的信息类型	61
配置文件面板可视化的类型	64
配置文件面板的首选项	68
导航到实体配置文件	69
从另一个控制台转向	69
使用网址进行导航	71
在 Splunk 中添加调查发现的 Detective 网址	74
转到另一个控制台	75
转到另一个实体配置文件	75
浏览活动详细信息	75
总体API通话量	76
地理位置	83
总VPC流量	85
Kubern API etes 的总体调用量	90
管理范围时间	93
设置具体的开始和结束日期和时间	94
编辑范围时间的时间长度	94
将范围时间设置为调查发现时间窗口	95
在摘要页面设置范围时间	95
查看实体的调查发现	95
大量实体	96
什么是大量实体？	96

在配置文件上查看大量实体通知	97
查看当前范围时间内的大量实体列表	97
搜索调查发现或实体	99
完成搜索	99
使用搜索结果	101
搜索故障排除	101
管理账户	102
限制和建议	102
成员账户的最大数量	102
账户和区域	103
使管理员帐户与 Security Hub 保持一致 GuardDuty	103
授予管理员账户所需的权限	103
在 Detective 中反映组织的最新动态	103
使用 Organizations 管理行为图账户	103
为组织指定 Detective 管理员账户。	104
启用组织账户作为成员账户	105
指定 Detective 管理员账户	105
指定 Detective 管理员	106
删除 Detective 管理员账号	109
账户的可用操作	111
查看账户列表	112
列出账户（控制台）	113
列出你的会员账号（DetectiveAPI，AWS CLI）	114
管理组织成员账户	115
启用新的组织账户	116
启用组织账户作为 Detective 成员账户	117
解除组织账户的关联	119
管理受邀成员账户	120
邀请个人账号加入行为图表	121
邀请成员账号列表加入行为图表	123
启用未启用的成员账户	124
删除成员账户	125
对于成员账号：管理邀请和成员资格	127
IAM成员账户的政策	127
查看行为图邀请	128
回复行为图邀请	130

从行为图中删除账户	131
账户操作的影响	132
Detective 已禁用	132
成员账户已从行为图中删除	132
成员账户退出组织	132
AWS 账户已暂停	133
AWS 账户已关闭	133
亚马逊 Detective Python 脚本	134
enableDetective.py 脚本概述	134
disableDetective.py 脚本概述	134
脚本所需的权限	135
为 Python 脚本设置运行环境	136
创建要添加或删除的 .csv 成员账户列表	138
运行 enableDetective.py	138
运行 disableDetective.py	139
Detective 与安全湖集成	141
启用集成	141
开始前的准备工作	142
第 1 步：在 Detective 中创建安全湖订阅者	143
第 2 步：添加所需的 IAM 权限	143
步骤 3：接受资源共享 ARN 邀请	146
更改 Detective 集成配置	152
支持的 AWS 区域	153
在 Detective 中查询原始日志	155
查询 AWS 角色的原始日志	157
查询 Amazon EKS 集群的原始日志	158
查询 Amazon EC2 实例的原始日志	158
禁用集成	159
删除堆 CloudFormation 栈	159
预测和监控成本	161
行为图免费试用简介	161
可选数据来源的免费试用	162
管理员账户使用情况和费用	162
每个账户摄取的数据量	162
行为图的预计费用	163
行为图的预计费用	163

源包摄取的数据量	163
成员账户使用情况跟踪	164
每个行为图的摄取量	164
各行为图的预计费用	165
Detective 如何计算预计费用	165
安全性	167
数据保护	167
密钥管理	168
身份和访问管理	169
受众	169
使用身份进行身份验证	170
使用策略管理访问	172
Amazon Detective 是如何使用的 IAM	174
基于身份的策略示例	179
AWS 托管策略	184
使用服务相关角色	194
对身份和访问进行故障排除	195
合规性验证	197
弹性	197
基础架构安全性	198
安全最佳实操	198
Detective 管理员帐户的最佳做法	198
成员账户的最佳实践	199
记录API通话	200
中的 Detective 信息 CloudTrail	200
了解 Detective 日志文件条目	201
地区和配额	203
Detective 区域和端点	203
Detective 配额	203
不支持 Internet Explorer 11 浏览器	203
管理标签	204
查看行为图的标签	204
向行为图添加标签	205
从行为图中移除标签	206
禁用 Amazon Detective	207
禁用 Detective (控制台)	207

禁用 Detective (侦探 API , AWS CLI)	207
禁用跨区域侦探 (Python 脚本已开启 GitHub)	208
文档历史记录	209
.....	ccxxix

什么是 Amazon Detective？

Amazon Detective 有助于分析、调查和快速识别安全调查发现或可疑活动的根本原因。Detective 会自动从 AWS 资源收集日志数据。然后，它使用机器学习、统计分析和图形理论生成可视化效果，帮助更快、更高效地进行安全调查。Detective 的预构建数据聚合、摘要和上下文可有助于分析和确定潜在安全问题的性质和程度。

使用 Detective，您最多可以访问一年的历史事件数据。这些数据可通过一组可视化图表显示，在选定的时间窗口内，活动的类型和数量发生了变化。Detective 将这些变化与 GuardDuty 调查结果联系起来。有关 Detective 中源数据的更多信息，请参阅[the section called “行为图中使用的源数据”](#)。

通过自动聚合数据和提供可视化工具，Amazon Detective 使您可以更快、更高效地进行安全调查。您可以快速分析潜在问题并确定安全威胁的范围。

主题

- [Amazon Detective 的特点](#)
- [访问 Amazon Detective](#)
- [Amazon Detective 的定价](#)
- [Detective 是如何运作的？](#)
- [谁在用 Detective？](#)
- [相关服务](#)

Amazon Detective 的特点

以下是 Amazon Detective 有助于调查 AWS 环境中的可疑活动和分析资源以确定安全问题的根本原因的一些关键方法。

Detective 寻找小组

Det@@@ [ective 查找组](#) 允许您检查与潜在安全事件相关的多项活动。您可以使用查找组来分析高严重性 GuardDuty 发现的根本原因。如果威胁行为者试图破坏您的 AWS 环境，他们通常会执行一系列操作，从而生成多个安全发现和异常行为。

Detective 中的查找组页面显示了从行为图中提取的所有相关查找组。有关如何利用查找组来分析安全发现的根本原因的更多信息，请参阅 Detective [中分析查找结果组](#)。

Detective 提供每个发现组的交互式可视化，以帮助您更快、更彻底地调查安全问题。该可视化旨在显示安全事件中涉及的实体和调查结果，从而更容易理解联系和根本原因。帮助您以更少的精力更快、更彻底地调查问题。“[查找结果组可视化](#)”面板显示查找结果和查找结果组中涉及的实体。

Detective 调查将对调查结果进行分类

借助 [Detective Investigation](#)，您可以使用泄露指标调查IAM用户和IAM角色，这可以帮助您确定安全事件中是否涉及资源。入侵指标 (IOC) 是在网络、系统或环境中或环境中观察到的一种伪影，它可以 (高度可信) 识别恶意活动或安全事件。借助 Detective 调查，您可以最大限度地提高效率，专注于安全威胁，并增强事件响应能力。

Detective Investigation 使用机器学习模型和威胁情报来仅发现最关键的可疑问题，从而使您能够专注于高级调查。它会自动分析您 AWS 环境中的资源，以识别潜在的泄露或可疑活动的迹象。这使您可以识别模式并了解哪些资源受到安全事件的影响，从而为识别和缓解威胁提供了一种主动的方法。

您可以使用“[运行侦探调查](#)”从 [Detective 控制台开始侦探调查](#)。要以编程方式进行调查，请使用 Detective API 的 [StartInvestigation](#) 操作。要使用 AWS Command Line Interface (AWS CLI) 运行调查，请运行 [开始调查](#) 命令。

Detective 与 Amazon 安全湖集成

[Detective 与 Amazon Security Lake](#) 集成，这意味着您可以查询和检索 Security Lake 存储的原始日志数据。通过此集成，您可以从 Security Lake 原生支持的以下来源收集日志和事件。

- AWS CloudTrail 管理事件版本 1.0 及更高版本
- 亚马逊 Virtual Private Cloud (亚马逊VPC) 流日志 1.0 及更高版本
- 亚马逊 Elastic Kubernetes Service (EKS亚马逊) 审核日志 2.0 版

将 Detective 与 Security Lake 集成后，Detective 开始从安全湖中提取与 AWS CloudTrail 管理事件和亚马逊VPC流日志相关的原始日志。您可以在 Detective 中 [查询原始日志](#) 以查看日志和事件。

调查VPC流量

借助 Detective，您可以 [交互式检查亚马逊弹性计算云 \(亚马逊VPC\) 实例和 Kubernetes 容器的虚拟私有云 \(EC2\) 网络流的活动详情](#)。Detective 会自动从您的受监控账户收集VPC流量日志，按 EC2实例汇总这些日志，并提供有关这些网络流的可视化摘要和分析。

对于EC2实例，“总VPC流量”的活动详细信息显示了选定时间范围内EC2实例与 IP 地址之间的交互情况。

对于 Kubernetes 容器，总体VPC流量显示所有目标 IP 地址的 Kubernetes 容器分配的 IP 地址的进出字节总量。

访问 Amazon Detective

Amazon Detective 在大多数版本中都可用 AWS 区域。有关目前可用 Detective 的区域列表，请参阅中的 [Amazon Detective 终端节点和配额AWS 一般参考](#)。AWS 区域 有关管理您的账户的信息 AWS 账户，请参阅AWS 账户管理 参考指南中的[指定 AWS 区域 您的账户可以使用](#)。

在每个区域，你可以通过以下任何一种方式与 Detective 合作。

AWS Management Console

AWS Management Console 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。作为该控制台的一部分，Amazon Detective 控制台提供对你的 Detective 账户、数据和资源的访问权限。您可以使用 Detective 控制台执行任何侦探任务，即查看潜在的安全威胁并分析、调查和确定安全发现的根本原因。

AWS 命令行工具

使用 AWS 命令行工具，你可以在系统的命令行中发出命令来执行 Detective 任务和 AWS 任务。与控制台相比，使用命令行更快、更方便。如果要构建执行任务的脚本，命令行工具也会十分有用。

AWS 提供了两组命令行工具：AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell。有关安装和使用的信息 AWS CLI，请参阅《[AWS Command Line Interface 用户指南](#)》。有关安装和使用的“工具”的信息 PowerShell，请参阅《[AWS Tools for PowerShell 用户指南](#)》。

AWS SDKs

AWS 由各种编程语言和平台（例如 Java、Go、Python、C++ 和 ）的库和示例代码组成。SDKs NET。它们SDKs提供了对 Detective 和其他人的便捷编程访问 AWS 服务。它们可以执行多种任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求等。有关安装和使用的信息 AWS SDKs，请参阅[构建工具 AWS](#)。

亚马逊 Detective REST API

Amazon Detective REST API 让您可以通过编程方式全面访问您的侦探账户、数据和资源。有了这个API，你可以直接向 Detective 发送HTTPS请求。但是，与 AWS 命令行工具和不同SDKs，使用 API它需要您的应用程序处理低级细节，例如生成哈希值来签署请求。有关这方面的信息API，请参阅 [Detective API 参考](#)。

Amazon Detective 的定价

与其他 AWS 产品一样，使用 Amazon Detective 没有合同或最低承诺。

Detective 的定价基于多个维度，无论来源如何，对所有数据按每 GB 的分层统一费率收费。有关更多信息，请参阅 [Amazon Detective 定价](#)。

为了帮助您了解和预测使用 Detective 的成本，Detective 提供了您账户的估计使用成本。您可以在 Amazon Detective 控制台上[查看这些估算值](#)，然后通过 Amazon Detective 进行访问API。根据您的使用服务的方式，将其他 AWS 服务 功能与某些侦探功能（例如 Security Lake 集成和 Detective Investigations）结合使用可能会产生额外费用。

首次启用 Detective 时，系统会自动注册 AWS 账户 Detective 的 30 天免费试用版。这包括作为 AWS Organizations 中组织的一部分启用的个人账户。在免费试用期间，在适用情况下使用 Detective 不收取任何费用 AWS 区域。

为了帮助您了解和预测免费试用期结束后使用 Detective 的费用，Detective 会根据您在试用期间使用 Detective 的情况为您提供估算的使用成本。您的使用数据还会显示免费试用期结束之前的剩余时间。您可以在 Amazon Detective 控制台上[查看你的 Detective 账户的使用相关数据](#)，然后通过亚马逊侦探访问这些数据API。

Detective 是如何运作的？

Detective 会自动从 Amazon 流量日志中提取基于时间的事件，例如登录尝试、API 呼叫 AWS CloudTrail 和网络 VPC 流量。它还会摄取由检测到的 GuardDuty 结果。

根据这些事件，Detective 利用机器学习和可视化效果，创建统一的交互式视图，可供了解资源行为及此类行为随时间推移的相互作用。您可以浏览此行为图来检查不同的操作，例如登录尝试失败或可疑 API 呼叫。您还可以查看这些操作如何影响诸如 AWS 账户和 Amazon EC2 实例之类的资源。您可以针对各种任务调整行为图的范围和时间轴：

- 迅速调查任何超出常规的活动。
- 确定可能表明存在安全问题的模式。
- 了解受调查发现影响的所有资源。

Detective 量身定制的可视化工具为账户信息提供了基准并对其进行了汇总。这些发现可以帮助回答诸如“这是对这个角色的不寻常 API 要求吗？”之类的问题 或者“预计该实例的流量会达到峰值吗？”

使用 Detective，无需整理任何数据，也无需开发、配置或调整自己的查询和算法。无需预付费用，只需为分析的事件付费，无需部署其他软件或订阅其他信息源。

谁在用 Detective？

某个账户启用 Detective 后，就会成为行为图的管理员账户。行为图是从一个或多个 AWS 账户中提取和分析的一组关联数据。管理员账户可以邀请成员账户向管理员账户的行为图提供数据。

Detective 还集成 AWS Organizations 了。组织管理账户为组织指定了 Detective 管理员账户。Detective 管理员账户可以将组织账户成为组织行为图中的成员账户。

有关 Detective 如何使用行为图账户中的源数据的信息，请参阅[the section called “行为图中使用的源数据”](#)。

有关管理员账户如何管理行为图的信息，请参阅[管理账户](#)。有关成员账户如何管理其行为图邀请和成员资格的信息，请参阅[the section called “对于成员账号：管理邀请和成员资格”](#)。

管理员帐户使用行为图生成的分析和可视化来调查 AWS 资源和 GuardDuty 发现。使用 Detective 与 GuardDuty 和集成 AWS Security Hub，您可以将这些服务中的 GuardDuty 发现直接切换到 Detective 控制台。

Detective 的调查侧重于与所涉 AWS 资源相关的活动。有关 Detective 调查流程的概述，请参阅《Detective 用户指南》中的[如何使用 Amazon Detective 进行调查](#)。

相关服务

为了进一步保护您的数据、工作负载和应用程序 AWS，请考虑将以下内容与 Amazon D AWS 服务 Detective 结合使用。

AWS Security Hub

AWS Security Hub 让您全面了解 AWS 资源的安全状态，并帮助您根据安全行业标准和最佳实践检查您的 AWS 环境。它的部分原因是使用、汇总、整理来自多个 AWS 服务（包括 Detective）和支持的 AWS 合作伙伴网络 (APN) 产品的安全发现并确定其优先级。Security Hub 可帮助您分析安全趋势，确定 AWS 环境中优先级最高的安全问题。

要了解有关 Security Hub 的更多信息，请参阅 [AWS Security Hub 用户指南](#)。

Amazon GuardDuty

Amazon GuardDuty 是一项安全监控服务，用于分析和处理某些类型的 AWS 日志，例如 Amazon S3 AWS CloudTrail 的数据事件日志 CloudTrail 和管理事件日志。它使用威胁情报源（例如恶意 IP 地址和域名列表）以及机器学习来识别 AWS 环境中意外且可能未经授权的恶意活动。

要了解更多信息 GuardDuty，请参阅 [Amazon GuardDuty 用户指南](#)。

Amazon Security Lake

Amazon Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动将来自 AWS 环境、SaaS 提供商、本地资源、云源和第三方来源的安全数据集中到存储在您账户中的专用数据湖中。AWS Security Lake 可以帮助您分析安全数据，让您更全面地了解整个组织的安全状况。借助 Security Lake，您还可以改善对工作负载、应用程序和数据的保护。

要了解有关安全湖的更多信息，请参阅 [Amazon 安全湖用户指南](#)。要了解有关同时使用 Detective 和 Security Lake 的更多信息，请参阅 [Detective 与安全湖集成](#)。

要了解其他 AWS 安全服务，请参阅 [上的“安全、身份和合规性”AWS](#)。

Amazon Detective 的概念和术语

以下术语和概念对了解 Amazon Detective 及其工作原理来说很重要。

管理员账户

这些区域有：AWS 账户 拥有行为图并使用行为图进行调查。

管理员账户邀请成员账户为行为图提供数据。有关更多信息，请参阅 [the section called “管理受邀成员账户”](#)。

对于组织行为图，管理员账户是组织管理账户指定的 Detective 管理员账户。有关更多信息，请参阅 [the section called “指定 Detective 管理员账户”](#)。Detective 管理员账户在组织行为图中选择要作为成员账户启用的组织账户。有关更多信息，请参阅 [the section called “管理组织成员账户”](#)。

管理员账户还可以查看行为图的数据使用情况，并从行为图中删除成员账户。

自治系统组织 (ASO)

被分配自治系统的有标题的组织。该自治系统是一个异构网络或一组使用类似路由逻辑和策略的网络。

行为图

一组由传入的源数据生成的关联数据集，该数据与一个或多个源数据相关联 AWS 账户。

每个行为图都使用相同的调查发现、实体和关系结构。

委派管理员账户 (AWS Organizations)

在 Organizations 中，服务的授权管理员账户能够管理组织对服务的使用。

在 Detective 中，除非 Detective 管理员账户是组织管理账户，否则 Detective 管理员账户也是授权管理员账户。组织管理账户不能是授权管理员账户。

在 Detective 中，允许自行授权。组织管理账户可以将自己的账户委托给 Detective 的授权管理员，但这只能在 Detective 的范围内注册或记忆，而不能在组织范围内注册或记忆。

Detective 管理员账号

组织管理账户指定为区域中组织行为图的管理员账户的账户。有关更多信息，请参阅 [the section called “指定 Detective 管理员账户”](#)。

Detective 建议组织管理账户选择除其账户之外的账户。

如果该账户不是组织管理账户，则 Detective 管理员账户也是 Detective in Organizations 的授权管理员账户。

Detective 源数据

以下各类信息源中经过处理的结构化信息：

- 日志来自 AWS 服务，例如 AWS CloudTrail 日志和 Amazon VPC 流日志
- GuardDuty 调查结果

Detective 使用 Detective 源数据填充行为图。为了支持 Detective 分析，Detective 还会存储 Detective 源数据的副本。

实体

从摄取的数据中提取的项目。

每个实体都有一个类型，用来标识它所代表的对象类型。实体类型的示例包括 IP 地址、Amazon EC2 实例和 AWS 用户。

实体可以是 AWS 您管理的资源，或与您的资源交互的外部 IP 地址。

对于每个实体，源数据也用于填充实体属性。属性值可以直接从源记录中提取，也可以跨多个记录中汇总。

调查发现

Amazon 检测到一个安全问题 GuardDuty。

调查发现群组

可能与同一事件或安全问题相关的相关调查发现、实体和证据的集合。Detective 基于内置的机器学习模型生成调查发现群组。

Detective 证据

Detective 会根据您在过去 45 天内收集的行为图中的数据，识别与调查发现群组相关的其他证据。该证据作为一项调查发现提出，其严重性值为信息。证据提供了辅助信息，突出显示了在调查发现群组内可能可疑的异常活动或未知行为。这方面的一个例子可能是新观察到的地理位置或在发现的范围内观察到的 API 呼叫。目前，这些调查发现只能在 Detective 中查看，不会发送到 Security Hub。

查找概述

提供有关调查发现的信息摘要的单个页面。

调查发现概述包含调查发现所涉及的实体列表。您可以从列表转到某个实体的配置文件。

调查发现概述还包含一个详细信息面板，其中含有调查发现属性。

大批量实体

在一段时间间隔内与大量其他实体建立联系或从大量其他实体建立连接的实体。例如，一个EC2实例可能有来自数百万个 IP 地址的连接。连接数超过了 Detective 可以容纳的阈值。

当目前范围时间包含超长时间间隔时，Detective 会通知用户。

有关更多信息，请参阅《Amazon Detective 用户指南》中的[查看大量实体的详细信息](#)。

调查

对可疑或关注的活动进行分类，确定其范围，找出其根源或起因，然后确定如何继续进行调查。

成员账户

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 AWS 账户 管理员账户被邀请向行为图贡献数据。在组织行为图中，成员账户可以是 Detective 管理员账户作为成员账户启用的组织账户。

受邀成员账号可以回复行为图邀请，并从行为图中删除自己的账户。有关更多信息，请参阅 [the section called “对于成员账号：管理邀请和成员资格”](#)。

组织账户不能更改其在组织行为图中的会成员资格。

所有成员账户还可以查看其账户在其提供数据的行为图中的使用信息。

他们没有其他访问行为图的权限。

组织行为图

Detective 管理员账户拥有的行为图。组织管理账户指定 Detective 管理员账户。有关更多信息，请参阅 [the section called “指定 Detective 管理员账户”](#)。

在组织行为图中，Detective 管理员账户控制组织账户是否为成员账户。组织账户不能从组织行为图中删除自己。

Detective 管理员账户还可以邀请其他账户访问组织行为图。

配置文件

提供与实体活动相关的数据可视化集合的单个页面。

对于调查发现，配置文件有助于分析人员确定调查发现是真正令人担忧还是误报。

配置文件提供的信息可支持对调查发现的调查或对可疑活动的全面搜寻。

配置文件面板

配置文件上的单一可视化。每个配置文件面板都旨在帮助回答一个或多个特定的问题，以协助分析人员进行调查。

配置文件面板可包含键值对、表格、时间轴、条形图或地理位置图。

关系

在各个实体之间发生的活动。关系也是从传入的源数据中提取的。

与实体类似，关系也有一个类型，用于标识所涉及的实体类型和连接方向。关系类型的一个示例是连接到 Amazon EC2 实例的 IP 地址。

范围时间

用于确定配置文件上显示的数据范围的时间窗口。

调查发现的默认范围时间反映了观察到可疑活动的第一次和最后一次时间。

实体配置文件的默认范围时间是前 24 小时。

开始使用 Amazon Detective

本教程介绍了 Amazon Detective。你将学习如何为你的 AWS 账户启用 Detective。你还将学习如何验证 Detective 是否已开始从你的 AWS 账户中提取数据并将其提取到你的行为图中。

启用 Amazon Detective 后，Detective 会创建一个以账户作为管理员账户的特定区域行为图。这是行为图中最初的唯一账户。然后，管理员账户可以邀请其他 AWS 账户将其数据贡献到行为图中。请参阅[管理账户](#)。

首次启用区域中 Detective 还可开始为期 30 天的行为图免费试用。如果该账户禁用 Detective 然后再次启用，则无法提供免费试用。请参阅[the section called “行为图免费试用简介”](#)。

免费试用期结束后，行为图中的每个账户都要为其提供的数据付费。管理员账户可以跟踪使用情况，并查看其整个行为图在典型的 30 天内的预计总费用。有关更多信息，请参阅[the section called “管理员账户使用情况和费用”](#)。成员账户可以跟踪其所属行为图的使用情况和预计费用。有关更多信息，请参阅[the section called “成员账户使用情况跟踪”](#)。

主题

- [设置您的 AWS 账户](#)
- [启用 Detective 的前提条件](#)
- [启用 Detective 的建议](#)
- [启用 Detective](#)

设置您的 AWS 账户

启用 Amazon Detective 之前，您必须有 AWS 账户。如果您没有 AWS 帐户，请完成以下步骤来创建一个帐户。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/注册>。
2. 按照屏幕上的说明操作。

在注册时，将接到电话，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 <https://aws.amazon.com/> 并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就可以使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS Management Console](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台 \)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Enabling AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Create a permission set](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [Add groups](#)。

启用 Detective 的前提条件

在启用 Detective 之前，请确保满足以下要求。

授予所需的 Detective 权限

在启用 Detective 之前，您必须确保 IAM 主体拥有所需的 Detective 权限。主体可以是已在使用的现有用户或角色，也可以创建新的用户或角色供 Detective 使用。

注册 Amazon Web Services (AWS) 后，账户将自动注册所有 AWS 服务，包括 Amazon Detective。但是，要启用和使用 Detective，您首先必须设置允许访问 Amazon Detective 控制台和 API 操作的权限。为此，您或您的管理员可以使用 AWS Identity and Access Management (IAM) 将[AmazonDetectiveFullAccess](#)托管策略附加到您的 IAM 委托人，从而授予对所有 Detective 操作的访问权限。如果没有这些 IAM 权限，则可以在 AWS 控制台中查看 Detective 入门页面。因此，在添加这些权限之前，控制台不会显示任何活动图表，即使该服务已启用。

支持的 AWS Command Line Interface 版本

要使用 AWS CLI 来执行 Detective 任务，所需的最低版本为 1.16.303。

启用 Detective 的建议

在启用 Detective 之前，请考虑遵循以下建议

建议与 GuardDuty 和对齐 AWS Security Hub

如果您已注册 GuardDuty 和 AWS Security Hub，我们建议您的账户成为这些服务的管理员帐户。如果所有三项服务的管理员账户相同，则以下集成点就能顺利运行。

- 在 O GuardDuty r Security Hub 中，在查看 GuardDuty 调查结果的详细信息时，您可以从查找结果详细信息切换到 Detective 查找配置文件。
- 在 Detective 中，在调查 GuardDuty 发现时，你可以选择将该发现存档的选项。

如果您对 GuardDuty 和 Security Hub 有不同的管理员帐户，我们建议您根据更频繁使用的服务来调整管理员帐户。

- 如果您 GuardDuty 更频繁地使用，请使用 GuardDuty 管理员帐户启用 Detective。

如果您使用管理帐户，AWS Organizations 请将 GuardDuty 管理员帐户指定为该组织的 Detective 管理员帐户。

- 如果您更频繁地使用 Security Hub，则使用 Security Hub 管理员账户启用 Detective。

如果您使用 Organizations 管理账户，请将 Security Hub 管理员账户指定为该组织的 Detective 管理员账户。

如果您无法在所有服务中使用相同的管理员账户，则在启用 Detective 后，可以选择创建跨账户角色。该角色赋予管理员账户访问其他账户的权限。

有关 IAM 如何支持此类角色的信息，请参阅 [IAM 用户指南中的向您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限](#)。

GuardDuty CloudWatch通知频率的建议更新

在中 GuardDuty，探测器配置了 Amazon CloudWatch 通知频率，用于报告发现的后续事件。这包括向 Detective 发送通知。

默认情况下，频率为 6 小时。这意味着，即使一项调查发现重复出现多次，新出现的情况也要到 6 个小时之后才会反映在 Detective 中。

为了缩短 Detective 接收这些更新的时间，我们建议 GuardDuty 管理员帐户将其探测器的设置更改为 15 分钟。请注意，更改配置不会影响使用成本 GuardDuty。

有关设置通知频率的信息，请参阅《亚马逊 GuardDuty 用户指南》中的“使用亚马逊 CloudWatch [事件监控 GuardDuty 结果](#)”。

启用 Detective

您可以通过 Detective 控制台、Detective API 或 AWS Command Line Interface 启用 Detective。

您在每个区域只能启用一次 Detective。如果您已经是该区域中某个行为图的管理员账户，则无法在该区域中再次启用 Detective。

Console

要启用 Detective (控制台)

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 选择开始。
3. 在“启用 Amazon Detective”页面上，对齐管理员账户（推荐）解释了在 Detective GuardDuty 和 Amazon 之间调整管理员账户的建议 AWS Security Hub。请参阅 [the section called “建议与 GuardDuty 和对齐 AWS Security Hub”](#)。
4. “附加 IAM 策略”按钮可将您直接带到 IAM 控制台并打开推荐的策略。您可以选择将推荐的策略附加到用于 Detective 的委托人。如您果没有在 IAM 控制台中操作的权限，则可以在所需权限中复制策略 Amazon 资源名称（ARN），将其提供给 IAM 管理员。他们可以代表您附加策略。

确认所需的 IAM 策略已落实到位。

5. 您可以通过添加标签部分向行为图添加标签。

要添加标签，请执行以下操作：

- a. 选择添加新标签。
- b. 对于键，输入标签的名称。
- c. 对于值，输入标签的值。

要删除标签，请为该标签选择删除选项。

6. 选择启用 Amazon Detective。
7. 启用 Detective 后，就可以邀请成员账户访问行为图。

要导航到账户管理页面，请选择立即添加成员。有关邀请成员账户的信息，请参阅[the section called “管理受邀成员账户”](#)。

Detective API, AWS CLI

您可以通过 Detective API 或 AWS Command Line Interface 启用 Amazon Detective。

要启用 Detective (Detective API , AWS CLI)

- Detective API：使用 [CreateGraph](#) 操作。
- AWS CLI：在命令行处，运行 [create-graph](#) 命令。

```
aws detective create-graph --tags '{"tagName": "tagValue"}
```

以下命令将启用 Detective 并将 Department 标签的值设置为 Security。

```
aws detective create-graph --tags '{"Department": "Security"}
```

Python script on GitHub

你可以使用 Detective Python 脚本启用跨区域侦探 GitHub。Detective 提供了一个开源脚本 GitHub，用于执行以下操作：

- 为指定区域列表中的管理员账户启用 Detective
- 将提供的成员账户列表添加到生成的每个行为图中
- 向成员账号发送邀请电子邮件
- 自动接受成员账户的邀请

有关如何配置和使用 GitHub 脚本的信息，请参见[the section called “亚马逊 Detective Python 脚本”](#)。

检查 Detective 是否正在从你的账户中提取数据 AWS

启用 Detective 后，它会开始从你的 AWS 账户中提取数据并将其提取到你的行为图中。

对于初始提取，数据通常会在 2 小时内出现在行为图中。

检查 Detective 是否正在提取数据的一种方法是在 Detective 搜索页面上查找示例值。

要在“搜索”页面上查看示例值

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在导航窗格中，选择搜索。
3. 从选择类型菜单中，选择一种项目类型。

数据示例包含行为图数据中选定类型标识符的样本集。

如果出现示例值，就说明数据已被采集并提取到行为图中。

Detective 行为图中的数据

在 Amazon Detective 中，可以使用 Detective 行为图中的数据进行调查。在本节中，您可以了解 Detective 行为图中使用的核心数据源，以及 Detective 如何使用源数据进行填充。

行为图是从一个或多个 Amazon Web Services (AWS) 账户采集的 Detective 源数据生成的一组关联数据。

行为图使用源数据执行以下操作。

- 全面了解系统、用户以及他们之间随着时间推移而产生的交互情况
- 对特定活动进行更详细的分析，有助于回答调查时出现的问题
- 将可能与同一事件或安全问题相关的调查发现、实体和证据集关联起来。

请注意，行为图数据的所有提取、建模和分析都是在每个单独行为图的上下文中进行的。

每个行为图表都包含来自一个或多个账户的数据。当一个账户启用 Detective 时，它会成为行为图的管理员账户，并为行为图选择成员账户。一张行为图最多可以有 1200 个成员账户。有关管理员帐户如何在行为图中管理成员帐户的信息，请参阅在 Detective [中管理帐户](#)。

内容

- [Detective 如何填充行为图](#)
- [新 Detective 行为图的培训期](#)
- [行为图数据结构概述](#)
- [Detective 行为图中使用的源数据](#)

Detective 如何填充行为图

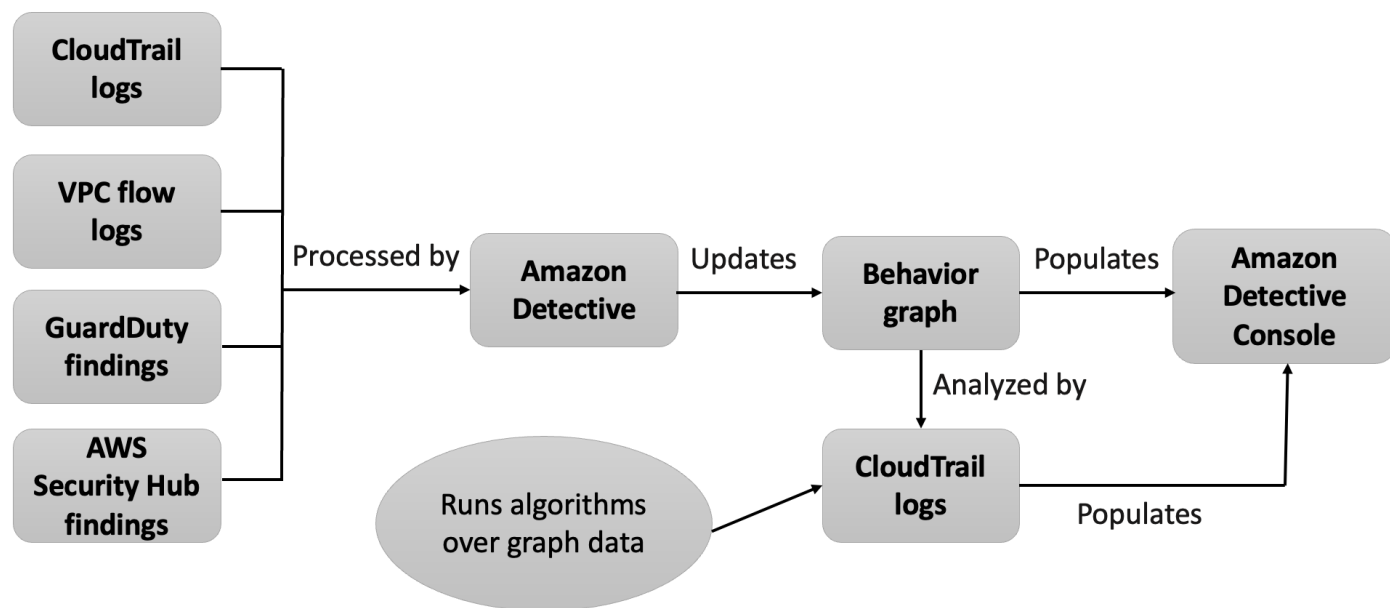
为了为调查提供原始数据，Detective 汇集了来自整个 AWS 环境及其他环境的数据，包括：

- 日志数据，包括亚马逊 Virtual Private Cloud (亚马逊VPC) 和 AWS CloudTrail
- 来自亚马逊的调查结果 GuardDuty
- 调查结果来自 AWS Security Hub

要详细了解行为图中使用的源数据，请参阅行为图[中使用的源数据](#)。

Detective 如何处理源数据

随着新数据的出现，Detective 使用提取和分析相结合的方法来填充行为图。



Detective 提取

提取根据配置的映射规则进行。映射规则基本上是说：“每当出现这段数据时，就以这种特定的方式使用它来更新行为图数据”。

例如，传入的 Detective 源数据记录可能包含一个 IP 地址。如果有，Detective 会使用该记录中的信息创建新的 IP 地址实体或更新现有的 IP 地址实体。

Detective 分析

分析是一种更复杂的算法，通过分析数据来深入了解与实体关联的活动。

例如，有一种 Detective 分析通过运行算法来分析活动发生的频率。对于进行 API 调用的实体，该算法会查找该实体通常不使用的 API 调用。该算法还会寻找 API 呼叫数量的大幅峰值。

分析见解通过为分析师的关键问题提供答案来支持调查，并且经常用于填充调查发现和实体配置文件面板。

新 Detective 行为图的培训期

一种调查发现的调查途径是将调查发现范围时间内的活动与检测到调查发现之前发生的活动进行比较。以前从未见过的活动可能更可疑。

一些 Amazon Detective 配置文件面板会突出显示在调查发现前一段时间内未观察到的活动。一些配置文件面板还显示基线值，显示范围时间之前 45 天内的平均活动。范围时间是实体在一段时间内的活动摘要。

随着越来越多的数据被提取到行为图中，Detective 就能更准确地了解组织中哪些活动是正常的，哪些活动是不正常的。

但是，要创建这张图，Detective 需要访问至少两周的数据。Detective 分析的成熟度也会随着行为图中账户数量的增加而增加。

激活 Detective 后的前两周被视为训练期。在此期间，将范围时间活动与之前的活动进行比较的配置文件面板会显示一条信息，表明 Detective 正在接受训练。

在试用期内，Detective 建议您在行为图中添加尽可能多的成员帐户。这为 Detective 提供了更大的数据池，使其能够更准确地了解组织的正常活动。

行为图数据结构概述

行为图数据结构定义了提取和分析数据的结构。它还定义了如何将源数据映射到行为图。

行为图数据结构中的元素类型

行为图数据结构由以下信息元素组成。

实体

实体表示从 Detective 源数据中提取的项目。

每个实体都有一个类型，用来标识它所代表的对象类型。实体类型的示例包括 IP 地址、Amazon EC2 实例和 AWS 用户。

对于每个实体，源数据也用于填充实体属性。属性值可以直接从源记录中提取，也可以跨多个记录中汇总。

某些属性由单个标量值或集合值组成。例如，对于一个 EC2 实例，Detective 会跟踪实例的类型和处理的总字节数。

时间序列属性可追踪一段时间内的活动。例如，Detect EC2 实例会随着时间的推移跟踪其使用的唯一端口。

关系

关系表示各个实体之间发生的活动。关系也是从 Detective 源数据中提取的。

与实体类似，关系也有一个类型，用于标识所涉及的实体类型和连接方向。关系类型的一个示例是连接到 EC2 实例的 IP 地址。

对于每个单独的关系，例如连接到特定实例的特定 IP 地址，Detective 会跟踪一段时间内的发生情况。

行为图数据结构中的实体类型

行为图数据结构由执行以下操作的实体和关系类型组成：

- 跟踪正在使用的服务器、IP 地址和用户代理
- 跟踪正在使用的 AWS 用户、角色和帐户
- 跟踪 AWS 环境中的网络连接和授权情况

行为图数据结构包含以下实体类型。

AWS 帐户

AWS Detective 源数据中存在的帐户。

对于每个帐户，Detective 都会回答几个问题：

- 该帐户使用了哪些 API 调用？
- 该帐户使用了哪些用户代理？
- 该帐户使用了哪些自治系统组织 (ASOs)？
- 该帐户在哪些地理位置处于活跃状态？

AWS 角色

AWS 存在于 Detective 源数据中的角色。

对于每个角色，Detective 都会回答几个问题：

- 该角色使用了什么 API 电话？
- 该角色使用了哪些用户代理？

- 这个角色使用ASOs了什么？
- 该角色在哪些地理位置处于活跃状态？
- 哪些资源代入了该角色？
- 该角色扮代入了哪些角色？
- 该角色涉及哪些角色环节？

AWS 用户

AWS 存在于 Detective 源数据中的用户。

对于每个用户，Detective 都会回答几个问题：

- 用户使用了哪些API电话？
- 该用户使用了哪些用户代理？
- 该用户在哪些地理位置处于活跃状态？
- 该用户代入了哪些角色？
- 该用户涉及哪些角色环节？

联合用户

联合用户的实例。联合用户的示例包括：

- 使用安全断言标记语言登录的身份 () SAML
- 使用网络身份联合验证登录的身份

对于每位联合用户，Detective 都会回答以下问题：

- 该联合用户是通过哪个身份提供商进行身份验证的？
- 该联合用户的受众有哪些？受众可以识别请求联合用户的网络身份令牌的应用程序。
- 该联合用户在哪些地理位置处于活跃状态？
- 该联合用户使用了哪些用户代理？
- 联合用户使用ASOs了什么？
- 该联合用户代入了哪些角色？
- 该联合用户涉及哪些角色环节？

EC2实例

EC2Detective 源数据中存在的实例。

例如，EC2Detective 回答了几个问题：

- 哪些 IP 地址与实例进行了通信？

- 使用了哪些端口与实例通信？
- 从实例发送和接收的数据量是多少？
- 实例VPC包含什么？
- 该EC2实例使用了哪些API调用？
- 该EC2实例使用了哪些用户代理？
- 该EC2实例使用ASOs了什么？
- 该EC2实例在哪些地理位置处于活动状态？
- 该EC2实例扮演了什么角色？

角色会话

代入角色的资源的实例。每个角色会话都由角色标识符和会话名称标识。

对于每个角色，Detective 都会回答几个问题：

- 该角色会话涉及哪些资源？换句话说，代入了什么角色，什么资源代入了该角色？

请注意，对于跨账户的角色代入，Detective 无法识别代入该角色的资源。

- 角色会话API使用了哪些调用？
- 该角色会话使用了哪些用户代理？
- 角色会话使用ASOs了什么？
- 该角色会话在哪些地理位置处于活跃状态？
- 哪个用户或角色开始了该角色会话？
- 哪些角色会话是从该角色会话开始的？

调查发现

亚马逊发现的调查结果 GuardDuty 已输入到Detective的源数据中。

对于每项调查发现，Detective 都会跟踪调查发现类型、来源和调查发现活动的时间窗口。

它还会存储与调查发现有关的特定信息，例如检测到的活动中涉及的角色或 IP 地址。

IP 地址

Detective 源数据中存在的 IP 地址。

对于每个 IP 地址，Detective 都会回答几个问题：

- 该地址使用了哪些API电话？
- 地址使用了哪些端口？

- 哪些用户和用户代理使用了 IP 地址？
- IP 地址在哪些地理位置处于活跃状态？
- 此 IP 地址已分配给哪些EC2实例并与哪些实例通信？

S3 存储桶

Detective 源数据中的 S3 存储桶。

对于每个 S3 存储桶，Detective 都会回答以下问题：

- 哪些主体与 S3 存储桶进行了交互？
- 对 S3 存储桶进行了哪些API调用？
- 委托人从哪些地理位置API调用 S3 存储桶？
- 使用了哪些用户代理与 S3 存储桶进行交互？
- 用来ASOs与 S3 存储桶交互的是什么？

可以删除 S3 存储桶，然后使用相同名称创建新的存储桶。由于 Detective 使用 S3 存储桶名称来标识 S3 存储桶，因此它将这些存储桶视为单个 S3 存储桶实体。在实体配置文件中，创建时间是第一次创建时间。删除时间是最近的删除时间。

要查看所有创建和删除事件，请将范围时间设置为以创建时间开始，以删除时间结束。在总体API通话量配置文件面板上，显示示波器时间的活动详细信息。筛选要显示的API方法Create和Delete方法。请参阅 [the section called “总体API通话量”](#)。

用户代理

Detective 源数据中存在的用户代理。

对于每个用户代理，Detective 都会回答以下问题：

- 用户代理使用了哪些API电话？
- 哪些用户和角色使用了用户代理？
- 哪些 IP 地址使用了用户代理？

EKS集群

EKSDetective 源数据中存在的集群。

Note

要查看此实体类型的完整详细信息，必须启用可选的EKS审核日志数据源。有关更多信息，请参阅[可选数据来源](#)

对于每个EKS集群，Detective 都会回答以下问题：

- 在这个集群中运行了哪些 Kubernetes API 调用？
- 此集群中有哪些 Kubernetes 用户和服务账号（主体）处于活跃状态？
- 此集群中启动了哪些容器？
- 使用哪些映像来启动该群集中的容器？

Kubernetes 容器组（pod）

Detective 源数据中存在的 Kubernetes 容器组（pod）。

Note

要查看此实体类型的完整详细信息，必须启用可选的EKS审核日志数据源。有关更多信息，请参阅[可选数据来源](#)

对于每个容器组（pod），Detective 都会回答以下问题：

- 该容器组（pod）中的哪些容器映像在我的账户中很常见？
- 针对该容器组（pod）有哪些活动？
- 该容器组（pod）中运行了哪些容器？
- 该容器组（pod）中容器的注册表在我的账户中是否常见？
- 工作负载的其他容器组（pod）中还运行着哪些容器？
- 该容器组（pod）中是否有工作负载的其他容器组（pod）中没有的异常容器？

容器映像

Detective 源数据中存在的容器映像。

Note

要查看此实体类型的完整详细信息，必须启用可选的EKS审核日志数据源。有关更多信息，请参阅[可选数据来源](#)

对于每个容器映像，Detective 都会回答以下问题：

- 我的环境中有哪些其他映像与此映像共享相同的存储库或注册表？

- 我的环境中正在运行该映像的多少副本？

Kubernetes 主题

Detective 源数据中存在的 Kubernetes 主题。Kubernetes 主题是用户或服务账户。

Note

要查看此实体类型的完整详细信息，必须启用可选的EKS审核日志数据源。有关更多信息，请参阅[可选数据来源](#)

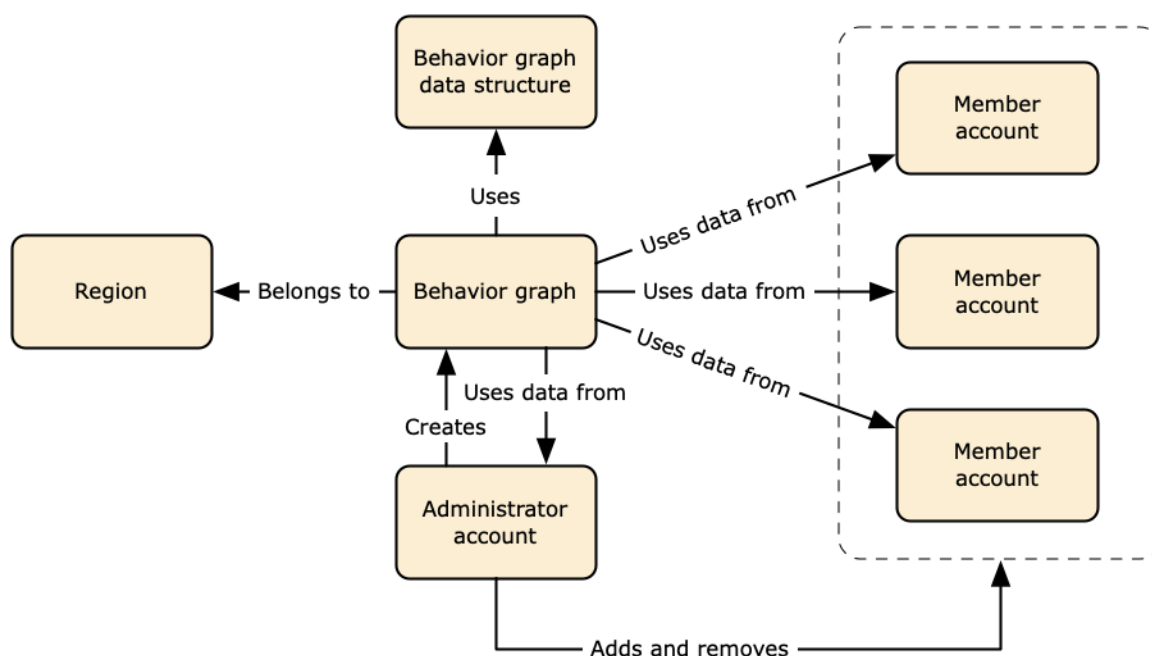
对于每个主题，Detective 都会回答以下问题：

- 哪些IAM校长被认证为这个主体？
- 哪些调查发现与该主题相关联？
- 该主题使用的是哪些 IP 地址？

Detective 行为图中使用的源数据

要填充行为图，Amazon Detective 会使用来自行为图管理员账户和成员账户的源数据。

使用 Detective，您最多可以访问一年的历史事件数据。这些数据可通过一组可视化图表显示，在选定的时间窗口内，活动的类型和数量发生了变化。Detective 将这些变化与 GuardDuty 调查结果联系起来。



有关行为图数据结构的详细信息，请参阅《Detective 用户指南》中的[行为图数据结构概述](#)。

Detective 中的核心数据来源类型

Detective 从以下类型的 AWS 日志中提取数据：

- AWS CloudTrail 日志
- 亚马逊 Virtual Private Cloud (亚马逊VPC) 流日志
 - 同时摄取IPv4和IPv6记录，但不采集由 Elastic Fabric Adapter MAC s 生成的记录。
 - 当log-status字段的值处于OK状态时提取日志记录。有关更多信息，请参阅 Amazon VPC 用户指南中的[流日志记录](#)。
 - VPCs仅提取在这些实例中运行的 Amazon 弹性计算云实例生成的流日志。不使用其他资源，例如 NAT网关、RDS实例或 Fargate 集群。
 - 提取已接受和已拒绝的流量。
- 对于注册的账户，Detective 还会摄取 GuardDuty 调查结果。GuardDuty

Detective 使用独立 CloudTrail 且重复的VPC流和流日志以及流日志来消耗 CloudTrail 和VPC流日志事件。这些流程不会影响或使用您的现有配置 CloudTrail 和VPC流日志配置。它们也不会影响这些服务的性能或增加费用。

Detective 中可选数据来源的类型

除了 Detective 核心包中提供的三个数据源（核心包包括 AWS CloudTrail 日志、VPC流程日志和 GuardDuty调查结果）外，Detective 还提供可选的源包。可随时启动或停止行为图的可选数据来源包。

Detective 为每个区域的所有核心和可选源包提供 30 天的免费试用。

Note

Detective 会保留从每个数据来源包收到的所有数据，最多保留 1 年。

目前提供以下可选源包：

- EKS 审计日志

这个可选的数据源包允许 Detective 获取有关您环境中EKS集群的详细信息，并将这些数据添加到您的行为图中。Detective 将用户活动与AWS CloudTrail 管理事件关联起来，将网络活动与 Amazon VPC Flow Logs 关联起来，无需您手动启用或存储这些日志。有关详细信息，请参阅 [亚马逊EKS审核日志](#)。

- AWS 安全调查结果

该可选数据来源包允许 Detective 从 Security Hub 获取数据，并将这些数据添加到行为图中。有关详细信息，请参阅 [AWS 安全调查结果](#)。

启动或停止可选数据来源：

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 从设置下的导航面板选择常规。
3. 在可选源包下，选择更新。然后选择要启用的数据来源，或取消选择已启用数据来源的复选框，并选择更新来更改已启用的数据来源包。

 Note

如果停止并重新启动可选数据来源，某些实体配置文件上显示的数据会出现空白。控制台显示屏上将显示这一空白，代表数据来源停止的时间段。重新启动数据来源时，Detective 不会追溯摄取数据。

亚马逊EKS审核日志

Amazon EKS 审计日志是一个可选的数据源包，可以添加到您的 Detective 行为图中。你可以从控制台的“设置”页面或通过 Detective 查看可用的可选源包及其在账户中的状态API。

该数据来源提供 30 天免费试用。要了解更多信息，请参阅[可选数据来源的免费试用](#)。

启用 Amazon EKS 审计日志允许 Detective 将有关使用亚马逊创建的资源的深入信息EKS添加到您的行为图中。该数据源增强了所提供的有关以下实体类型的信息：EKS集群、Kubernetes Pod、容器镜像和 Kubernetes 主题。

此外，如果您在 Amazon 中启用了EKS审计日志作为数据源，GuardDuty 则可以从中查看 Kubernetes 调查结果的详细信息。GuardDuty有关启用此数据源的更多信息，GuardDuty 请参阅亚马逊中的[Kubernetes 保护。GuardDuty](#)

Note

2022 年 7 月 26 日之后创建的新行为图默认启用此数据来源。对于 2022 年 7 月 26 日之前创建的行为图，必须手动启用。

添加或删除作为可选数据源的 Amazon EKS 审计日志：

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 从设置下的导航面板选择常规。
3. 在“源包”下，选择EKS审核日志以启用此数据源。如果已启用，请再次选择它以停止将EKS审核日志提取到您的行为图中。

AWS 安全调查结果

AWS 安全发现是一个可选的数据源包，可以添加到你的 Detective 行为图中。

你可以从控制台的“设置”页面或通过 Detective 查看可用的可选源包及其在账户中的状态API。

该数据来源提供 30 天免费试用。要了解更多信息，请参阅[可选数据来源的免费试用](#)。

启用AWS 安全调查结果允许 Detective 使用由 Security Hub 从上游服务中汇总的 Security Hub 发现结果，采用一种称为AWS安全格式 (ASFF) 的标准调查结果格式，从而无需进行耗时的数据转换工作。然后，它将从各个产品摄取的调查发现进行关联，以确定最重要问题的优先级。

添加或删除 AWS 安全发现作为可选数据源：

Note

2023 年 5 月 16 日之后创建的新行为图默认启用 AWS 安全发现数据源。对于 2023 年 5 月 16 日之前创建的行为图，必须手动启用。

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 从设置下的导航面板选择常规。
3. 在“源包”下，选择 AWS 安全发现以启用此数据源。如果已启用，请再次选择该选项，以停止将 AWS安全调查结果格式 (ASFF) 结果提取到您的行为图中。

目前支持的调查发现

Detective从亚马逊拥有的服务中提取Security Hub中的所有ASFF发现，或者 AWS。

- 要查看支持的服务集成列表，请参阅 AWS Security Hub 用户指南中的[可用AWS服务集成](#)。
- 有关支持的资源列表，请参阅《AWS Security Hub 用户指南》中的[资源](#)。
- AWS 未将合规状态设置为FAILED且跨区域汇总结果的服务调查结果不会被采集。

Detective 如何摄取和存储源数据

启用 Detective 后，Detective 会开始从行为图管理员账户摄取源数据。当成员账户被添加到行为图中时，Detective 也开始使用来自这些成员账户的数据。

Detective 源数据由结构化和经过处理的原始信息源版本组成。为了支持 Detective 分析，Detective 会存储 Detective 源数据的副本。

Detective 将流程信息源数据摄取到 Detective 源数据存储中的 Amazon Simple Storage Service (Amazon S3) 存储桶中。当新的源数据到达时，其他 Detective 组件会接收数据并开始提取和分析流程。有关更多信息，请参阅《Detective 用户指南》中的[Detective 如何使用源数据填充行为图](#)。

Detective 如何执行行为图的数据量配额

Detective 对每个行为图的数据量都有严格的配额限制。数据量是指每天流入 Detective 行为图的数据量。

当管理员账户启用 Detective 和成员账户接受邀请加入行为图时，Detective 就会执行这些配额。

- 如果管理员账户每天的数据量超过 10 TB，则管理员账户无法启用 Detective。
- 如果成员账户增加的数据量会导致行为图每天超过 10 TB，则无法启用该成员账户。

行为图的数据量也可以随着时间的推移而自然增长。Detective 每天都会检查行为图的数据量，确保其不超过配额。

如果行为图数据量接近配额，Detective 会在控制台显示一条警告消息。为避免超出配额，可以删除成员账户。

如果行为图数据量每天超过 10 TB，则无法在行为图中添加新的成员账户。

如果行为图数据量每天超过 15 TB，则 Detective 就会停止向行为图中摄取数据。每天 15 TB 的配额既反映了正常的数据量，也反映了数据量的峰值。达到此配额后，不会向行为图摄取任何新数据，但不会

删除现有数据。仍可以使用这些历史数据进行调查。控制台会显示一条消息，说明行为图的数据摄取已暂停。

如果数据采集已暂停，则必须与合作 支持 才能将其重新启用。如果可能，在联系之前 支持，请尝试删除成员帐户，以使数据量低于配额。这样就能更轻松地重新启用行为图的数据摄取。

使用 Detective 摘要仪表板

使用 Amazon Detective 中的“摘要”控制面板来识别需要调查过去 24 小时内活动起源的实体。Amazon Detective 摘要控制面板可帮助您识别与特定类型的异常活动相关的实体。这是调查的几个可能起点之一。

要显示“摘要”面板，请在 Detective 导航窗格中选择“摘要”。首次打开 Detective 控制台时，也会默认显示“摘要”控制台。

在“摘要”仪表板中，您可以识别符合以下条件的实体：

- 显示 Detective 发现的潜在安全事件的调查
- 与在新观察到的地理位置中发生的活动相关的实体
- API 拨打电话次数最多的实体
- EC2 流量最大的实例
- 容器数量最多的容器集群

在每个“摘要”仪表板面板中，您可以透视到选定实体的配置文件。

查看摘要仪表板时，您可以调整范围时间，以查看过去 365 天内任何 24 小时时间范围内的活动。更改开始日期和时间后，结束日期和时间会自动更新为所选开始时间后的 24 小时。

使用 Detective，您最多可以访问一年的历史事件数据。这些数据可通过一组可视化图表显示，在选定的时间窗口内，活动的类型和数量发生了变化。Detective 将这些变化与 GuardDuty 调查结果联系起来。

有关 Detective 中源数据的更多信息，请参见[行为图中使用的源数据](#)。

调查

调查向您显示 Detective 发现的潜在安全事件。在“调查”面板上，您可以查看关键调查以及在设定的一段时间内受到安全事件影响的相应 AWS 角色和用户。调查汇总了泄露指标，以帮助确定 AWS 资源是否参与了可能表明恶意行为及其影响的异常活动。

选择查看所有调查，以查看调查发现、分类调查发现组和资源详细信息，从而加速安全调查。根据所选的时间范围显示调查。您可以调整时间范围，以便查看过去 365 天的 24 小时调查。您可以直接转至关键调查，查看详细的调查报告。

如果您发现某个 AWS 角色或用户似乎有可疑活动，则可以直接从“调查”面板切换到该角色或用户以继续调查。转到角色或用户，然后单击进行调查以生成调查报告。针对角色或用户运行调查后，该角色或用户将移至已调查选项卡。

观察到新的地理位置

新观察到的地理位置突出显示了在过去 24 小时内发生活动的地理位置，但在此之前的基线时间段内没有观察到这些地理位置。

该面板最多可包含 100 个地理位置。这些地点在地图上标记，并在地图下方的表格中列出。

对于每个地理位置，该表显示了过去 24 小时内从该地理位置API拨出的失败和成功呼叫的次数。

您可以展开每个地理位置以显示从该地理位置拨API打电话的用户和角色列表。该表列出了每个主体的类型和关联的 AWS 账户。

如果您发现某个用户或角色似乎可疑，则可以直接从面板转到用户或角色配置文件，继续进行调查。要转到某个配置文件，请选择用户或角色标识符。

Detective 使用 MaxMind GeoIP 数据库确定请求的位置。MaxMind 尽管准确性因国家和知识产权类型等因素而异，但它们在国家一级的数据的准确性非常高。有关的更多信息 MaxMind，请参阅 [MaxMind IP 地理定位](#)。如果您认为任何 GeoIP 数据不正确，可以通过“更正地理数据”向 Maxmind 提交 [MaxMind 正](#) 请求。IP2

过去 7 天内活跃的调查发现群组

过去 7 天内活跃的调查发现群组会显示在设定时间段内发生在环境中的 Detective 调查发现、实体和证据的相关群组。这些分组与可能表明恶意行为的异常活动相关联。摘要仪表板最多显示五个小组，按包含上周活跃的最关键发现的组进行排序。

您可以选择策略、账户、资源和调查发现内容中的值，查看更多详细信息。

每天都会生成调查发现群组。如果您确定了相关的调查发现群组，则可以选择标题转到群组配置文件的详细视图，继续进行调查。

API通话量最大的角色和用户

API呼叫量最大的角色和用户标识了在过去 24 小时内API拨打的呼叫次数最多的用户和角色。

该面板最多可包含 100 个用户和角色。可能会出现每个用户或角色的类型（用户或角色）和关联的账户。您还可以查看该用户或角色在过去 24 小时内发出的 API 呼叫数。

默认情况下，会显示与服务相关联的角色。与服务相关的角色可能会产生大量 AWS CloudTrail 活动，这会取代您要进一步调查的主人。您可以选择关闭“显示服务相关角色”，从摘要仪表板视图中筛选出与服务相关的角色。

您可以导出包含此面板中数据的逗号分隔值 (.csv) 文件。

还有过去 7 天的 API 通话量时间表。时间表可以帮助您确定该委托人的 API 通话量是否异常。

如果您发现某个用户或角色的 API 通话量可能令人怀疑，则可以直接从面板切换到用户或角色配置文件以继续调查。您还可以查看与用户或角色关联的账户配置文件。要查看某个配置文件，请选择用户、角色或账户标识符。

EC2 流量最大的实例

EC2 流量最大的实例标识了在过去 24 小时内总流量最大的 EC2 实例。

该面板最多可以包含 100 个 EC2 实例。对于每个 EC2 实例，您可以查看关联的账户以及过去 24 小时的入站字节数、出站字节数和总字节数。

您可以导出包含该面板中数据的逗号分隔值 (.csv) 文件。

还可能出现显示过去 7 天的入站和出站流量的时间轴。时间轴可以帮助确定该 EC2 实例的流量是否异常。

如果您发现某个 EC2 实例的流量可疑，则可以直接从面板进入 EC2 实例配置文件以继续调查。您还可以查看拥有该 EC2 实例的账户的个人资料。要查看个人资料，请选择 EC2 实例或账户标识符。

拥有最多 Kubernetes 容器组 (pod) 的容器集群

创建 Kubernetes 容器组 (pod) 最多的容器集群可确定在过去 24 小时内运行容器最多的集群。

该面板包括多达 100 个集群，按与之关联的调查发现最多的集群排列。对于每个集群，您可以查看关联的账户、该集群中的当前容器数量以及过去 24 小时内与该集群关联的调查发现数量。您可以导出包含该面板中数据的逗号分隔值 (.csv) 文件。

如果您发现某个集群有最新调查发现，则可以直接从面板转到集群配置文件，继续进行调查。您还可以转到拥有集群的账户的配置文件。要转到配置文件，请选择集群名称或账户标识符。

近似值通知

对于API呼叫量最大的角色和用户以及流量最大的EC2实例，如果值后跟星号 (*)，则表示该值是近似值。真实值等于或大于显示值。

出现这种情况是因为 Detective 使用了一种方法来计算每个时间间隔的流量。在摘要页面上，时间间隔为一小时。

Detective 会计算每小时容量最大的 1,000 个用户、角色或EC2实例的总容量。它不包括其余用户、角色或EC2实例的数据。

如果某个资源有时在前 1000 名，有时不在前 1000 名，则该资源的计算流量可能不包括所有数据。不包括未进入前 1000 名的时间间隔的数据。

请注意，这仅适用于摘要页面。用户、角色或EC2实例的配置文件提供了精确的详细信息。

如何使用 Detective 进行调查

Amazon Detective 可轻松分析、调查和快速识别安全调查发现或可疑活动的根本原因。Detective 提供了支持整个调查过程的工具。Detective 中的调查可以从调查发现、调查发现群组或实体开始。

Detective 的调查阶段

任何 Detective 调查过程都涉及以下阶段：

分类

收到有关恶意或高风险活动的可疑实例时，调查过程就开始了。例如，您被指派调查亚马逊 GuardDuty 和 Amazon Inspector 等服务发现的结果或警报。

在分类阶段，要确定您认为该活动是真阳性（真正的恶意活动）还是假阳性（非恶意或高风险活动）。通过深入了解相关实体的活动，Detective 配置文件可为分类流程提供支持。

对于真阳性的实例，您可以继续进入下一阶段。

范围界定

在范围界定阶段，分析人员要确定恶意或高风险活动的范围以及根本原因。

范围界定可以回答以下类型的问题：

- 哪些系统和用户受到了威胁？
- 攻击的源头在哪里？
- 攻击持续了多长时间？
- 还有其他相关活动需要发现吗？例如，如果攻击者正在从系统中提取数据，他们是如何获得这些数据的？

Detective 可视化有助于确定涉及或受影响的其他实体。

响应

最后一步是对攻击做出响应，以阻止攻击，将损失降到最低，并防止类似攻击再次发生。

侦探调查的起点

Detective 中的每一项调查都有一个基本的出发点。例如，您可能被分配一个要调查的 Amazon GuardDuty 或 AWS Security Hub 调查结果。或者，您可能担心某个 IP 地址会出现异常活动。

调查的典型起点包括检测到的调查结果 GuardDuty 和从 Detective 源数据中提取的实体。

检测到的结果 GuardDuty

GuardDuty 使用您的日志数据来发现可疑的恶意或高风险活动实例。Detective 提供的资源有助于您调查这些调查发现。

对于每项调查发现，Detective 都会提供关联的调查发现详细信息。Detective 还显示了与调查结果相关的实体，例如 IP 地址和 AWS 账户。

然后，您就可以浏览相关实体的活动，以确定从调查发现中检测到的活动是否真正令人担忧。

有关更多信息，请参阅 [the section called “调查发现概述”](#)。

AWS 由 Security Hub 汇总的安全调查结果

AWS Security Hub 将来自不同调查结果提供者的安全调查结果汇总到一个地方，并为您提供中 AWS 安全状态的全面视图。Security Hub 消除了处理来自多个提供商的大量调查发现的复杂性。它可以减少管理和提高所有 AWS 账户、资源和工作负载安全所需的精力。Detective 提供的资源有助于您调查这些调查发现。

对于每项调查发现，Detective 都会提供关联的调查发现详细信息。Detective 还显示了与调查结果相关的实体，例如 IP 地址和 AWS 账户。

有关更多信息，请参阅 [the section called “调查发现概述”](#)。

从 Detective 源数据中提取的实体

Detective 从摄取的 Detective 源数据中提取 IP 地址和 AWS 用户等实体。您可以使用其中一个作为调查出发点。

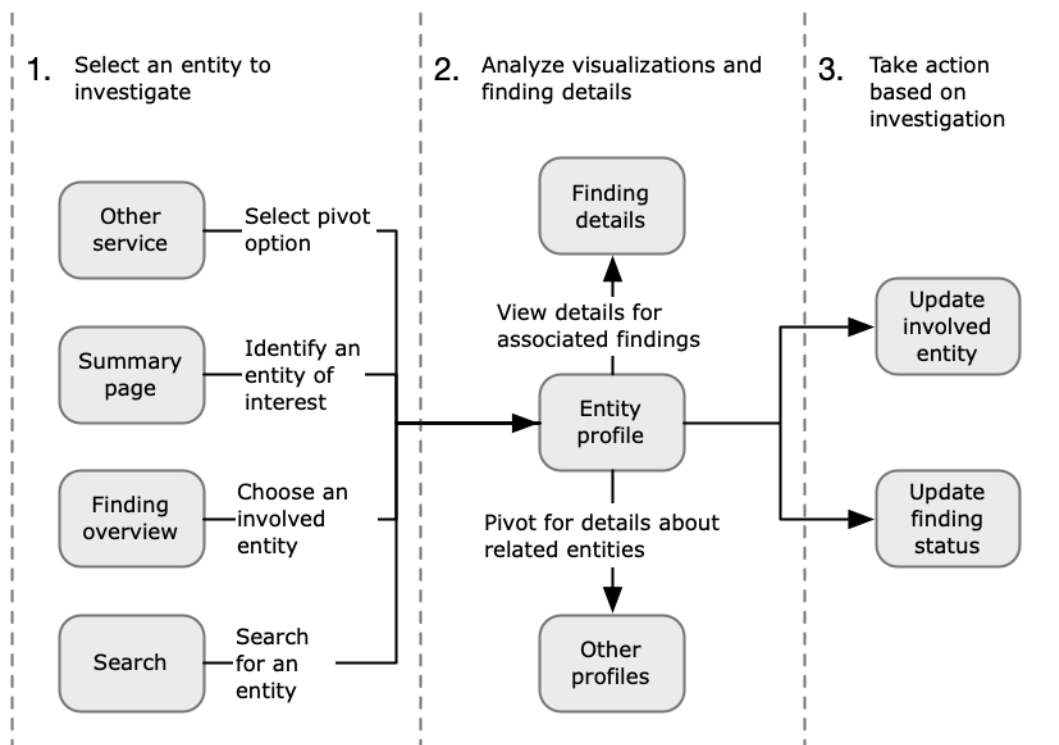
Detective 提供有关该实体的一般详细信息，例如 IP 地址或用户名。它还提供了有关活动历史记录的信息。例如，Detective 可以报告某个实体已连接、被连接或使用的其他 IP 地址。

有关更多信息，请参阅 [分析实体](#)。

Detective 调查流程

您可以使用 Amazon Detective 来调查实体，例如 EC2 实例或 AWS 用户。您也可以调查安全调查发现。

简而言之，下图显示了 Detective 调查的过程。



第 1 步：选择要调查的实体

在查看调查结果时 GuardDuty，分析师可以选择在 Detective 中调查关联实体。请参阅 [the section called “从另一个控制台转向”](#)。

选择实体后，您将进入 Detective 中的实体配置文件。

第 2 步：分析配置文件的可视化内容

每个实体配置文件都包含一组从行为图生成的可视化内容。行为图是根据输入到 Detective 的日志文件和其他数据创建的。

可视化内容显示与实体相关的活动。您可以使用这些可视化内容回答问题，以确定实体活动是否异常。请参阅 [分析实体](#)。

为了帮助指导调查，您可以使用为每种可视化内容提供的 Detective 指南。该指南概述了所显示的信息，提出了供询问的问题，并根据答案提出了后续步骤。请参阅 [the section called “使用配置文件面板指南”](#)。

每个配置文件都包含关联调查发现的列表。您可以查看调查发现的详细信息，也可以查看调查发现概述。请参阅 [the section called “查看实体的调查发现”](#)。

您可以从实体配置文件转到其他实体和调查发现配置文件，进一步调查相关资产的活动。

第 3 步：采取措施

根据调查结果，采取适当措施。

对于假阳性调查发现，您可以将其存档。在 Detective 中，您可以存档 GuardDuty 调查结果。有关更多详情，请参阅[存档 Amazon GuardDuty 调查结果](#)。

否则，您需要采取适当措施来解决漏洞问题并减轻损失。例如，您可能需要更新某个资源的配置。

Detective 调查

您可以使用 Amazon Detective Investigation 使用泄露指标来调查 IAM 用户和 IAM 角色，这可以帮助您确定安全事件中是否涉及资源。入侵指标 (IOC) 是在网络、系统或环境中或环境中观察到的一种伪影，它可以 (高度可信) 识别恶意活动或安全事件。借助 Detective Investigations，您可以最大限度地提高效率，专注于安全威胁，并增强事件响应能力。

Detective Investigation 使用机器学习模型和威胁情报自动分析 AWS 环境中的资源，以识别潜在的安全事件。借助它，您可以主动、高效地使用在 Detective 行为图之上构建的自动化来改善安全运营。使用 Detective Investigation，您可以调查攻击策略、不可能的旅行、标记的 IP 地址和寻找群组。它执行初步安全调查步骤并生成一份报告，重点说明由 Detective 识别的风险，以帮助了解安全事件并应对潜在事件。

主题

- [进行侦探调查](#)
- [查看 Detective 调查报告](#)
- [了解 Detective 调查报告](#)
- [Detective 调查报告摘要](#)
- [下载 Detective 调查报告](#)
- [存档 Detective 调查报告](#)

进行侦探调查

使用“运行调查”来分析 IAM 用户和 IAM 角色等资源并生成调查报告。生成的报告详细说明了表明潜在危害的异常行为。

Console

按照以下步骤使用 Amazon Detective 控制台从“调查”页面进行侦探调查。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 在“调查”页面中，选择右上角的“运行调查”。
4. 在“选择资源”部分，您可以通过三种方式进行调查。您可以选择对 Detective 推荐的资源进行调查。您可以对特定资源进行调查。您也可以从 Detective 搜索页面调查资源。

1. Choose a recommended resource— Detective 根据其在调查结果和发现小组中的活动来推荐资源。要对 Detective 推荐的资源进行调查，请在推荐资源表中选择要调查的资源。

推荐资源表提供以下详细信息：

- 资源 ARN-资源的亚马逊资源名称 (ARN)。 AWS
- 调查原因：显示调查资源的关键原因。 Detective 建议调查资源的原因如下：
 - 过去 24 小时内高严重性调查发现涉及资源。
 - 过去 7 天内观察到的调查发现组中涉及资源。 Detective 调查发现组使您能够检查与潜在安全事件相关的多项活动。有关更多详细信息，请参阅[the section called “寻找群组”](#)。
 - 过去 7 天内调查发现涉及资源。
- 最新调查发现：最新调查发现的优先级排在列表顶部。
- 资源类型：标识资源的类型。例如，AWS 用户或 AWS 角色。

2. Specify an AWS role or user with an ARN— 您可以选择 AWS 角色或 AWS 用户，然后对特定资源进行调查。

按照以下步骤调查特定的资源类型。

- a. 从选择资源类型下拉列表中，选择 AWS 角色或 AWS 用户。
- b. 输入 ARN 资源的 IAM 资源。有关资源的更多详细信息 ARNs，请参阅 IAM 用户指南中的[Amazon 资源名称 \(ARNs\)](#)。

3. Find a resource to investigate from the Search page— 你可以从 Detective Search 页面搜索所有 IAM 资源。

按照以下步骤从“搜索”页面调查资源。

- a. 在导航窗格中，选择搜索。
- b. 在“搜索”页面中，搜索 IAM 资源。

5. 在调查范围时间部分中，选择调查范围时间，以评估所选资源的活动。您可以选择开始日期和开始时间；以及UTC格式中的结束日期和结束时间。所选的时间范围可以介于最少 3 小时到最多 30 天之间。
6. 选择进行调查。

API

要以编程方式进行调查，请使用 Detective API 的 [StartInvestigation](#) 操作。要使用 AWS Command Line Interface (AWS CLI) 运行调查，请运行 [开始调查](#) 命令。

在您的请求中，使用以下参数在 Detective 中运行调查：

- GraphArn— 指定行为图的 Amazon 资源名称 (ARN)。
- EntityArn— 指定 IAM 用户和 IAM 角色的唯一 Amazon 资源名称 (ARN)。
- ScopeStartTime：(可选) 指定开始调查的日期和时间。该值是一个 UTC ISO86 01 格式的字符串。例如， 2021-08-18T16:35:56.284Z。
- ScopeEndTime：(可选) 指定结束调查的日期和时间。该值是一个 UTC ISO86 01 格式的字符串。例如， 2021-08-18T16:35:56.284Z。

此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
aws detective start-investigation \  
--graph-arn arn:aws:detective:us-east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0 \  
--entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-  
time 2023-09-27T20:00:00.00Z \  
--scope-end-time 2023-09-28T22:00:00.00Z
```

您也可以从 Detective 的以下页面运行调查：

- Detective 中的 IAM 用户或 IAM 角色资料页面。
- 调查发现组的图形可视化窗格。
- 所涉及资源的操作列。
- IAM 查找页面上的用户或 IAM 角色。

在 Detective 对资源运行调查后，将生成调查报告。要访问报告，请从导航窗格转到调查。

查看 Detective 调查报告

调查报告允许您查看生成的报告，了解您之前在 Detective 中运行的调查。

查看调查报告

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。

记录调查报告中的以下属性。

- ID：调查报告生成的标识符。您可以选择此 ID 来阅读调查报告的摘要，其中包含调查的详细信息。
- 状态：每个调查都与一个基于调查完成状态的状态相关联。状态值可以是进行中、成功或失败。
- 严重性：为每个调查分配一个严重性。Detective 自动为调查发现分配严重性。

严重性表示在给定时间范围内通过调查单个资源所分析的处置情况。调查报告的严重性并不意味着或以其他方式表明受影响的资源可能对您的组织具有的关键程度或重要性。

调查严重性值可从最严重到最不严重依次为严重、高、中、低或信息性。

应优先考虑被指定为“严重”或“高”严重性值的调查，以便进一步检查，因为它们更有可能表示 Detective 发现的高影响安全问题。

- 实体：实体列包含有关调查中检测到的特定实体的详细信息。有些实体是 AWS 帐户，例如用户和角色。
- 状态：创建日期列包含有关首次创建调查报告的日期和时间的详细信息。

了解 Detective 调查报告

Detective Investigations 报告列出了表明泄露的罕见行为或恶意活动的摘要。它还列出了 Detective 为降低安全风险而提出的建议。

查看特定调查 ID 所对应的调查报告。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 在报告表中，选择调查 ID。

Admin report summary

Info

High

We observed anomalous behavior for the role from [redacted] indicating potential compromise. The role invoked CloudTrail management actions mapped to Impact MITRE tactic(s). The role was also involved in Findings that map to the MITRE tactic(s) Discovery, as well as other tactic(s). The role was also involved in 10 findings, 1 finding group, 170 impossible travels, 3 new geolocations, and 5 new user agents.

Scope time 05/25/2023 13:00 UTC - 05/31/2023 19:00 UTC role [redacted]	Indicators of compromise 5 Tactics 0 Flagged IP 170 Impossible travel 1 Finding group	Recommendation Based on our investigation, we recommend you take action to mitigate what we've found on AWS role Admin. Please review Security Best Practices in IAM to secure your AWS resource.
---	---	--

Detective 针对选定的时间范围和用户生成报告。该报告包含漏洞指标部分，其中包括有关下面列出的一个或多个漏洞指标的详细信息。在查看每个漏洞指标时，可以选择要深入了解的项并查看其详细信息。

- 策略。技术和程序-确定在潜在安全事件中使用的策略、技术和程序 (TTPs)。MITRE ATT&CK 框架用于理解。TTPs策略基于[企业的 MITRE ATT &CK 矩阵](#)。
- 威胁情报标记的 IP 地址：根据 Detective 威胁情报，标记可疑 IP 地址并将其标记为关键或严重威胁。
- 不可能的异地活动：检测并识别账户中异常和不可能的用户活动。例如，该指标列出了用户在短时间内源位置与目标位置之间的巨大变化。
- 相关调查发现组：显示与潜在安全事件相关的多项活动。Detective 使用图表分析技术来推断调查发现和实体之间的关系，并将它们分在调查发现组。
- 相关调查发现：与潜在安全事件相关的相关活动。列出与资源或调查发现组有关的所有不同类别的证据。
- 新地理位置：识别在资源或账户级别使用的新地理位置。例如，该指标根据之前的用户活动列出了一个观察到的地理位置，该地理位置是一个不经常出现或未使用的位置。
- 新用户代理：识别在资源或账户级别使用的新用户代理。
- 新建 ASOs-标识在资源或账户级别使用的新自治系统组织 (ASOs)。例如，此指标列出了一个被指定为ASO。

Detective 调查报告摘要

调查摘要重点说明了选定时间范围内需要注意的异常指标。使用摘要，您可以更快地确定潜在安全问题的根本原因，识别模式，并了解受安全事件影响的资源。

在详细调查报告摘要中，您可以查看以下详细信息。

调查概述

在“概述”面板中，您可以看到IPs具有高严重性活动的可视化，这可以提供有关攻击者路径的更多背景信息。

Detective 重点介绍了调查中的异常活动，例如IAM用户无法从来源前往遥远的目的地。

Detective 将调查映射到潜在安全事件中使用的策略、技术和程序 (TTPs)。MITRE ATT&CK 框架用于理解。TTPs策略基于[企业的 MITRE ATT &CK 矩阵](#)。

调查指标

您可以使用指标窗格中的信息，来确定可能表明恶意行为及其影响的异常活动中是否涉及 AWS 资源。入侵指标 (IOC) 是在网络、系统或环境中或环境中观察到的一种伪影，它可以 (高度可信) 识别恶意活动或安全事件。

下载 Detective 调查报告

您可以下载JSON格式的 Detective Investigations 报告，以便对其进行进一步分析，也可以将其存储到您首选的存储解决方案 (例如 Amazon S3 存储桶) 中。

从“报告”表下载调查报告。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 从报告表中选择一个调查，然后选择下载。

从摘要页面下载调查报告。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 从报告表中选择一个调查。
4. 在调查摘要页面中，选择下载。

存档 Detective 调查报告

在 Amazon Detective 中完成调查后，您可以将调查报告存档。已存档的调查表明您已完成对调查的查看。

只有当您是 Detective 管理员时，您才能存档或取消存档调查。Detective 会将您存档的调查存储 90 天。

从“报告”表存档调查报告。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 从报告表中选择一个调查，然后选择存档。

从摘要页面存档调查报告。

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查。
3. 从报告表中选择一个调查。
4. 在调查摘要页面中，选择存档。

分析 Amazon Detective 中的发现

调查发现是指检测到的潜在恶意活动或其他风险的实例。亚马逊 GuardDuty 和 AWS 安全调查结果已加载到 Amazon Detective 中，这样您就可以使用 Detective 来调查与相关实体相关的活动。GuardDuty 调查结果是 Detective 核心包的一部分，默认情况下会被摄取。由 Security Hub 汇总的所有其他 AWS 安全发现都将作为可选数据源摄取。有关更多详细信息，请参阅[行为图中使用的源数据](#)。

Detective 调查发现概述提供了有关该调查发现的详细信息。它还显示相关实体的摘要，以及指向关联实体配置文件的链接。

如果某个调查发现与较大的活动相关，Detective 会通知您转到调查发现群组。我们建议使用调查发现群组来继续调查，因为调查发现群组使您能够检查与潜在安全事件相关的多项活动。请参阅 [the section called “寻找群组”](#)。

Amazon Detective 提供调查发现群组的交互式可视化。这种可视化设计有助于以更少的精力更快更彻底地调查问题。调查发现群组可视化面板显示调查发现群组中涉及的调查发现和实体。可以使用这种交互式可视化方法来分析、了解和分类调查发现群组的影响。该面板有助于可视化涉及的实体和涉及的调查发现表中显示的信息。可以从可视化演示中选择调查发现或实体进行进一步分析。请参阅[查找群组可视化](#)。

内容

- [在 Detective 中分析发现概述](#)
- [分析调查发现群组](#)
- [由生成式人工智能支持的调查发现组摘要](#)
- [存档 Amazon 的 GuardDuty 调查结果](#)

在 Detective 中分析发现概述

Detective 调查发现概述提供了有关该调查发现的详细信息。它还显示相关实体的摘要，以及指向关联实体配置文件的链接。

用于调查发现概述的范围时间

调查发现概述的范围时间设置为调查发现时间窗口。调查发现时间窗口反映了第一次和最后一次观察到调查发现活动的时间。

调查发现详细信息

右侧面板包含调查发现的详细信息。这些是调查发现提供者提供的详细信息。

根据调查发现详细信息，您还可以将调查发现存档。有关更多详情，请参阅[存档 Amazon GuardDuty 调查结果](#)。

相关实体

调查发现概述包含调查发现中所涉及的实体列表。对于每个实体，列表都会提供有关该实体的概述信息。该信息反映了相应实体配置文件中实体详细信息配置文件面板上的信息。

您可以根据实体类型筛选列表。您还可以根据实体的标识符中的文本筛选列表。

要转向实体的配置文件，请选择查看配置文件。当您转向实体的配置文件时，会发生以下情况：

- 范围时间设置为调查发现时间窗口。
- 在实体的关联调查发现面板上，选择调查发现。调查发现的详细信息仍显示在实体配置文件的右侧。

排查“找不到页面”问题

当您在 Detective 中导航到实体或调查发现时，可能会看到找不到页面错误消息。

要解决该问题，可以执行下列一项操作：

- 确保该实体或调查发现属于您的一个成员账户。有关如何查看成员账户的信息，请参阅[查看账户列表](#)。
- 确保您的管理员帐户与 GuardDuty 和/或 Security Hub 保持一致，以便从这些服务转向 Detective。有关建议，请参见[建议与 GuardDuty 和 Security Hub 对齐](#)。
- 检查调查发现是否发生在成员账户接受您的邀请之后。
- 检查 Detective 行为图是否正在从可选的数据来源包中摄取数据。有关 Detective 行为图中使用的[源数据的更多信息，请参见行为图中使用的源数据](#)。
- 要允许 Detective 从 Security Hub 提取数据并将该数据添加到您的行为图中，您必须将 AWS 安全发现作为数据源包启用 Detective。有关更多信息，请参阅[AWS 安全调查结果](#)。
- 如果您要导航到实体简介或在 Detective 中查找概述，请确保格式正确。URL 有关配置文件形成的详细信息 URL，请参阅[导航到实体配置文件或使用 URL 查找概述](#)。

分析调查发现群组

Amazon Detective 调查发现组使您能够检查与潜在安全事件相关的多项活动。当 Detective 检测到多个发现之间的模式或关系表明它们与同一潜在安全事件有关时，就会在 Amazon Detective 中创建调查组。这种分组有助于更有效地管理和调查相关发现。

您可以使用查找组来分析高严重性 GuardDuty 发现的根本原因。如果威胁行为者试图破坏您的 AWS 环境，他们通常会执行一系列操作，从而导致多项安全发现和异常行为。这些操作通常跨越不同的时间和实体。如果单独调查安全调查发现，可能会导致对其重要性的误解，也可能导致难以找到根本原因。Amazon Detective 通过应用图表分析技术来解决这一问题，该技术可以推断出调查发现和实体之间的关系，并将它们分组在一起。我们建议将调查发现群组视为调查相关实体和调查发现的起点。

Detective 分析调查发现中的数据，并根据它们共享的资源将其与其他可能相关的调查发现分组。例如，与相同 IAM 角色会话采取的操作或来自相同 IP 地址的操作相关的发现很可能是同一基础活动的一部分。即使 Detective 提出的关联不相关，将调查发现和证据作为一个组进行调查也很有价值。

查找组是根据以下标准创建的。

- 时间邻近性 — 在近期内发生的发现通常归为一组，因为它们可能与同一事件有关。
- 常见实体 — 涉及相同实体（例如 IP 地址、用户或资源）的发现结果归为一组。这有助于了解环境不同部分的事件范围。
- 模式和行为 — Detective 分析调查结果中的模式和行为，例如类似类型的攻击或可疑活动，以确定关系并相应地对其进行分组。
- 战术、技术和程序 (TTPs) — 如在 MITRE ATT &CK 等框架中描述的那样 TTPs，将具有相似内容的发现组合在一起，以突出潜在的协调攻击。

这些标准有助于简化调查流程，因此您可以专注于可能代表相同安全事件的相关调查结果。

除调查发现外，每个组还包括调查发现所涉及的实体。这些实体可以包含 IP 地址或用户代理之 AWS 类的外部资源。

Note

在出现与另一项 GuardDuty 发现相关的初步发现后，将在 48 小时内创建包含所有相关发现和所有相关实体的发现组。

了解调查发现群组页面

查找小组页面列出了 Amazon Detective 从您的行为图中收集的所有查找组。请注意查找结果组的以下属性：

群组的严重性

根据相关发现 AWS 的安全结果格式 (ASFF) 严重性为每个发现组分配一个严重性。ASFF 查找严重性值为“严重”、“高”、“中”、“低”或“信息性”，从最严重到最不严重。分组的严重性等于该分组中调查发现的最高严重性调查发现。

对于由影响大量实体的急或高严重性调查发现组成的群组，应优先进行调查，因为它们更有可能代表影响较大的安全问题。

群组标题

在“标题”栏中，每个群组都有一个唯一的 ID 和一个非唯一的标题。它们基于群组的 ASFF 类型命名空间以及集群中该命名空间内的查找结果数量。例如，如果一个分组的标题是：分组：TTP(2)、Effect (1) 和异常行为 (2)，则它总共包括五个调查结果，包括命名空间中的两个查找结果、效果 TTP 命名空间中的一个查找结果和两个在“异常行为”命名空间中的查找结果。有关命名空间的完整列表，请参阅[类型分类法](#)。ASFF

群组策略

群组策略栏详细说明了该活动属于哪个策略类别。以下列表中的战术、技术和程序类别与 [MITRE ATT&CK 矩阵](#) 对齐。

你可以选择链上的战术来查看该战术的描述。链后面是组内检测到的策略列表。这些类别及其通常代表的活动如下：

- 初始存取 — 攻击者正试图进入他人的网络。
- 执行 — 攻击者正试图进入他人的网络。
- 维持 — 攻击者正努力保持其立足点。
- 权限升级 — 攻击者正试图获得更高级别的权限。
- 防御规避 — 攻击者正试图避免被检测到。
- 凭证访问 — 攻击者正试图窃取账户名和密码。
- 发现 — 攻击者正试图了解和学习环境。
- 横向移动 — 攻击者正试图在环境中移动。
- 收集 — 攻击者正试图收集与其目标相关的数据。

- 命令与控制 — 攻击者正试图进入他人的网络。
- 渗漏 — 攻击者正试图窃取数据。
- 影响 — 攻击者正试图操纵、中断或破坏您的系统和数据。
- 其他 — 表示调查发现中的活动与矩阵中列出的策略不一致。

群组内的实体

实体栏包含在该分组中检测到的特定实体的详细信息。选择此值可根据以下类别对实体进行细分：身份、网络、存储和计算。每个类别中的实体示例如下：

- 身份-IAM 主体和 AWS 账户，例如用户和角色
- 网络-IP 地址或其他网络 and VPC 实体
- 存储 — 亚马逊 S3 存储桶或 DDBs
- 计算 Amazon EC2 实例或 Kubernetes 容器

群组内的账户

“账户”列会告诉您哪些 AWS 账户拥有与群组中的调查结果相关的实体。AWS 账户按姓名和 AWS ID 列出，因此您可以优先调查涉及关键账户的活动。

群组内的调查发现

调查发现栏按严重性列出了群组内中的实体。调查结果包括亚马逊的调查 GuardDuty 结果、Amazon Inspector 的调查结果、AWS 安全调查结果和 Detective 的证据。您可以选择图表，查看按严重性分列的调查发现的精确计数。

GuardDuty 调查结果是 Detective 核心包的一部分，默认情况下会被摄取。由 Security Hub 汇总的所有其他 AWS 安全发现都将作为可选数据源摄取。有关更多详细信息，请参阅[行为图中使用的源数据](#)。

调查发现群组的信息调查发现

Amazon Detective 会根据您在过去 45 天内收集的行为图中的数据，识别与调查发现群组相关的其他信息。Detective 将这一信息作为一项调查发现与信息严重性一并提交。证据提供了辅助信息，突出显示了在调查发现群组内可能可疑的异常活动或未知行为。这可能包括新观察到的地理位置或在发现的范围内观察到的 API 呼叫。证据发现只能在 Detective 中查看，不会发送到 AWS Security Hub。

Detective 使用 MaxMind GeoIP 数据库确定请求的位置。MaxMind 尽管准确性因国家和知识产权类型等因素而异，但它们在国家一级的数据的准确性非常高。有关的更多信息 MaxMind，请参阅

[MaxMind IP 地理定位](#)。如果您认为任何 GeoIP 数据不正确，可以通过“更正地理数据”向 Maxmind 提交 [MaxMind 更正](#) 请求。IP2

您可以观察不同主体类型（例如 IAM 用户或 IAM 角色）的证据。对于某些证据类型，您可以观察所有账户的证据。这意味着证据会影响您的整个行为图。如果观察到所有账户的证据发现，您还会看到至少一项针对个人 IAM 角色的相同类型的信息性证据发现。例如，如果出现观察到所有账户新的地理位置调查发现，则会出现另一个观察到主体新的地理位置。

调查发现群体的证据类型

- 观察到新的地理位置
- 观察到新的自治系统组织 (ASO)
- 观察到新的用户代理
- 已发出新 API 呼叫
- 观察到所有账户新的地理位置
- 所有账户均观察到新的 IAM 本金

调查发现群组配置文件

选择群组标题后，将打开一个调查发现群组配置文件，其中包含有关该群组的其他详细信息。调查发现群组配置文件页面中的详细信息面板支持显示多达 1000 个实体和调查发现，用于调查发现群组父组和子组。

群组配置文件页面显示群组的设定范围时间。这是一组中从最早的调查发现或证据到最近更新的调查发现或证据的日期和时间。还会出现调查发现群组的严重性，该严重性等于该群组中调查发现中最高的严重性类别。此配置文件面板中的其他详细信息包括：

- 涉及策略链会显示哪些策略归因于群组中调查发现。策略基于 [MITRE ATT&CK 企业矩阵](#)。这些策略以彩色圆点链的形式显示，代表攻击从最早阶段到最新阶段的典型发展过程。这意味着，链上最左侧的圆圈通常代表不太严重的活动，即攻击者试图获取或保持对环境的访问权限。相反，右侧的活动最为严重，可能包括篡改或破坏数据。
- 该群组与其他群组的关系。有时，可以根据新发现的联系，将一组或多组以前没有联系的调查发现组合为一组新的调查发现，例如，涉及现有组实体的调查发现。在这种情况下，Amazon Detective 会停用父群组并创建一个子群组。您可以追溯到任何群组的父群组。群组之间可能有以下关系：
 - 子调查发现群组 — 当涉及其他两个调查发现群组的调查发现又涉及到一个新的调查发现时，就会创建一个调查发现群组。将列出所有子群组的调查发现的父群组。

- 父调查发现群组 — 从调查发现群组创建子群组时，该调查发现群组即为父群组。如果调查发现群组是父群组，则会随之列出相关的子群组。当父群组合并到活动子群组时，其状态变为非活动。

有两个信息选项卡可以打开配置文件面板。使用涉及的实体和涉及的调查发现选项卡，您可以查看有关群组的更多详细信息。

使用进行调查生成调查报告。生成的报告详细说明了表明存在漏洞的异常行为。

群组内的个人资料

涉及的实体

重点关注调查发现群组中的实体，包括每个实体与群组内哪些调查发现相关联。每个实体所附的标签也会显示出来，这样就可以根据标签快速识别重要实体。选择一个实体，查看其实体配置文件。

涉及的调查发现

提供有关每项调查发现的详细信息，包括调查发现的严重性、涉及的每个实体以及第一次和最后一次发现该调查发现的时间。在列表中选择调查发现类型以打开调查发现详细信息面板，其中包含有关该调查发现的更多信息。作为涉及的调查发现面板的一部分，可能会出现基于行为图中 Detective 证据的信息调查发现。

调查发现群组可视化

Amazon Detective 提供调查发现群组的交互式可视化。这种可视化设计有助于以更少的精力更快更彻底地调查问题。调查发现群组可视化面板显示调查发现群组中涉及的调查发现和实体。可以使用这种交互式可视化方法来分析、了解和分类调查发现群组的影响。该面板有助于可视化涉及的实体和涉及的调查发现表中显示的信息。可以从可视化演示中选择调查发现或实体进行进一步分析。

包含汇总调查发现的 Detective 调查发现群组是一个与相同类型资源相关的调查发现的集群。借助汇总调查发现，就可以快速评估调查发现群组的构成，更快地解释安全问题。在调查发现群组详细信息面板中，相似的调查发现被合并在一起，可以扩展调查发现，以便同时查看相对相似的调查发现。例如，汇总了一个证据节点，该节点具有相同类型的信息调查发现和中等调查发现。目前，可以查看具有汇总调查发现的调查发现群组的标题、来源、类型和严重性。

可以在此交互式面板上：

- 使用进行调查生成调查报告。生成的报告详细说明了表明存在漏洞的异常行为。如需了解更多详情，请参阅 [Detective 调查](#)。

- 查看更多关于具有汇总调查发现的调查发现群组的详细信息，以分析涉及的证据、实体和调查发现。
- 查看实体和调查发现的标签，以确定存在潜在安全问题的受影响实体。您可以切换关闭标签。
- 重新排列实体和调查发现，以便更好地了解它们之间的相互关联性。通过移动调查发现群组中的选定项目，将实体和调查发现从群组中分离出来。
- 选择证据、实体和调查发现，查看有关它们的更多详细信息。要选择多个项目，请选择 **command/control**，然后选择项目或使用指针拖放项目。
- 调整布局，使所有实体和调查发现都能在调查发现群组窗口中显示。查看调查发现群组中常见的实体类型。

Note

调查发现群组可视化面板支持显示包含多达 100 个实体和调查发现的调查发现群组。

您可以使用下拉列表查看径向、圆形、力导向或网格布局中的发现结果和实体。径向布局提供了改进的可视化效果，便于数据解释。力导向布局可以定位实体和调查发现，使项目之间的链接长度保持一致，并且链接分布均匀。这有助于减少重叠。所选择的布局定义了调查发现在可视化面板中的位置。

时间轴布局

时间轴布局提供了一种动态的方式来可视化您的搜索结果组如何随着时间的推移而演变。这使您可以查看事件的进展，从而使用 Detective 更好地了解安全事件的顺序和潜在的因果关系。

使用可视化面板底部的时间轴滑块选择特定的时间点。可视化效果将更新，以显示您的搜索结果组当时的状态。播放按钮，允许您在时间轴上自动前进。单击“播放”按钮开始播放动画。可视化将实时更新，显示查找组如何随时间变化。使用暂停按钮可随时停止动画。

现在，您可以使用“筛选”下拉列表根据其严重性级别筛选结果。当您应用筛选器时，可视化效果将更新，仅显示与所选严重性级别相匹配的结果。筛选器仅影响时间轴中显示的结果，而不影响完整的“查找结果组”可视化效果。这使您可以快速关注高优先级问题或调查特定类型的发现。

您可以将筛选功能与时间轴布局结合使用，以查看不同严重性级别的发现是如何随着时间的推移而出现的和演变的。

增强的调查工作流程

通过添加时间轴布局和筛选功能，您现在可以进行更全面的调查：

1. 首先使用一种静态布局（径向、圆形、力导向或网格）查看整个查找组。
2. 使用时间表来了解情况是如何随着时间的推移而发展的。
3. 使用播放按钮在时间轴上自动前进，关注关键时刻或模式。
4. 在重要时刻停下来进一步调查。
5. 应用过滤器，重点关注特定严重性级别的调查结果。
6. 使用键盘快捷键和选择工具更深入地研究感兴趣的实体和发现。

这种增强的工作流程允许对复杂的安全场景进行更细致和彻底的调查。您可以进行更高效、更有效的安全调查，从而更快地解决事件并改善整体安全状况。

键盘快捷键

您可以使用以下键盘快捷键与查找组可视化面板进行交互：

- 单击 — 选择单个节点，取消选择所有其他节点，如果单击空白，则取消选择所有节点。
- Ctrl + Click — 选择单个节点，不取消选择其他节点。
- 拖动-平移视图。
- Ctrl + Drag — Marquee 选择，不取消选择其他节点。
- Shift + Drag — Marquee 选择、取消选择所有其他节点。
- 箭头键-更改节点之间的焦点。
- Ctrl + 空格 — 选择或取消选择当前聚焦的节点。
- Shift + 箭头键-更改节点之间的焦点并选择它们。

动态图例会根据当前图表中的实体和调查发现进行更改。它有助于确定每个视觉元素所代表的内容。

由生成式人工智能支持的调查发现组摘要

默认情况下，Amazon Detective 会自动提供单个调查发现组的摘要。这些摘要由 [Amazon Bedrock](#) 上托管的生成式人工智能（生成式 AI）模型提供支持。

通过使用调查发现组，您可以检查与潜在安全事件相关的多个安全调查发现，并识别潜在的威胁行为者。调查发现组的调查发现组摘要基于这些功能而构建。调查发现组摘要使用调查发现组的数据，快速分析调查发现与受影响资源之间的关系，然后采用自然语言总结潜在威胁。您可以利用这些摘要来识别更大的安全威胁，提高调查效率并缩短响应时间。

 Note

由生成式人工智能提供支持的调查发现组摘要可能而且并不总是能提供完全准确的信息。请参阅 [AWS 负责任的人工智能政策了解](#) 更多信息。

查看调查发现组摘要

调查发现组的调查发现组摘要为您提供有关安全事件的清晰、详细的解释。在自然语言中，解释包括简洁的标题、所涉及的资源摘要以及有关这些资源的精选信息。

查看调查发现组摘要

1. 打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择调查发现组。
3. 在调查发现组表中，选择要显示其摘要的调查发现组。此时将会显示详细信息页面。

在详细信息页面上，您可以使用摘要窗格，来查看为调查发现组中最重要的调查发现生成的描述性摘要。您还可以查看调查发现组中主要威胁事件的分析，然后可以对其进行进一步调查。要将生成的摘要添加到备忘录或票务系统中，请在窗格中选择复制图标。这会将摘要复制到剪贴板。您还可以在摘要中共享您对调查发现组摘要输出的反馈，这样将来可以提供更好的体验。要共享您的反馈，请根据反馈的性质选择“赞成”或“反对”图标。

 Note

如果您提供有关调查发现组摘要的反馈，则您的反馈不会用于模型调整。我们使用它只是为了便于有效制作 Detective 中的提示。

**Summary - new Info**

Credentials exfiltration from i-0e5f7e596391b28eb using role privilegedRole

Instance i-0e5f7e596391b28eb had newly observed API calls and user agents for role privilegedRole.

Credentials for role privilegedRole on i-0e5f7e596391b28eb were exfiltrated and used from account [REDACTED] and IP [REDACTED].

The exfiltrated credentials were used to access S3 bucket private-bucket-[REDACTED].

i-0e5f7e596391b28eb was vulnerable to CVE-2021-44228 and CVE-2021-45046.



禁用调查发现组摘要

默认情况下，调查发现组的调查发现组摘要处于启用状态。您可以随时禁用调查发现组摘要。如果禁用，则可在日后再次将其启用。

禁用调查发现组摘要

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择首选项。
3. 在调查发现组摘要下，选择编辑。
4. 关闭启用。

5. 选择保存。

启用调查发现组摘要

如果您之前禁用了调查发现组的调查发现组摘要，则可以随时再次将其启用。

启用调查发现组摘要

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择首选项。
3. 在调查发现组摘要下，选择编辑。
4. 打开启用。
5. 选择保存。

支持的区域

以下是@@ 查找组摘要 AWS 区域。

- 美国东部 (弗吉尼亚州北部)
- 美国西部 (俄勒冈)
- Asia Pacific (Tokyo)
- 欧洲地区 (法兰克福)

存档 Amazon 的 GuardDuty 调查结果

当你完成对亚马逊调查 GuardDuty 结果的调查后，你可以存档 Amazon Detective 的调查结果。这为您省去了必须返回 GuardDuty 进行更新的麻烦。存档调查发现表示您已经完成了对该调查发现的调查。

只有当你同时也是与 GuardDuty 调查结果关联的帐户的 GuardDuty 管理员帐户时，才能在 Detective 中存档该调查结果。如果您不是 GuardDuty 管理员帐户并尝试存档调查结果，则 GuardDuty 会显示错误。

存档 GuardDuty 调查结果

1. 登录 AWS 管理控制台。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在 Detective 控制台的调查发现详细信息面板中，选择存档调查发现。
3. 如果提示确认，请选择存档。

您可以在 GuardDuty 控制台中查看存档的 GuardDuty 调查结果。存档的查找结果将在 GuardDuty 其中存储 90 天，在此期间可以随时查看。您可以在 GuardDuty 控制台中查看隐藏的查找结果，方法是从查找结果表中选择“已存档”，或者 GuardDuty API 使用 `service.arch` [ListFindingsAPI](#) `lived` 等于 `true` 的 `findingCriteria` 标准。要了解更多信息，请参阅 Amazon GuardDuty 用户指南中的[禁止规则](#)。

分析 Amazon Detective 中的实体

实体是从源数据中提取的单个对象。示例包括特定的 IP 地址、Amazon EC2 实例或 AWS 账户。有关实体类型的列表，请参阅[the section called “行为图数据结构中的实体类型”](#)。

Amazon Detective 实体配置文件是一个单独页面，提供有关该实体及其活动的详细信息。您可能会使用实体配置文件来获取调查发现的支持详情，或作为一般可疑活动搜寻的一部分。

内容

- [使用实体配置文件](#)
- [查看 Detective 个人资料面板并与之互动](#)
- [直接导航到实体配置文件或调查发现概述](#)
- [从配置文件面板转到另一个控制台](#)
- [在配置文件面板上浏览活动详细信息](#)
- [管理范围时间](#)
- [在 Detective 中查看相关发现的详细信息](#)
- [在 Detective 中查看大量实体的详细信息](#)

使用实体配置文件

您执行以下操作之一时，就会显示实体配置文件：

- 在 Amazon GuardDuty 控制台中，选择调查与所选调查结果相关的实体的选项。

请参阅 [the section called “从另一个控制台转向”](#)。

- 前往 Detective 网址查看实体配置文件。

请参阅 [the section called “使用网址进行导航”](#)。

- 使用 Detective 控制台中的 Detective 搜索来查找实体。
- 从其他实体配置文件或调查发现概述中选择指向实体配置文件的链接。

实体配置文件的范围时间

在不提供范围时间的情况下直接导航到实体配置文件时，范围时间将设置为前 24 小时。

从另一个实体配置文件导航到实体配置文件时，当前选择的范围时间保持不变。

从调查发现概述导航到实体配置文件时，范围时间会设置为调查发现时间窗口。

有关自定义范围时间以限制实体配置文件上显示的数据的信息，请参阅[管理范围时间](#)。

实体的标识符和类型

配置文件的顶部是实体标识符和实体类型。每种实体类型都有一个对应的图标，以提供配置文件类型的可视指示。

涉及的调查发现

每个配置文件都包含该实体在范围时间期间涉及的调查发现的列表。

您可以查看每个调查发现的详细信息，更改范围时间以反映调查发现的时间窗口，并进入调查发现概述以查找其他相关资源。

请参阅 [the section called “查看实体的调查发现”](#)。

涉及该实体的调查发现群组

每个配置文件都包含一个实体所属的调查发现群组列表。

调查发现群组由 Detective 收集到的调查发现、实体和证据组成，为可能存在的安全问题提供更多上下文信息。

有关调查发现群组的更多信息，请参阅[the section called “寻找群组”](#)。

包含实体详细信息和分析结果的配置文件面板

每个实体配置文件都包含一组或多个选项卡。每个选项卡都包含一个或多个配置文件面板。每个配置文件面板都包含由行为图数据生成的文本和可视化内容。特定的选项卡和配置文件面板是根据实体类型量身定制的。

对于大多数实体，第一个选项卡顶部的面板会提供有关该实体的高级摘要信息。

其他配置文件面板则突出显示了不同类型的活动。对于涉及调查发现的实体，实体配置文件面板上的信息可提供更多支持证据，帮助完成调查。每个配置文件面板都提供有关如何使用信息的指导。有关更多信息，请参阅 [the section called “使用配置文件面板指南”](#)。

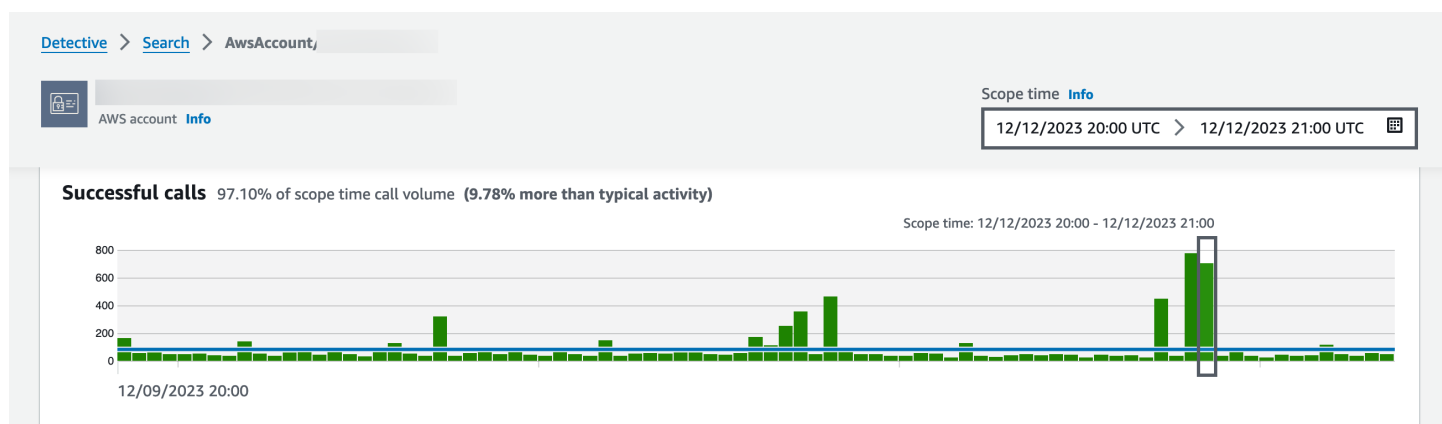
有关配置文件面板、其中包含的数据类型以及与之交互的可用选项的更多详细信息，请参阅[the section called “型材面板”](#)。

在实体配置文件中导航

一个实体配置文件都包含一组或多个选项卡。每个选项卡都包含一个或多个配置文件面板。每个配置文件面板都包含由行为图数据生成的文本和可视化内容。

当您向下滚动浏览配置文件选项卡时，以下信息仍显示在配置文件顶部：

- 实体类型
- 实体标识符
- 范围时间



查看 Detective 个人资料面板并与之互动

Amazon Detective 控制台上的每个实体配置文件都由一组配置文件面板组成。配置文件面板是一种可视化工具，可提供一般详细信息或突出显示与实体关联的特定活动。配置文件面板使用不同类型的可视化方式来呈现不同类型的信息。它们还可以提供指向其他详细信息或其他配置文件的链接。

每个配置文件面板都旨在帮助分析人员找到有关实体及其关联活动的特定问题的答案。这些问题的答案有助于得出关于该活动是否构成真正威胁的结论。

配置文件面板使用不同类型的可视化方式来呈现不同类型的信息。

配置文件面板上的信息类型

配置文件面板通常提供以下类型的数据。

面板数据类型	描述
有关调查发现或实体的高级信息	最简单的面板类型提供了有关实体的一些基本信息。 信息面板上包含的信息示例包括标识符、名称、类型和创建日期。 Role details AWS role Principal ID AWS account Created by Created date Last observed Role description 09/20/2022 16:46 UTC 大多数实体配置文件都包含该实体的信息面板。
一段时间内活动的总结概括	显示实体一段时间内活动的总结概括。 这种类型的面板可以全面了解实体在范围事件期间的行为。 AWS role Scope time 09/19/2022 18:00 UTC > 09/20/2022 18:00 UTC Overall API call volume Overall volume of API calls issued by this resource around the scope time. Successful calls 66.65% of scope time call volume (15.87% more than typical activity) Linear Log 09/17/2022 16:00 UTC - 09/17/2022 20:00 UTC Successful calls: 429 Baseline: 212 Failed calls 33.35% of scope time call volume (15.87% less than typical activity) 09/17/2022 16:00 09/19/2022 18:00 - 09/20/2022 18:00 以下是 Detective 配置文件面板上提供的一些摘要数据示例： - 失败和成功的API呼叫 - 入站和出站VPC量
按值分组的活动摘要	显示按特定值分组的实体活动摘要。

面板数据类型	描述																				
	您可以在EC2实例的配置文件上看到这种类型的配置文件面板。 配置文件面板显示与特定服务类型关联的常用端口往返EC2实例的平均VPC流日志数据量。 Average VPC volume for common ports Displays the average VPC volume for a selected set of common ports. Volume that exceeds the baseline average is highlighted. Select a specific port to see a time series of its traffic. Inbound Outbound Linear Log SSH (22) DNS (53) HTTP (80) HTTPS (443) 0 B 50 kB 100 kB 150 kB 200 kB 250 kB 300 kB 350 kB 400 kB Hypertext Transfer Protocol over SSL/TLS (443) Scope: 11/29, 16:00 - 11/29, 18:00 100 kB 50 kB 0 B 11/26, 16:00 仅在范围时间内开始的活动 在调查期间，了解哪些活动是在特定的时间范围内才开始发生的，这一点非常重要。 例如，是否有以前从未见过的API电话、地理位置或用户代理？ Newly observed API calls The following API methods were newly observed during the scope time. Q Filter by API call name or Service name <table><tr><th>Service name</th><th>API call</th><th>Count</th><th>Success rate</th></tr><tr><td>▼ secretmanager</td><td>ListSecrets</td><td>164</td><td>100.00%</td></tr><tr><td>▶ waf</td><td>GetLoggingConfiguration</td><td>82</td><td>0.00%</td></tr><tr><td>▶ waf</td><td>GetWebACL</td><td>82</td><td>100.00%</td></tr><tr><td>▶ eks</td><td>DescribeCluster</td><td>15</td><td>100.00%</td></tr></table> Scope start: 05/14, 17:00 Scope end: 05/28, 17:00 4 3 2 1 0 05/27, 00:00 如果行为图仍处于训练模式，则配置文件面板会显示一条通知消息。当行为图积累了至少两周的数据后，该信息就会被删除。有关训练模式的更多信息，请参阅the section called “新行为图的训练期”。	Service name	API call	Count	Success rate	▼ secretmanager	ListSecrets	164	100.00%	▶ waf	GetLoggingConfiguration	82	0.00%	▶ waf	GetWebACL	82	100.00%	▶ eks	DescribeCluster	15	100.00%
Service name	API call	Count	Success rate																		
▼ secretmanager	ListSecrets	164	100.00%																		
▶ waf	GetLoggingConfiguration	82	0.00%																		
▶ waf	GetWebACL	82	100.00%																		
▶ eks	DescribeCluster	15	100.00%																		

面板数据类型	描述										
在范围时间期间发生显著变化的活动	与新的活动面板类似，配置文件面板也可以显示范围时间期间发生重大变化的活动。 例如，用户可能每周定期API拨打几次电话。如果同一用户突然在一天内多次发出相同的调用，这可能是发生恶意活动的证据。 API calls with increased volume The following API methods were observed at a substantially higher rate during the scope time. Filter by API call name or Service name <table><tr><th>Service name</th><th>API call</th><th>Rate increase</th><th>Internal call count</th><th>External call count</th></tr><tr><td>iam</td><td>GetRolePolicy</td><td>100.00%</td><td>2</td><td>0</td></tr></table> Scope start: 05/14, 17:00 Scope end: 06/28, 17:00	Service name	API call	Rate increase	Internal call count	External call count	iam	GetRolePolicy	100.00%	2	0
Service name	API call	Rate increase	Internal call count	External call count							
iam	GetRolePolicy	100.00%	2	0							
	如果行为图仍处于训练模式，则配置文件面板会显示一条通知消息。当行为图积累了至少两周的数据后，该信息就会被删除。有关训练模式的更多信息，请参阅the section called “新行为图的训练期”。										

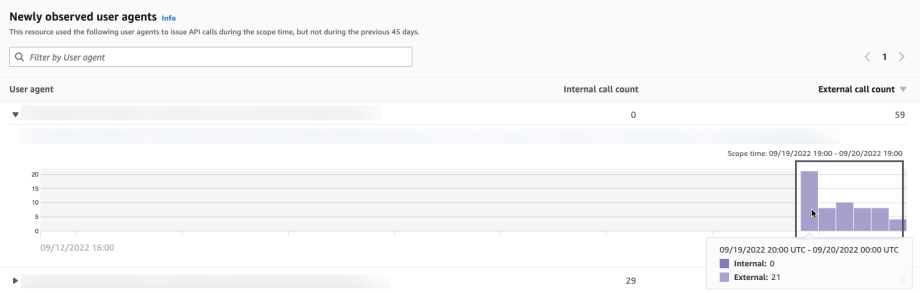
配置文件面板可视化的类型

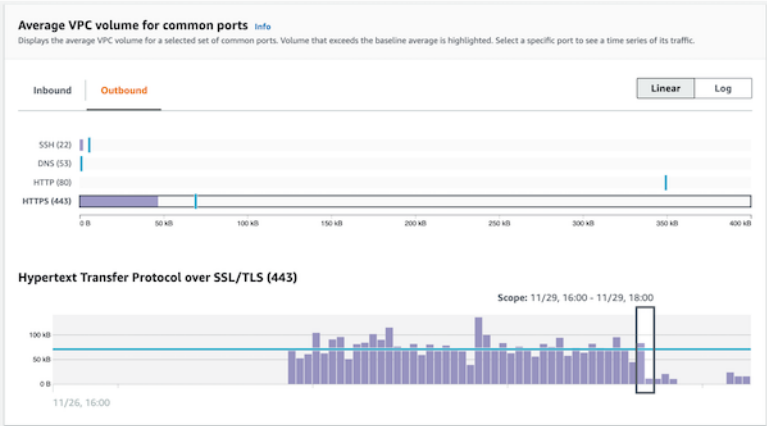
配置文件面板内容可以采用以下形式之一。

可视化类型	描述															
键值对	最简单的可视化类型是一组键值对。 调查发现或实体信息面板是键值对面板最常见的示例。 Role details Info <table><tr><td>AWS role</td><td>Principal ID</td><td>AWS account</td></tr><tr><td>Created by</td><td>Created date</td><td>Last observed</td></tr><tr><td>-</td><td>-</td><td>09/20/2022 16:46 UTC</td></tr><tr><td>Role description</td><td></td><td></td></tr><tr><td>-</td><td></td><td></td></tr></table>	AWS role	Principal ID	AWS account	Created by	Created date	Last observed	-	-	09/20/2022 16:46 UTC	Role description			-		
AWS role	Principal ID	AWS account														
Created by	Created date	Last observed														
-	-	09/20/2022 16:46 UTC														
Role description																
-																
	键值对还可用于向其他类型的面板添加其他信息。 在键值对面板中，如果某个值是某个实体的标识符，则您可以转到其配置文件。															

可视化类型	描述						
表	表格是一个简单的多栏项目列表。 Observed IP address assignments based on VPC Flow These IP addresses were assigned to this EC2 instance and also had traffic with the instance Filter by IP CIDR < 1 > <table><tr><th>IP address</th><th>First observed</th><th>Last observed</th></tr><tr><td>10.101.0.119</td><td>04/27/2021 15:19 UTC</td><td>09/20/2022 17:45 UTC</td></tr></table> 您可以对表格进行排序、筛选和翻页。 您可以更改每页显示的条目数量。请参阅 the section called “配置文件面板的首选项”。 如果表中的某个值是某个实体的标识符，则您可以转到其配置文件。	IP address	First observed	Last observed	10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC
IP address	First observed	Last observed					
10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC					

时间轴	时间轴可视化显示一段时间内定义的时间间隔的汇总值。 AWS role Info Scope time Info 09/19/2022 18:00 UTC > 09/20/2022 18:00 UTC Overall API call volume Info Overall volume of API calls issued by this resource around the scope time. Linear Log Successful calls 66.65% of scope time call volume (15.87% more than typical activity) Scope time: 09/19/2022 18:00 - 09/20/2022 18:00 09/12/2022 16:00 09/17/2022 16:00 UTC - 09/17/2022 20:00 UTC 09/17/2022 16:00 UTC - 09/17/2022 20:00 UTC Successful calls: 429 Baseline: 212 To see more details, choose a time interval bar Failed calls 33.35% of scope time call volume (15.87% less than typical activity) Scope time: 09/19/2022 18:00 - 09/20/2022 18:00 09/12/2022 16:00 09/17/2022 16:00 UTC - 09/17/2022 20:00 UTC 09/17/2022 16:00 UTC - 09/17/2022 20:00 UTC Successful calls: 429 Baseline: 212 To see more details, choose a time interval bar To see more details, choose a time interval bar or display details for scope time
-----	--

可视化类型	描述
可扩展表格	可扩展表格结合了表格和时间轴。  可视化开始时是一张表格。 您可以对表格进行排序、筛选和翻页。 您可以更改每页显示的条目数量。请参阅 the section called “配置文件面板的首选项”。 然后您可以展开每一行，显示该行特定的时间轴可视化内容。

条形图	条形图根据分组显示数值。 您可以根据图表的不同选择一个条形图来显示相关活动的时间轴。 
-----	---

可视化类型	描述															
地理位置图	地理位置图显示的是一张标记为根据地理位置突出显示数据的地图。后面可能是一张包含各个地理位置详细信息的表格。 Newly observed geolocations info This resource was observed operating in the following geolocations during the scope time. Select a location to see more details.  Legend: Newly observed during scope time (orange), Observed before and during scope time (blue) <table><thead><tr><th>Observed</th><th>Geolocation</th><th>Number of times observed</th><th>Percentage of total API calls</th><th>Annotations</th></tr></thead><tbody><tr><td>Observed before and during scope time</td><td>Ashburn, US</td><td>33</td><td>67.35%</td><td>Details ></td></tr><tr><td>Observed before and during scope time</td><td>Dublin, IE</td><td>16</td><td>32.65%</td><td>Details ></td></tr></tbody></table> 请注意，在处理传入的地理数据时，Detective 会将经纬度值四舍五入到小数点后一位。	Observed	Geolocation	Number of times observed	Percentage of total API calls	Annotations	Observed before and during scope time	Ashburn, US	33	67.35%	Details >	Observed before and during scope time	Dublin, IE	16	32.65%	Details >
Observed	Geolocation	Number of times observed	Percentage of total API calls	Annotations												
Observed before and during scope time	Ashburn, US	33	67.35%	Details >												
Observed before and during scope time	Dublin, IE	16	32.65%	Details >												

关于配置文件面板内容的注意事项

查看配置文件面板的内容时，需要注意以下事项：

近似计数数据警告

此警告表明，由于适用的数据量太大，计数极低的项目不会出现。

要确保计数完全准确，请减少数据量。要做到这一点，最简单的方法就是缩短范围时间。请参阅 [the section called “管理范围时间”](#)。

按地理位置进行四舍五入

Detective 会将所有经纬度值四舍五入到小数点后一位。

Detective 表示API电话的方式发生了变化

从 2021 年 7 月 14 日开始，Detective 会追踪拨打每个API电话的服务。每当 Detective 显示API方法时，它还会显示关联的服务。在显示API呼叫信息的配置文件面板上，呼叫始终按服务分组。对于 Detective 在该日期之前采集的数据，服务名称列为未知服务。

同样从 2021 年 7 月 14 日起，对于账户和角色，“总体API通话量配置文件”面板AKID的活动详细信息将不再显示发出通话的资源。对于账户，Detective 会显示发出调用的主体（用户或角色）的标识符。对于角色，Detective 会显示角色会话的标识符。对于 Detective 在 2021 年 7 月 14 日之前采集的数据，该标识符列为未知资源。

对于显示API呼叫列表的配置文件面板，相关的时间轴会突出显示此过渡发生的时间段。从 2021 年 7 月 14 日开始突出显示，直到更新在 Detective 中全面传播时结束。

设置配置文件面板的首选项

对于配置文件面板，您可以通过配置时间戳格式首选项来自定义配置文件面板上每个页面上显示的行数。

设置表格长度

对于包含表格或可扩展表格的配置文件面板，您可以配置要在每页上显示的行数。

设置您对每页条目数量的偏好。

1. 打开 Amazon Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在 Detective 导航窗格中的设置下，选择首选项。
3. 在首选项页面的表格长度下，单击编辑。
4. 选择您要在每页上显示的表格行数。
5. 选择保存。

设置时间戳格式

对于配置文件面板，您可以配置时间戳格式首选项，该首选项将应用于 Detective 中每个IAM用户或IAM角色的所有时间戳。

Note

时间戳格式首选项不适用于整个 AWS 账户。

设置时间戳的首选项。

1. 打开 Amazon Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。

2. 在 Detective 导航窗格中的设置下，选择首选项。
3. 在首选项页面的时间戳首选项下，查看和更改所有时间戳的首选显示方式。
4. 默认情况下，时间戳格式设置为。UTC单击编辑，选择您的本地时区。

例如：

Example

UTC-09/20/22 16:39 UTC

本地-2022 年 9 月 20 日 9:39 (-07:00) UTC

5. 选择保存。

直接导航到实体配置文件或调查发现概述

使用以下选项之一可直接导航到 Amazon Detective 中的实体配置文件或调查发现概述。

- 从 Amazon GuardDuty 或者 AWS Security Hub，你可以从 GuardDuty 调查结果转到相应的 Detective 发现档案。
- 您可以汇编 Detective 网址，用于标识调查发现或实体，并设置要使用的范围时间。

转到实体资料或从 Amazon GuardDuty 查找概述或 AWS Security Hub

在 Amazon GuardDuty 控制台中，您可以导航到与调查结果相关的实体的实体档案。

您还可以从 GuardDuty 和 AWS Security Hub 控制台导航到查找概览。这还提供了相关实体的实体配置文件链接。

这些链接有助于简化调查流程。您可以快速使用 Detective 查看关联的实体活动，并确定后续步骤。然后，如果调查发现是误报，则可以将其存档，也可以进一步深入了解，确定问题的范围。

如何转到 Amazon Detective 控制台

所有调查 GuardDuty 结果均有调查链接。GuardDuty 还允许您选择是导航到实体配置文件还是导航到查找结果概览。

从 GuardDuty 主机切换到 Detective

1. 打开 GuardDuty 控制台，[网址为 https://console.aws.amazon.com/guardduty/](https://console.aws.amazon.com/guardduty/)。

2. 如有必要，选择左侧导航窗格中的调查发现。
3. 在 GuardDuty 调查结果页面上，选择调查结果。

调查发现详细信息窗格显示在调查发现列表的右侧。

4. 在调查发现详细信息窗格上，选择在 Detective 中进行调查。

GuardDuty 显示 Detective 中可供调查的可用物品列表。

该列表既包含相关实体（例如 IP 地址或 EC2 实例），也包含调查发现。

5. 选择实体或调查发现。

Detective 控制台将打开新的选项卡。控制台将打开实体或调查发现配置文件。

如果尚未启用 Detective，则控制台会打开一个登陆页面，提供 Detective 的概述。您可在此选择启用 Detective。

要从 Security Hub 控制台转到 Detective

1. 打开 AWS Security Hub 控制台，[网址为 https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/)。
2. 如有必要，选择左侧导航窗格中的调查发现。
3. 在 Security Hub 调查结果页面上，选择一项 GuardDuty 调查结果。
4. 在详细信息窗格中，选择在 Detective 中进行调查，然后选择对调查发现进行调查。

当您选择对调查发现进行调查时，在新的选项卡中将打开 Detective 控制台。打开控制台，显示调查发现概述。

即使从聚合区域进行转向，总是打开 Detective 控制台，显示调查发现来源的区域。有关调查发现聚合的更多信息，请参阅《AWS Security Hub 用户指南》中的[跨区域聚合调查发现](#)。

如果您未启用 Detective，则将打开控制台，显示 Detective 登录页面。您可在此启用 Detective。

对转向故障排除

要使用转向功能，必须满足以下条件之一：

- 账户必须既是 Detective 的管理员账户，也是要转向的服务的管理员账户。
- 已代入跨账户角色，该角色授予管理员账户访问行为图的权限。

有关调整管理员账户的的建议的更多信息，请参阅与 [Amazon 保持一致的建议 GuardDuty 和 AWS Security Hub](#)。

如果转向功能不起作用，请检查以下内容。

- 在行为图中，该调查发现是否属于已启用的成员账户？如果关联账户未被邀请以成员账户的身份访问行为图，则行为图中不包含该账户的数据。

如果受邀成员账户未接受邀请，则行为图中不包含该账户的数据。

- 调查发现是否存档？Detective 没有收到来自的存档调查结果 GuardDuty。
- 这一调查发现是否发生在 Detective 开始将数据导入行为图之前？如果 Detective 采集的数据中不存在该调查发现，则行为图中就不包含相关数据。
- 调查发现是否来自正确的区域？每个行为图都针对一个区域。行为图不包含来自其他区域的数据。

使用网址导航到实体配置文件或调查发现概述

要导航到 Amazon Detective 中的实体配置文件或调查发现概述，您可以使用提供直接链接的网址。网址可标识调查发现或实体。它还可以指定在配置文件上使用的范围时间。Detective 最多可保存一年的历史事件数据。

配置文件网址的格式

Note

如果您使用的是旧网址格式，Detective 会自动重定向到新网址。网址的旧格式是：

`https://console.aws.amazon.com/detective/home?`

`region=Region#type/namespace/instanceID?parameters`

配置文件网址的新格式如下：

- 对于实体 - `https://console.aws.amazon.com/detective/home?region=Region#entities/namespace/instanceID?parameters`
- 对于调查发现 - `https://console.aws.amazon.com/detective/home?region=Region#findings/instanceID?parameters`

网址需要以下值。

##

您要使用的区域。

##

您要导航到的配置文件的项目类型。

- `entities` - 表示您正在导航到实体配置文件
- `findings` - 表示您正在导航到调查发现概述

####

对于实体，命名空间是实体类型的名称。

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

instanceID

调查发现或实体的实例标识符。

- 对于 GuardDuty 查找结果，为查找 GuardDuty 结果标识符。
- 对于 AWS 账户，为账户 ID。
- 对于 AWS 角色和用户，是角色或用户的委托人 ID。
- 对于联合用户，即联合用户的主体 ID。主体 ID 为 `<identityProvider>:<username>` 或 `<identityProvider>:<audience>:<username>`。

- 对于 IP 地址，即 IP 地址。
- 对于用户代理，即用户代理名称。
- 对于 EC2 实例，即实例 ID。
- 对于角色会话，即会话标识符。会话标识符使用格式
`<rolePrincipalID>:<sessionName>`。
- 对于 S3 存储桶，即存储桶名称。
- 对于 FindingGroups，一个 UUID。例如，ca6104bc-a315-4b15-bf88-1c1e60998f83
- 对于 EKS 资源，请使用以下格式：
 - EKS 集群：`<clusterName>~<accountId>~EKS`
 - `Kubernetes Pod#~EKS` `<podUid><clusterName><accountId>`
 - Kubernetes 主题：`<subjectName>~<clusterName>~<accountId>`
 - 容器映像：`<registry>/<repository>:<tag>@<digest>`

调查发现或实体必须与行为图中已启用的账户相关联。

网址还可以包含以下可选参数，用于设置范围时间。有关范围时间以及其如何在配置文件中使用的更多信息，请参阅[the section called “管理范围时间”](#)。

scopeStart

在配置文件中使用的范围时间的开始时间。开始时间必须在过去 365 天内。

该值是事件时间戳。

如果您提供了开始时间，但没有提供结束时间，则范围时间将在当前时间结束。

scopeEnd

在配置文件中使用的范围时间的结束时间。

该值是事件时间戳。

如果您提供了结束时间，但没有提供开始时间，则范围时间包括结束时间之前的所有时间。

如果您未指定范围时间，则使用默认的范围时间。

- 对于调查发现，默认范围时间使用观察到调查发现活动的第一次和最后一次时间。
- 对于实体，默认范围时间是前 24 小时。

以下是 Detective 网址示例：

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/  
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

该示例网址提供了以下说明。

- 显示 IP 地址 192.168.1 的实体配置文件。
- 使用从 GMT 2019 年 3 月 18 日 (星期一) 上午 12:00:00 开始，到 GMT 2019 年 3 月 18 日 (星期一) 下午 12:00:00 结束的范围时间。

对网址故障排除

如果网址未显示预期配置文件，请首先检查网址是否使用了正确的格式，以及提供的值是否正确。

- 是否使用了正确的网址 (findings 或 entities) ？
- 是否指定了正确的命名空间？
- 是否提供了正确的标识符？

如果数值正确，您还可以检查以下内容。

- 在行为图中，该调查发现或实体是否属于已启用的成员账户？如果关联账户未被邀请以成员账户的身份访问行为图，则行为图中不包含该账户的数据。

如果受邀成员账户未接受邀请，则行为图中不包含该账户的数据。

- 对于调查发现，该调查发现是否存档？Detective 不会收到来自亚马逊的存档调查结果 GuardDuty。
- 这一调查发现或实体是否发生在 Detective 开始将数据导入行为图之前？如果 Detective 采集的数据中不存在该调查发现或实体，则行为图中就不包含相关数据。
- 调查发现或实体是否来自正确的区域？每个行为图都针对一个区域。行为图不包含来自其他区域的数据。

在 Splunk 中添加调查发现的 Detective 网址

Splunk Trumpet 项目允许您将数据从 AWS 服务发送到 Splunk。

您可以将 Trumpet 项目配置为为亚马逊的 GuardDuty 调查结果生成侦探网址。然后，您可以使用这些网址直接从 Splunk 转到相应的 Detective 调查发现配置文件。

Trumpet 项目可从 GitHub <https://github.com/splunk/splunk-aws-project-trumpet> 获得。

在 Trumpet 项目的配置页面上，从“AWS CloudWatch 事件”中选择 Detective GuardDuty URL。

从配置文件面板转到另一个控制台

对于EC2实例、IAM用户和IAM角色，您可以直接从详细信息配置面板导航到相应的控制台。控制台提供的信息可以为您的安全调查提供更多输入。

在EC2实例详情配置面板上，EC2实例标识符链接到 Amazon EC2 控制台。

在用户详细信息配置文件面板上，用户名链接到IAM控制台。

在角色详细信息配置文件面板上，角色名称链接到IAM控制台。

从配置文件面板转到另一个实体配置文件

当配置文件面板包含不同实体的标识符时，它通常是指向该实体配置文件的链接。例外的是EC2实例、IAM用户EC2和IAM角色配置文件中指向 Amazon 和IAM控制台的链接。请参阅 [the section called “转到另一个控制台”](#)。

例如，您可以从 IP 地址列表中显示特定 IP 地址的配置文件。这样您就可以了解是否有其他信息可以帮助您完成调查。

在配置文件面板上浏览活动详细信息

在调查期间，您可能需要进一步调查某个实体的活动模式。

在以下配置文件面板中，您可以显示活动详细信息摘要：

- 总体API通话量，用户代理配置文件上的配置文件面板除外
- 观察到新的地理位置
- 总VPC流量
- VPC对于@@ 与单个 IP 地址关联的查找结果，进出查找 IP 地址的流量
- 容器详细信息
- VPC集群的@@ 流量
- Kubernetes API 的整体活动

活动详情可以回答以下类型的问题：

- 使用了哪些 IP 地址？
- 这些 IP 地址位于哪里？
- 每个 IP 地址API拨打了哪些电话，这些呼叫来自哪些服务？
- 使用了哪些主体或访问密钥标识符 (AKIDs) 来拨打电话？
- 使用了哪些资源来进行调用？
- 进行了多少次调用？成功和失败的调用各有多少次？
- 向每个 IP 地址发送或从每个 IP 地址发送了多少VPC流日志数据？
- 在特定集群、映像或容器组 (pod) 中，哪些容器处于活动状态？

主题

- [总API通话量的活动详情](#)
- [地理位置的活动详细信息](#)
- [总VPC流量的活动详情](#)
- [涉及集群的 Kubernetes API 总体活动 EKS](#)

总API通话量的活动详情

“总API呼叫量”的活动详细信息显示选定时间范围内发出的API呼叫。

要显示单个时间间隔的活动详细信息，请选择图表上的时间间隔。

要显示当前范围时间的活动详细信息，请选择显示范围时间的详细信息。

请注意，从2021年7月14日起，Detective开始存储和显示API通话的服务名称。该日期会在配置文件面板时间轴上突出显示。对于在该日期之前发生的活动，服务名称为未知服务。

活动详细信息的内容 (用户、角色、账户、角色会话、EC2实例、S3 存储桶)

对于IAM用户、IAM角色、账户、角色会话、EC2实例和 S3 存储桶，活动详细信息包含以下信息：

- 每个选项卡都提供有关在所选时间范围内发出的一组API呼叫的信息。

对于 S3 存储桶，该信息反映了对 S3 存储桶的API调用。

这些API呼叫按呼叫它们的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

- 对于每个条目，活动详细信息显示成功和失败的调用次数。观察到的 IP 地址选项卡还显示每个 IP 地址的位置。
- 每个条目都显示进行调用者的信息。对于账户，活动详细信息可用于确定用户或角色。对于角色而言，活动详细信息可用于确定角色会话。对于用户和角色会话，活动详细信息标识了访问密钥标识符 (AKIDs)。

请注意，自 2021 年 7 月 14 日起，对于账户资料，活动详情显示的是用户或角色，而不是 AKIDs。对于角色配置文件，活动详细信息显示的是角色会话，而不是 AKIDs。对于 2021 年 7 月 14 日之前发生的活动，调用者被列为未知资源。

活动详细信息包含以下选项卡：

观察到的 IP 地址

最初显示用于发出 API 呼叫的 IP 地址列表。

您可以展开每个 IP 地址以显示从该 IP 地址发出的 API 呼叫列表。这些 API 呼叫按呼叫它们的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

然后，您可以展开每个 API 呼叫以显示来自该 IP 地址的来电者列表。根据个人资料，来电者可能是用户、角色、角色会话或 AKID。

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | API method by service | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

IP address	Successful calls	Failed calls	Location
10.0.0.0/24	421	311	-
s3	316	311	
config	61	0	
kms	15	0	
DescribeKey	14	0	
DescribeKey	14	0	
ListKeys	1	0	
rds	7	0	
ec2	4	0	
autoscaling	3	0	
secretsmanager	2	0	
guardduty	2	0	
es	2	0	

API 按服务分类的方法

最初显示已发出的 API 呼叫列表。API 呼叫按发出呼叫的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

您可以展开每种 API 方法以显示发出呼叫的 IP 地址列表。

然后，您可以展开每个 IP 地址以显示从该 IP 地址发出API呼叫的列表。AKIDs

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses

API method by service

Resource

Q Filter by IP CIDR, Service name, API Method name, or Resource string

< 1 2 >

API method ▾	Successful calls ▾	Failed calls ▾
▶ s3	316	311
▶ config	61	0
▼ kms	15	0
▼ DescribeKey	14	0
▶ Role session	14	0
▶ ListKeys	1	0
▶ rds	7	0
▶ ec2	4	0
▶ autoscaling	3	0
▶	...	...

资源或访问密钥 ID

最初显示用户、角色、角色会话或AKIDs用于发出API呼叫的用户列表。

您可以展开每个来电者以显示来电者发出API呼叫的 IP 地址列表。

然后，您可以展开每个 IP 地址以显示该API呼叫者从该 IP 地址发出的呼叫列表。API呼叫按发出呼
叫的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的
服务，则该调用将列在未知服务下。

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses

API method by service

Resource

Q Filter by IP CIDR, Service name, API Method name, or Resource string

< 1 2 >

Resource ▾	Successful calls ▾	Failed calls ▾
▶ Role session	322	310
▼ Role session	91	0
▼ Role session	91	0
▶ config	61	0
▼ kms	15	0
DescribeKey	14	0
ListKeys	1	0
▶ ec2	3	0
secretsmanager	2	0
guardduty	2	0
...	...	...

活动详细信息的内容 (IP 地址)

对于 IP 地址，活动详细信息包含以下信息：

- 每个选项卡都提供有关在所选时间范围内发出的一组API呼叫的信息。API呼叫按发出呼
叫的服务进行分组。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。
- 对于每个条目，活动详细信息显示成功和失败的调用次数。

活动详细信息包含以下选项卡：

资源

最初显示从该 IP 地址发出API呼叫的资源列表。

对于每种资源，列表都包括资源名称、类型和 AWS 账户。

您可以展开每个资源以显示该资源从该 IP 地址发出的API呼叫列表。API呼叫按发出呼叫的服务进行分组。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource

API method by service

Filter by Resource string, Service name or API Method name

< 1 2 3 4 >

Resource	Successful calls	Failed calls	Account ID
▼ AWS role	3,520	0	
▼ config	1,754	0	
DescribeComplianceByConfigRule	1,408	0	
PutEvaluations	244	0	
SelectResourceConfig	78	0	
DescribeDeliveryChannelStatus	8	0	
DescribeConfigurationRecorderSta...	8	0	
DescribeConfigurationRecorders	8	0	
▶ ec2	1,690	0	
▶ shield	50	0	
▶ waf-regional	26	0	
▶ AWS role	1,715	0	
▶ AWS role	504	480	

API按服务分类的方法

最初显示已发出的API呼叫列表。API呼叫按发出呼叫的服务进行分组。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

您可以展开每个API呼叫以显示在所选时间段内从该 IP 地址发出API呼叫的资源列表。

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource

API method by service

Filter by Resource string, Service name or API Method name

< 1 2 3 4 >

API method	Successful calls	Failed calls
▶ config	3,787	0
▶ ec2	2,538	0
▶ s3	1,269	1,016
▼ ssm	481	16
▼ ListCommands	392	0
AWS role	222	0
AWS role	170	0
▶ SendCommand	89	16
▶ logs	165	0
▶ sts	149	0
▶ iam	149	12

对活动详细信息进行排序

您可以按列表中的任何一列对活动 ([活动详细信息]) 进行排序。

使用第一列进行排序时，只对顶层列表进行排序。较低级别的列表始终按成功API呼叫次数排序。

筛选活动详细信息

您可以使用筛选选项将重点放在活动 ([活动详细信息]) 中表示的活动的特定子集或方面。

在所有选项卡上都可以根据第一列中的任何值筛选列表。

添加筛选器

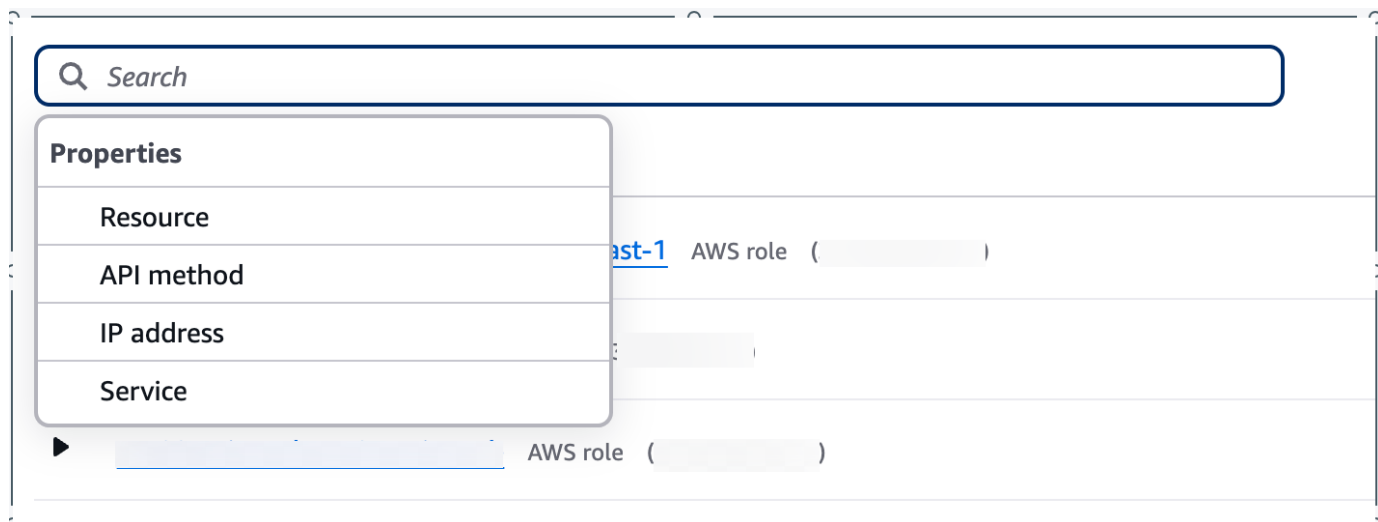
1. 选择筛选器框。
2. 从属性中，选择要用于筛选的属性。
3. 提供用于筛选的值。筛选器支持部分值。例如，当您按方法筛选时，如果按API方法进行筛选 **Instance**，则结果将包括其名称Instance中包含的所有API操作。因此，ListInstanceAssociations 和 UpdateInstanceInformation 都能匹配。

对于服务名称、API方法和 IP 地址，您可以指定值或选择内置过滤器。

对于“常用API子字符串”，选择表示操作类型的子字符串，例如ListCreate、或。Delete每个API方法名称都以操作类型开头。

对于CIDR模式，您可以选择仅包含公有 IP 地址、私有 IP 地址或与特定CIDR模式匹配的 IP 地址。

4. 选择布尔值选项 **Resource** 或 **Service**：包含或！：不包含；或 **API method** 或 **IP address** = 等于或！：不等于设置过滤器。



要删除筛选器，请选择标签右上角的 x 标记。

要清除所有筛选器，请选择清除筛选器。

为活动详细信息选择时间范围

首次显示活动详细信息时，时间范围是范围时间或选定的时间间隔。您可以更改活动详细信息的时间范围。

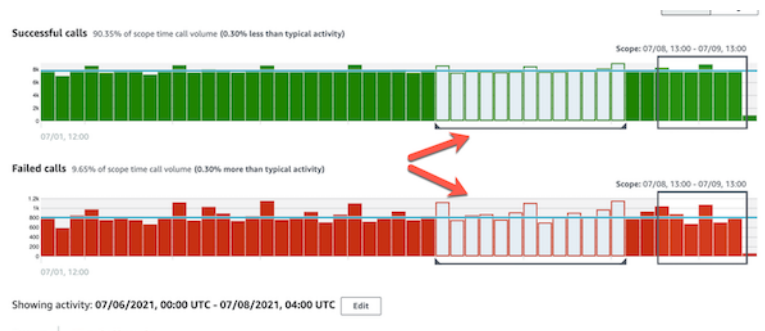
要更改活动详细信息的时间范围

1. 选择编辑。
2. 在编辑时间窗口上，选择要使用的开始和结束时间。

要将时间窗口设置为配置文件的默认范围时间，请选择设置为默认范围时间。

3. 选择更新时间窗口。

活动详细信息的时间范围在配置文件面板图表上突出显示。



查询原始日志

Amazon Detective 与 Amazon Security Lake 集成，这意味着您可以查询和检索 Security Lake 存储的原始日志数据。有关此集成的更多信息，请参阅[Detective 与安全湖集成](#)。

使用此集成，您可以从 Security Lake 原生支持的以下来源收集和查询日志与事件。

- AWS CloudTrail 管理事件版本 1.0 及更高版本
- 亚马逊 Virtual Private Cloud (亚马逊VPC) 流日志 1.0 及更高版本
- 亚马逊 Elastic Kubernetes Service (EKS亚马逊) 审核日志 2.0 版

Note

在 Detective 中查询原始数据日志不会产生额外费用。包括亚马逊 Athena 在内的其他 AWS 服务的使用费仍按公布费率收取。

查询原始日志

1. 选择显示时间范围的详细信息。
2. 在此处，您可以开始查询原始日志。
3. 在原始日志预览表中，您可以查看通过查询 Security Lake 数据检索到的日志和事件。有关原始事件日志的更多详细信息，您可以查看 Amazon Athena 中显示的数据。

在查询原始日志表中，您可以取消查询请求，在 Amazon Athena 中查看结果，并下载结果 [下载为逗号分隔值 (.csv) 文件]。

如果您在 Detective 中看到日志，但查询未返回任何结果，则可能是由于以下原因而引起的。

- 原始日志可能会先在 Detective 中可用，然后才显示在 Security Lake 日志表中。请稍后重试。
- Security Lake 中可能缺少日志。如果您等待了很长时间，则表示 Security Lake 中缺少日志。要解决该问题，请联系您的 Security Lake 管理员。

地理位置的活动详细信息

新观察到的地理位置的活动详细信息显示了在瞄准镜时间内从地理位置发出的API呼叫。这些API呼叫包括从地理位置发出的所有呼叫。它们不限于使用调查发现或配置文件实体的调用。对于 S3 存储桶，活动调用是对 S3 存储桶的API调用。

Detective 使用 MaxMind GeoIP 数据库确定请求的位置。MaxMind 尽管准确性因国家和知识产权类型等因素而异，但它们在国家一级的数据的准确性非常高。有关的更多信息 MaxMind，请参阅 [MaxMind IP 地理定位](#)。如果您认为任何 GeoIP 数据不正确，可以通过“更正地理数据”向 Maxmind 提交更[MaxMind 正](#)请求。IP2

API呼叫按发出呼叫的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

要显示活动详细信息，请执行以下操作之一：

- 在地图上选择一个地理位置。
- 在列表中，选择地理位置的详细信息。

活动详细信息取代了地理位置列表。要返回到地理位置列表，请选择返回到所有结果。

请注意，从2021年7月14日起，Detective开始存储和显示API通话的服务名称。对于在该日期之前发生的活动，服务名称为未知服务。

活动详细信息的内容

每个选项卡都提供有关在范围时间内从地理位置发出的所有API呼叫的信息。

对于每个 IP 地址、资源和API方法，列表都显示成功和失败的API呼叫数。

活动详细信息包含以下选项卡：

观察到的 IP 地址

最初显示用于从所选地理位置发出API呼叫的 IP 地址列表。

您可以展开每个 IP 地址以显示从该 IP 地址发出API呼叫的资源。列表显示资源名称。要查看主体 ID，请将鼠标悬停在名称上。

然后，您可以展开每个资源以显示该资源从该 IP 地址发出的特定API呼叫。API呼叫按发出呼叫的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

Ashburn, US from 05/14/2021 - 06/28/2021

Observed IP addressesResource

Filter by IP CIDR, API Method name, or Resource string

IP address	Successful calls	Failed calls
10.0.0.0/24	27,564	2,453
10.0.0.0/24 AWS role	27,564	2,453
ssm	25,111	0
UpdateInstanceInformation	13,066	0
ListInstanceAssociations	6,482	0
PutInventory	2,544	0
GetDeployablePatchSnapshotForIns...	2,453	0
UpdateInstanceAssociationStatus	466	0
PutComplianceItems	98	0
GetDocument	2	0
sts	2,453	0
s3	0	2,453
10.0.0.0/24	24,635	1,512
10.0.0.0/24	24,632	1,511

资源

最初显示从所选地理位置发出API呼叫的资源列表。列表显示资源名称。要查看主体 ID，请在名称上暂停一下。对于每种资源，资源选项卡还会显示关联的 AWS 账户。

您可以展开每个用户或角色以显示该资源发出的API呼叫列表。API呼叫按发出呼叫的服务进行分组。对于 S3 存储桶，服务始终是 Amazon S3。如果 Detective 无法确定发出调用的服务，则该调用将列在未知服务下。

然后，您可以展开每个API呼叫以显示资源发出API呼叫的 IP 地址列表。

Ashburn, US from 05/14/2021 - 06/28/2021

Observed IP addressesResource

Filter by IP CIDR, API Method name, or Resource string

Resource	Successful calls	Failed calls	Account ID
10.0.0.0/24 AWS role	189,097	17	123456789012
10.0.0.0/24 AWS role	49,267	3,023	123456789012
ssm	46,254	0	
UpdateInstanceInformation	25,932	0	
10.0.0.0/24	12,968	0	
10.0.0.0/24	12,964	0	
ListInstanceAssociations	12,964	0	
PutInventory	3,194	0	
GetDeployablePatchSnapshotForIns...	3,011	0	
UpdateInstanceAssociationStatus	949	0	
PutComplianceItems	199	0	
GetDocument	5	0	
sts	3,013	0	
s3	0	3,023	

对活动详细信息进行排序

您可以按列表中的任何一列对活动详细信息进行排序。

使用第一列进行排序时，只对顶层列表进行排序。较低级别的列表始终按成功API呼叫次数排序。

筛选活动详细信息

您可以使用筛选选项将重点放在活动详细信息中表示的活动的特定子集或方面。

在所有选项卡上都可以根据第一列中的任何值筛选列表。

添加筛选器

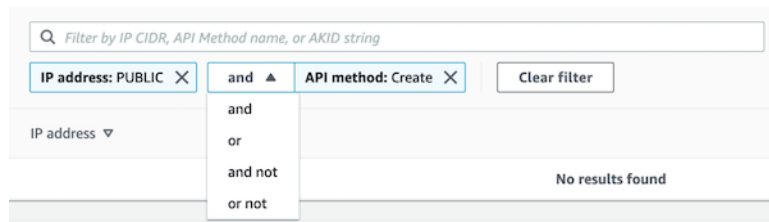
1. 选择筛选器框。
2. 从属性中，选择要用于筛选的属性。
3. 提供用于筛选的值。筛选器支持部分值。例如，当您按方法筛选时，如果按API方法进行筛选**Instance**，则结果将包括其名称Instance中包含的所有API操作。因此，`ListInstanceAssociations` 和 `UpdateInstanceInformation` 都能匹配。

对于服务名称、API方法和 IP 地址，您可以指定值或选择内置过滤器。

对于“常用API子字符串”，选择表示操作类型的子字符串，例如ListCreate、或。Delete每个API方法名称都以操作类型开头。

对于CIDR模式，您可以选择仅包含公有 IP 地址、私有 IP 地址或与特定CIDR模式匹配的 IP 地址。

4. 如果您有多个筛选器，请选择 Boolean 选项来设置这些筛选器的连接方式。



5. 要删除筛选器，请选择标签右上角的 x 标记。
6. 要清除所有筛选器，请选择清除筛选器。

总VPC流量的活动详情

对于EC2实例，“总VPC流量”的活动详细信息显示了选定时间范围内EC2实例与 IP 地址之间的交互情况。

对于 Kubernetes 容器，总体VPC流量显示所有目标 IP 地址的 Kubernetes 容器分配的 IP 地址的进出字节总量。在 `hostNetwork:true` 时，Kubernetes 容器组 (pod) 的 IP 地址不是唯一的。在这种情况下，面板会显示到具有相同配置的其他容器组 (pod) 的流量以及托管它们的节点。

对于 IP 地址，“总VPC流量”的活动详细信息显示了选定时间范围内该 IP 地址与EC2实例之间的交互情况。

要显示单个时间间隔的活动详细信息，请选择图表上的时间间隔。

要显示当前范围时间的活动详细信息，请选择显示范围时间的详细信息。

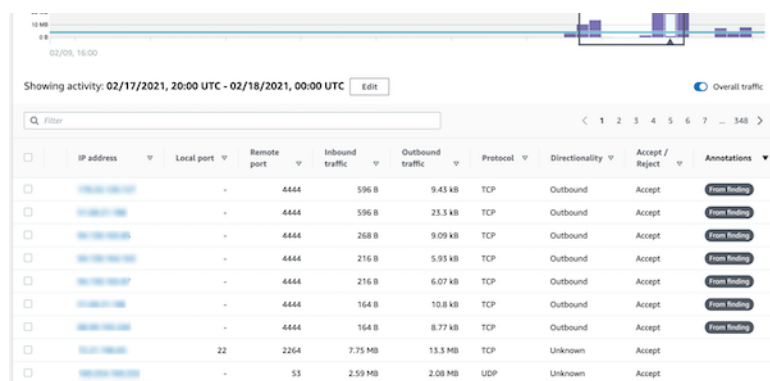
活动详细信息的内容

内容反映所选时间范围内的活动。

对于EC2实例，活动详细信息包含 IP 地址、本地端口、远程端口、协议和方向的每个唯一组合的条目。

对于 IP 地址，活动详细信息包含EC2实例、本地端口、远程端口、协议和方向的每个唯一组合的条目。

每个条目都显示入站流量、出站流量以及访问请求是被接受还是被拒绝。在调查发现配置文件上，注释列会指示 IP 地址何时与当前调查发现相关。



	IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Annotations
☐	10.0.0.1	-	4444	596 B	9.43 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	596 B	25.3 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	268 B	9.09 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	216 B	5.93 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	216 B	6.07 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	164 B	10.8 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	-	4444	164 B	8.77 kB	TCP	Outbound	Accept	From Finding
☐	10.0.0.1	22	2264	7.75 MB	13.3 MB	TCP	Unknown	Accept	
☐	10.0.0.1	-	53	2.59 MB	2.08 MB	UDP	Unknown	Accept	

对活动详细信息进行排序

您可以按表中的任何一列对活动详细信息进行排序。

默认情况下，活动详细信息首先按照注释排序，然后按照入站流量排序。

筛选活动详细信息

要关注特定活动，您可以按以下值筛选活动详细信息：

- IP 地址或EC2实例
- 本地或远程端口
- 方向

- 协议
- 请求是被接受还是被拒绝

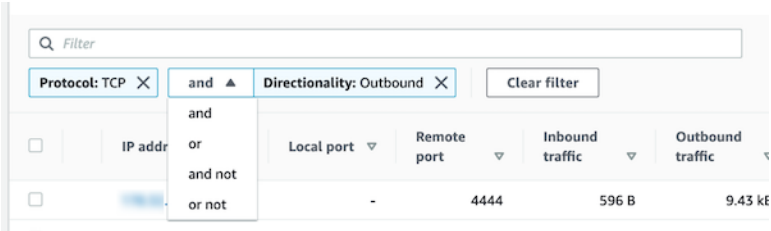
要添加和删除筛选器

1. 选择筛选器框。
2. 从属性中，选择要用于筛选的属性。
3. 提供用于筛选的值。筛选器支持部分值。

要按 IP 地址进行筛选，您可以指定一个值或选择一个内置筛选器。

对于CIDR模式，您可以选择仅包含公有 IP 地址、私有 IP 地址或与特定CIDR模式匹配的 IP 地址。

4. 如果您有多个筛选器，请选择 Boolean 选项来设置这些筛选器的连接方式。



5. 要删除筛选器，请选择标签右上角的 x 标记。
6. 要清除所有筛选器，请选择清除筛选器。

为活动详细信息选择时间范围

首次显示活动详细信息时，时间范围是范围时间或选定的时间间隔。您可以更改活动详细信息的时间范围。

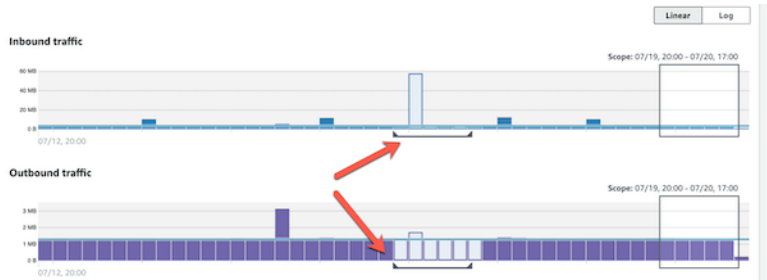
要更改活动详细信息的时间范围

1. 选择编辑。
2. 在编辑时间窗口上，选择要使用的开始和结束时间。

要将时间窗口设置为配置文件的默认范围时间，请选择设置为默认范围时间。

3. 选择更新时间窗口。

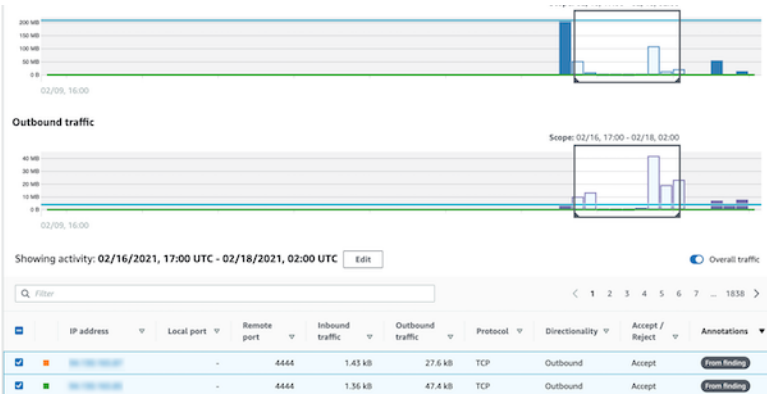
活动详细信息的时间范围在配置文件面板图表上突出显示。



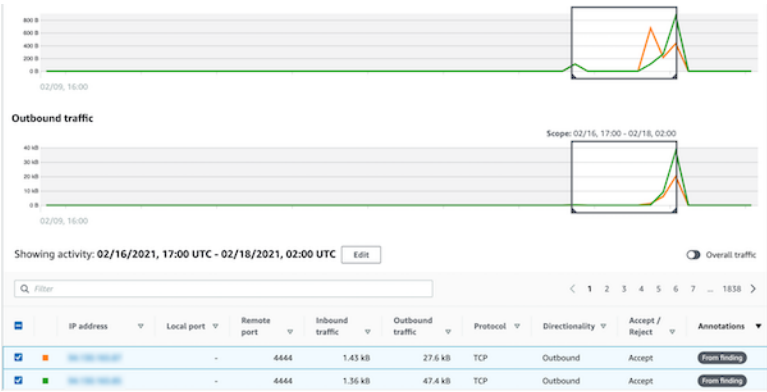
显示选定行的流量

当您确定了感兴趣的行，就可以在主图表上显示这些行在一段时间内的流量。

对于要添加到图表中的每行，请选中该复选框。对于选定的每行，容量在入站或出站图表上显示为一条线。



要关注所选条目的流量，您可以隐藏总流量。要显示或隐藏总流量，请切换总流量。



显示集EKS群的VPC流量流量

Detective 可以看到你的亚马逊虚拟私有云 (亚马逊VPC) 流日志，这些日志代表了穿越你的亚马逊 Elastic Kubernetes Service (亚马逊) 集群的流量。EKS对于 Kubernetes 资源，VPC流日志的内容取决于集群中部署的容器网络接口 (CNI)。EKS

具有默认配置的EKS集群使用 Amazon VPC CNI 插件。有关更多详细信息，请参阅 Amazon EKS 用户指南VPC CNI中的[管理](#)。Amazon VPC CNI 插件使用容器的 IP 地址发送内部流量，并将源 IP 地址转换为节点的 IP 地址以进行外部通信。Detective 可以捕获内部流量并将其关联到正确的容器组（pod），但却无法捕获外部流量。

如果你想让 Detective 可以看到你的 pod 的外部流量，请启用“外部源网络地址转换”（SNAT）。启用 SNAT有其局限性和缺点。有关更多详细信息，[SNAT请参阅《Amazon EKS 用户指南》中的 pod](#)。

如果你使用其他CNI插件，Detective 对带有 pod 的可见性有限hostNetwork:true。对于这些 pod，Flo VPCw 面板会显示发往该容器的 IP 地址的所有流量。这包括到主机节点的流量，以及任何具有 hostNetwork:true 配置的节点上容器组（pod）的流量。

Detective 在EKS容器的VPC流量面板中显示以下EKS集群配置的流量：

- 在带有 Amazon VPC CNI 插件的集群中，任何具有该配置的 pod 都会在VPC集群内部hostNetwork:false发送流量。
- 在带有 Amazon VPC CNI 插件和配置的集群中AWS_VPC_K8S_CNI_EXTERNALSNAT=true，任何在VPC集群之外hostNetwork:false发送流量的容器。
- 任何具有配置 hostNetwork:true 的容器组（pod）。来自该节点的流量会与来自其他具有配置 hostNetwork:true 的容器组（pod）的流量混合在一起。

Detective 不会在VPC流量面板中显示以下各项的流量：

- 在带有 Amazon VPC CNI 插件和配置的集群中AWS_VPC_K8S_CNI_EXTERNALSNAT=false，任何具有该配置的 pod 都会向集群外部hostNetwork:false发送流量。VPC
- 在没有适用于 Kubernetes 的 Amazon VPC CNI 插件的集群中，任何具有该配置的 pod。hostNetwork:false
- 任何向托管在同一节点中的另一个容器组发送流量的容器组（pod）。

显示共享的 Amazon 的VPC流量 VPCs

Detective 可以查看你的 Amazon Virtual Private Cloud（亚马逊VPC）共享的流日志VPCs：

- 如果 Detective 成员账户有共享的 Amazon VPC而其他非侦探账户使用共享的亚马逊VPC，则 Detective 会监控来自该账户的所有流量VPC，并提供内部所有流量的可视化效果。VPC

- 如果您在共享的亚马逊内有一个亚马逊EC2实例，VPC并且共享VPC所有者不是侦探会员，则 Detective 将不会监控来自该服务器的任何流量VPC。如果您想查看其中的流量VPC，则必须将亚马逊VPC所有者添加为 Detective 图表的成员。

涉及集群的 Kubernetes API 总体活动 EKS

涉及EKS集群的整体 Kubernetes API 活动的活动详细信息显示了在选定时间范围内发出的成功和失败的 Kubernetes API 调用的数量。

要显示单个时间间隔的活动详细信息，请选择图表上的时间间隔。

要显示当前范围时间的活动详细信息，请选择显示范围时间的详细信息。

活动详细信息的内容 (集群、容器组 (pod)、用户、角色、角色会话)

对于集群、容器组 (pod)、用户、角色或角色会话，活动详细信息包含以下信息：

- 每个选项卡都提供有关在所选时间范围内发出的一组API呼叫的信息。

对于集群，API呼叫发生在集群内部。

对于 pod，API调用目标是 pod。

对于用户、角色和角色会话，API调用是由经过身份验证为该用户、角色或角色会话的 Kubernetes 用户发出的。

- 对于每个条目，活动详细信息都显示成功、失败、未经授权和禁止的调用次数。
- 这些信息包括 IP 地址、Kubernetes 调用类型、受调用影响的实体以及进行调用的主体 (服务账户或用户)。从活动详细信息中，您可以转到 IP 地址、主题和受影响实体的配置文件。

活动详细信息包含以下选项卡：

主题

最初显示用于拨API打电话的服务帐户和用户的列表。

您可以展开每个服务帐号和用户，以显示该账户或用户从中API拨打电话的 IP 地址列表。

然后，您可以展开每个 IP 地址以显示该账户或用户从该 IP 地址发出的 Kubernetes API 调用。

展开 Kubernetes API 调用以查看，requestURI 以识别已完成的操作。

Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC

Edit

Subject

IP address

Kubernetes API call

Filter by Kubernetes subject, IP CIDR, API verb, or API method name

< 1 2 3 >

Subject ▾	Success ▾	Failure ▾	Unauthorized ▾	Forbidden ▾
cloud-controller-manager Kubernetes user	186,651	1	0	0
10.0.100.200 IP address	161,406	1	0	0
▶ update	80,343	0	0	0
▶ get	80,343	1	0	0
▶ watch	720	0	0	0
▶ 10.0.0.0/24 IP address	25,245	0	0	0

IP 地址

最初显示API发出呼叫的 IP 地址列表。

您可以展开每个调用，显示发出该调用的 Kubernetes 主题（服务账号和用户）列表。

然后，您可以将每个主体展开为该主体在作用域时间内拨打的API呼叫类型列表。

展开API呼叫类型以查看请求URI以识别已完成的操作。

Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC

Edit

Subject

IP address

Kubernetes API call

Filter by Kubernetes subject, IP CIDR, API verb, or API method name

< 1 2 3 4 5 6 7 ... 27 >

IP address ▾	Success ▾	Failure ▾	Unauthorized ▾	Forbidden ▾	Location ▾
10.0.100.200 IP address	599,250	2,706	0	0	-
cloud-controller-manager Kubernetes user	161,406	1	0	0	
update	80,343	0	0	0	
/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-provider-extraction-migration	40,172	0	0	0	
/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-controller-manager	40,171	0	0	0	

Kubernetes 调用 API

最初显示 Kubernetes 的调API用动词列表。

您可以展开每个API动词以显示 requestURIs 与该动作相关的动词。

然后，你可以展开每个请求URI以查看发出调用的 Kubernetes 主体（服务账号和用户）。API

展开主题以查看IPs该主体曾经拨打过API电话。

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses

API method by service

Resource

Q Filter by IP CIDR, Service name, API Method name, or Resource string

Resource	Successful calls	Failed calls
▶ ... Role session (...)	322	310
▼ ... Role session (...)	91	0
▼ ...	91	0
▶ config	61	0
▼ kms	15	0
DescribeKey	14	0
ListKeys	1	0
▶ ec2	3	0
secretsmanager	2	0
guardduty	2	0
...	...	...

对活动详细信息进行排序

您可以按列表中的任何一列对活动详细信息进行排序。

使用第一列进行排序时，只对顶层列表进行排序。较低级别的列表始终按成功API呼叫次数排序。

筛选活动详细信息

您可以使用筛选选项将重点放在活动详细信息中表示的活动的特定子集或方面。

在所有选项卡上都可以根据第一列中的任何值筛选列表。

为活动详细信息选择时间范围

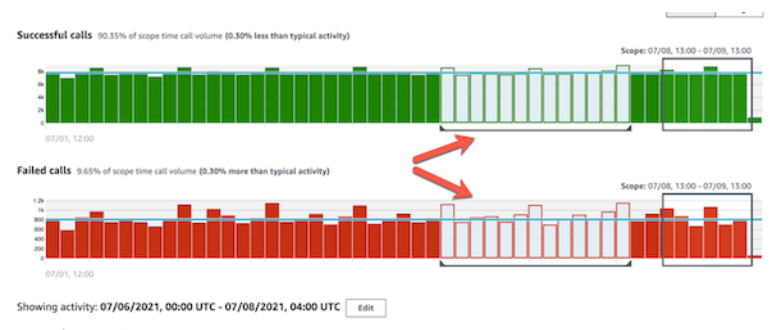
首次显示活动详细信息时，时间范围是范围时间或选定的时间间隔。您可以更改活动详细信息的时间范围。

要更改活动详细信息的时间范围

1. 选择编辑。
2. 在编辑时间窗口上，选择要使用的开始和结束时间。

要将时间窗口设置为配置文件的默认范围时间，请选择设置为默认范围时间。
3. 选择更新时间窗口。

活动详细信息的时间范围在配置文件面板图表上突出显示。



在调查期间使用配置文件面板指南

每个配置文件面板都旨在为在进行调查和分析相关实体的活动时出现的特定问题提供答案。

为每个配置文件面板提供的指南有助于您找到这些答案。

配置文件面板指南以面板本身的一句话开头。本指南简要说明了面板上显示的数据。

要显示面板的更详细指南，请从面板标题中选择更多信息。此扩展指南显示在帮助窗格中。

该指南可以提供以下类型的信息：

- 面板内容概述
- 如何使用面板回答相关问题
- 根据答案建议的后续步骤

管理范围时间

自定义用于限制实体配置文件上显示的数据的范围时间。

实体配置文件上显示的图表、时间轴和其他数据均基于当前的范围时间。范围时间是实体在一段时间内的活动摘要。它显示在 Amazon Detective 控制台中每个配置文件的右上角。这些图表、时间轴和其他可视化内容上显示的数据基于范围时间。对于某些配置文件面板，在范围时间之前和之后会增加额外时间以提供上下文情况。在 Detective 中，所有时间戳默认都以 UTC 显示。您可以通过更改时间戳首选项来选择本地时区。要更新时间戳首选项，请参阅[the section called “设置时间戳格式”](#)。

Detective 分析在检查异常活动时使用范围时间。分析流程获取范围时间内的活动，然后将其与范围时间之前 45 天内的活动进行比较。它还利用这 45 天的时间框架来生成活动基线。

在调查发现概述中，范围时间反映了第一次和最后一次观察到该调查发现的时间。有关调查发现概述的更多信息，请参阅[the section called “调查发现概述”](#)。

您可以在进行调查时调整范围时间。例如，如果最初的分析基于某一天的活动，则您可能需要将其延长到一周或一个月。延长的时间有助于您更好地了解活动是符合正常模式还是异常。

您还可以设置范围时间，使其与当前实体的关联调查发现相匹配。

当您要更改范围时间时，Detective 会根据新的范围时间重复分析并更新显示的数据。

范围时间不能短于一小时，也不能长于一年。开始时间和结束时间必须以小时为单位。

设置具体的开始和结束日期和时间

您可以从 Detective 控制台设置范围时间的开始和结束日期。

要为新的范围时间设置具体的开始和结束时间

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在实体配置文件上，选择范围时间。
3. 在编辑范围时间面板的开始下，为范围时间选择新的开始日期和时间。对于新的开始时间，您只需选择小时。
4. 在结束下，为范围时间选择新的结束日期和时间。对于新的结束时间，您只需选择小时。结束时间必须比开始时间晚至少一个小时。
5. 编辑完成后，要保存更改并更新显示的数据，请选择更新范围时间。

编辑范围时间的时间长度

设置范围时间长度时，Detective 会将范围时间设置为从当前时间算起的时间量。

要编辑范围时间的时间长度

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在实体配置文件上，选择范围时间。
3. 在编辑范围时间面板的历史旁边，选择范围时间的时间长度。

指定时间范围会更新开始和结束设置。

4. 编辑完成后，要保存更改并更新显示的数据，请选择更新范围时间。

将范围时间设置为调查发现时间窗口

每个调查发现都有一个关联的时间窗口，它反映了第一次和最后一次观察到该调查发现的时间。查看调查发现概述时，范围时间会更改为调查发现时间窗口。

在实体配置文件中，您可以将范围时间与关联调查发现的时间窗口保持一致。这样您就可以调查这段时间内发生的活动。

要将范围时间与调查发现时间窗口保持一致，请在关联调查发现面板上选择您要使用的调查发现。

Detective 会填充搜索调查发现详细信息，并将范围时间设置为调查发现时间窗口。

在摘要页面设置范围时间

查看摘要页面时，您可以调整范围时间，以查看过去 365 天内任意 24 小时时间段的活动。

要在“摘要”页面上设置范围时间

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择摘要。
3. 在范围时间面板的摘要旁边，您可以更改开始日期和时间。开始时间必须在过去 365 天内。

更改开始日期和时间后，结束日期和时间会自动更新为所选开始时间后的 24 小时。

Note

使用 Detective，您最多可以访问一年的历史事件数据。有关 Detective 中源数据的更多信息，请参见[行为图中使用的源数据](#)。

4. 编辑完成后，要保存更改并更新显示的数据，请选择更新范围时间。

在 Detective 中查看相关发现的详细信息

每个实体配置文件都包含一个关联调查发现的面板，其中列出了在当前范围时间内涉及该实体的调查发现。一个实体遭到入侵的一个迹象是它涉及了多项调查发现。调查发现的类型还可以让人们深入了解需要关注的活动类型。

关联调查发现的面板显示在实体详细信息配置面板的正下方。

对于每个调查发现，该表包含以下信息：

- 调查发现标题，也是指向调查发现概述的链接。
- 与调查结果关联的 AWS 账户，也是指向账户资料的链接
- 调查发现类型。
- 最早观察到这一调查发现的时间
- 最近一次观察到这一调查发现的时间
- 调查发现的严重性

要显示调查发现的调查发现详细信息，请选择该调查发现的单选按钮。Detective 填充页面右侧的调查发现详细信息面板。Detective 还将范围时间更改为调查发现时间窗口。这样就可以专注于这段时间内发生的活动。

如果您从调查发现概述导航到实体配置文件，则会自动选择该调查发现并显示调查发现的详细信息。

在调查发现详细信息中，要导航返回调查发现概述，请选择查看所有相关实体。

您也可以将调查发现存档。如需了解更多详情，请参阅[存档 Amazon GuardDuty 调查结果](#)。

在 Detective 中查看大量实体的详细信息

在[行为图](#)中，Amazon Detective 跟踪实体之间的关系。例如，每个行为图都会跟踪 AWS 用户何时创建 AWS 角色以及 EC2 实例何时连接到 IP 地址。

当一个实体在一段时间内有太多关系时，Detective 无法存储所有关系。如果在当前范围时间内发生这种情况，Detective 会通知您。Detective 还提供了大量实体出现的列表。

什么是大量实体？

在给定的时间间隔内，实体可能是大量连接的起点或目的地。例如，一个 EC2 实例可能有来自数百万个 IP 地址的连接。

Detective 对在每个时间间隔内可以容纳的连接数量设有限制。如果实体超过该限制，则 Detective 将丢弃该时间间隔内的连接。

例如，假设每个时间间隔的限制为 1 亿个连接。如果在某个时间间隔内通过超过 1 亿个 IP 地址连接到 EC2 实例，则 Detective 会丢弃该时间间隔内的连接。

但是，您也许可以根据关系另一端的实体来分析该活动。继续举例来说，虽然一个 EC2 实例可能从数百万个 IP 地址连接，但一个 IP 地址连接到的 EC2 实例要少得多。每个 IP 地址配置文件都提供有关 IP 地址所连接的 EC2 实例的详细信息。

在配置文件上查看大量实体通知

如果调查发现或实体配置文件的范围时间包含实体的超长时间间隔，则 Detective 会在调查发现或实体配置文件的顶部显示一条通知。为了调查发现配置文件，该通知是针对相关实体的。

该通知中包括具有超长时间间隔的关系列表。每个列表条目都包含对关系的描述以及超长时间间隔的起始时间。

超长时间间隔可能表明存在可疑活动。要了解同时发生了哪些其他活动，您可以将调查重点放在超长时间间隔上。大量实体通知包括将范围时间设置为该时间间隔的选项。

要将范围时间设置为超长时间间隔

1. 在大量实体通知中，选择时间间隔。
2. 在弹出式菜单上，选择应用范围时间。

查看当前范围时间内的大量实体列表

大量实体页面包含当前范围时间内的超长时间间隔和实体的列表。

要显示大量实体页面

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择大量实体。

列表中的每个条目都包含以下信息：

- 超长时间间隔的起始时间
- 实体的标识符和类型
- 关系的描述，例如“从 IP 地址连接的 EC2 实例”

您可以按任何一列对列表进行筛选和排序。您也可以导航到相关实体的实体配置文件。

要导航到实体的配置文件

1. 在大量实体列表中，选择要从中导航的行。
2. 选择使用超长范围时间查看配置文件。

当您要使用此选项导航到实体配置文件时，范围时间设置如下：

- 范围时间从超长时间间隔前 30 天开始。
- 范围时间在超长时间间隔结束时结束。

在 Detective 中搜索发现或实体

使用 Amazon Detective 搜索功能，您可以搜索调查发现或实体。从搜索结果中，您可以导航到实体配置文件或调查发现概述。如果搜索返回的结果超过 10000 个，则仅显示前 10000 个结果。更改排序顺序会改变返回的结果。

您可以将搜索结果导出为逗号分隔值 (.csv) 文件。该文件包含搜索页面中返回的数据。数据以逗号分隔值 (CSV) 格式导出。导出数据的文件名遵循模式 detective-page-panel-yyyy-mm-dd.csv 格式。您可以使用其他支持 CSV 导入的 AWS 服务、第三方应用程序或电子表格程序来操纵数据，从而丰富您的安全调查。

Note

如果当前正在导出数据，请等到导出完成后再尝试导出其他数据。

完成搜索

要完成搜索，请选择要搜索的实体类型。然后提供确切标识符或带有通配符 * 或 ? 的标识符。要搜索一定范围的 IP 地址，也可以使用 CIDR 或点符号。请参阅以下搜索字符串示例。

对于 IP 地址：

- 1.0.*.*
- 1.0.133.*
- 1.0.0.0/16
- 0.239.48.198/31

对于所有其他类型的实体：

- Admin
- ad*
- ad*n
- ad*n*
- adm?n
- a?m*

- *min

对于每种实体类型，都支持以下标识符：

- 对于调查结果，是查找标识符或查找 Amazon 资源名称 (ARN)。
- 对于 AWS 账户，为账户 ID。
- 对于 AWS 角色和 AWS 用户，可以是委托人 ID、姓名或ARN。
- 对于容器集群，使用集群名称或ARN。
- 对于容器映像，即存储库或容器映像的完整摘要。
- 对于容器 Pod 或 Tasks，是容器 Pod UID 的名称或 Pod 的。
- 对于EC2实例，请使用实例标识符或ARN。
- 对于调查发现群组，即调查发现群组标识符。
- 对于 IP 地址，使用CIDR或点号表示的地址。
- 对于 Kubernetes 主体（服务账户或用户），即名称。
- 对于角色会话，您可以使用以下任何值进行搜索：
 - 角色会话标识符。

角色会话标识符使用格式 `<rolePrincipalID>:<sessionName>`。

以下是一个示例：AROA12345678910111213:MySession。

- 角色会话 ARN
- 会话名称
- 所代入角色的主体 ID
- 所代入的角色的名称
- 对于 S3 存储桶，为存储桶名称或存储桶ARN。
- 对于联合用户，即主体 ID 或用户名。主体 ID 为 `<identityProvider>:<username>` 或 `<identityProvider>:<audience>:<username>`。
- 对于用户代理，即用户代理名称。

要搜索调查发现或实体

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。

2. 在导航窗格中，选择搜索。
3. 从选择类型菜单中，选择您要查找的项目类型。

请注意，选择用户时，您可以搜索 AWS 用户或联合用户。

数据示例包含行为图数据中选定类型标识符的样本集。要显示其中一个示例的配置文件，请选择其标识符。

4. 输入要搜索的确切标识符或带通配符的标识符。

搜索不区分大小写。

5. 选择搜索或按输入。

使用搜索结果

完成搜索后，Detective 会显示一个包含多达 10000 个匹配结果的列表。对于使用唯一标识符的搜索，只有一个匹配结果。

要从结果中浏览实体配置文件或调查发现概述，请选择标识符。

对于搜索结果、角色、用户和 EC2 实例，搜索结果包括关联的账户。要导航到该账户的配置文件，请选择账户标识符。

搜索故障排除

如果 Detective 找不到调查发现或实体，请先检查输入的标识符是否正确。如果标识符正确，您还可以检查以下内容。

- 在行为图中，该调查发现或实体是否属于已启用的成员账户？如果关联账户未被邀请以成员账户的身份访问行为图，则行为图中不包含该账户的数据。

如果受邀成员账户未接受邀请，则行为图中不包含该账户的数据。

- 对于调查发现，该调查发现是否存档？Detective 不会收到来自亚马逊的存档调查结果 GuardDuty。
- 这一调查发现或实体是否发生在 Detective 开始将数据导入行为图之前？如果 Detective 采集的数据中不存在该调查发现或实体，则行为图中就不包含相关数据。
- 调查发现或实体是否来自正确的区域？每个行为图都特定于 AWS 区域。行为图不包含来自其他区域的数据。

在 Detective 中管理账户

当一个账户启用 Detective 时，它会成为行为图的管理员账户，并为行为图选择成员账户。管理员账户可以邀请账号加入行为图。当账户接受邀请时，Detective 会将该账户启用为成员账户。通过邀请添加的成员账户可以从行为图中删除自己。

当一个账户被启用为成员账户时，Detective 就会开始摄取并提取该成员账户的数据到行为图中。

每个行为图表都包含来自一个或多个账户的数据。一张行为图最多可以有 1200 个成员账户。

如果您已与集成 AWS Organizations，则组织管理帐户会为该组织指定 Detective 管理员帐户。然后，该 Detective 管理员账户成为组织行为图的管理员账户。Detective 管理员账户在组织行为图中选择要作为成员账户启用的组织账户。组织账户不能从组织行为图中删除自己。

Detective 会根据每个账户为每个行为图提供的数据收取费用。有关在行为图中跟踪每个账户的数据量的信息，请参阅[预测和监控 Amazon Detective 成本](#)。

内容

- [Detective 中的账号限制和建议](#)
- [使用 Organizations 管理行为图账户](#)
- [为组织指定 Detective 管理员](#)
- [账户的可用操作](#)
- [查看账户列表](#)
- [以 Detective 成员账户的身份管理组织账户](#)
- [在 Detective 中管理受邀成员账户](#)
- [对于成员账号：管理行为图邀请和成员资格](#)
- [账户操作对行为图的影响](#)
- [使用 Detective Python 脚本管理账户](#)

Detective 中的账号限制和建议

管理 Amazon Detective 中的账户时，请注意以下限制和建议。

成员账户的最大数量

Detective 允许每个行为图中最多有 1200 个成员账户。

如果您使用 AWS Organizations 管理账户，默认情况下，Detective 会在账户管理页面上显示最多 5000 个成员账户。如果要查看所有帐户，请选择加载所有帐户。返回所有结果可能需要几分钟。

账户和区域

如果您使用 AWS Organizations 管理帐户，则组织管理帐户会为组织指定一个 Detective 管理员帐户。该 Detective 管理员账户成为组织行为图的管理员账户。

所有区域的 Detective 管理员账户必须相同。组织管理账户在每个区域分别指定 Detective 管理员账户。Detective 管理员账户还分别管理每个区域的组织行为图和成员账户。

对于通过邀请创建的成员账户，管理员-成员关联仅在发出邀请的区域创建。管理员账户必须在每个区域启用 Detective，并且每个区域都有单独的行为图。然后，管理员账户会邀请每个账户作为该区域的成员账户进行关联。

一个账户可以是同一区域内多个行为图的成员账户。每个区域只能有一个行为图的管理员账户。一个账户可以是不同区域的管理员账户。

使管理员帐户与 Security Hub 保持一致 GuardDuty

为确保与 Amazon AWS Security Hub 和 Amazon 的集成顺利 GuardDuty 进行，我们建议在所有这些服务中使用同一个账户作为管理员账户。

请参阅 [the section called “建议与 GuardDuty 和对齐 AWS Security Hub”](#)。

授予管理员账户所需的权限

为确保管理员账户拥有管理其行为图所需的权限，请将[AmazonDetectiveFullAccess托管策略](#)附加到IAM委托人。

在 Detective 中反映组织的最新动态

组织的更改不会立即反映在 Detective 中。

对于大多数更改，如新增和删除组织账户，Detective 可能需要一个小时才能收到通知。

对 Organizations 中指定的 Detective 管理员账户进行更改所需的传播时间较短。

使用 Organizations 管理行为图账户

可能有一个现有的行为图，其中包含接受手动邀请的成员账户。如果您已注册 AWS Organizations，请使用以下步骤使用 Organizations 来启用和管理成员账户，而不是使用手动邀请流程：

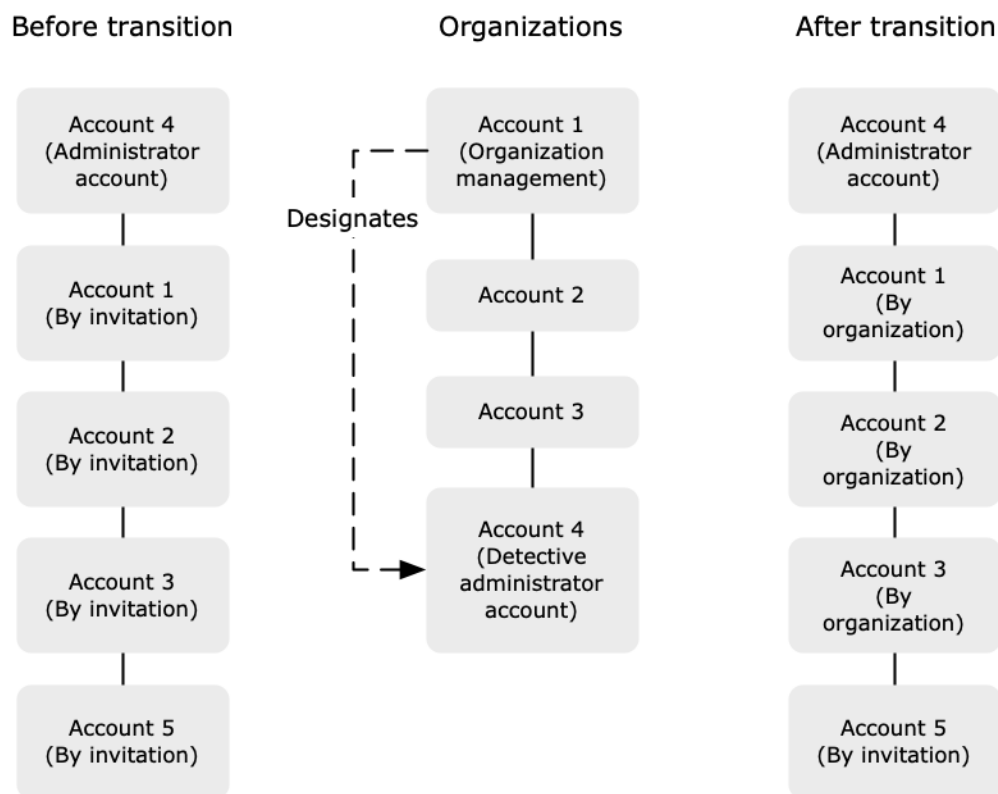
1. 为组织指定 Detective 管理员账户。这将创建组织行为图。

如果 Detective 管理员账户已有行为图，则该行为图就会成为组织行为图。

2. 启用组织账户作为组织行为图中的成员账户。

如果组织行为图中现有的成员账户为组织账户，则这些账户会自动启用。

下图显示了过渡前的行为图结构、Organizations 中的配置和过渡后的行为图账户结构概述。



为组织指定 Detective 管理员账户。

组织管理账户指定了您所在组织的 Detective 管理员账户。请参阅 [the section called “指定 Detective 管理员账户”](#)。

为了简化过渡，Detective 建议选择当前的管理员账户作为该组织的 Detective 管理员账户。

如果 Organizations 中有 Detective 的授权管理员账户，则必须使用该账户或组织管理账户作为 Detective 管理员账户。

否则，首次指定一个非组织管理账户的 Detective 管理员账户时，Detective 会调用 Organizations，将该账户设为 Detective 的授权管理员账户。

启用组织账户作为成员账户

Detective 管理员账户是组织行为图的管理员账户。Detective 管理员账户在组织行为图中选择要作为成员账户启用的组织账户。请参阅 [the section called “管理组织成员账户”](#)。

在账户页面，Detective 管理员账户可以访问所有组织账户。

如果 Detective 管理员账户已经是某个行为图的管理员账户，则该行为图就会成为组织行为图。在该行为图中已是成员账户的组织账户会自动启用为成员账户。其他组织账户的状态为非成员。

组织账户的类型为按组织，即使它们以前是按邀请的成员账户也是如此。

不属于该组织的成员账户的类型为按邀请。

账户管理页面还提供了自动启用新组织账户选项，可在新账户添加到组织时自动启用。请参阅 [the section called “启用新的组织账户”](#)。该选项最初处于关闭状态。

Detective 管理员账户首次显示账户管理页面时，会显示一条包含启用所有组织账户按钮的消息。选择启用所有组织账户时，Detective 会执行以下操作：

- 启用所有当前组织账户作为成员账户。
- 打开自动启用新组织账户的选项。

成员账户列表中还有一个启用所有组织账户选项。

为组织指定 Detective 管理员

在组织行为图中，Detective 管理员账户管理所有组织账户的行为图成员资格。

如何管理 Detective 管理员帐户 — 组织管理帐户为每个组织指定侦探管理员帐户 AWS 区域。

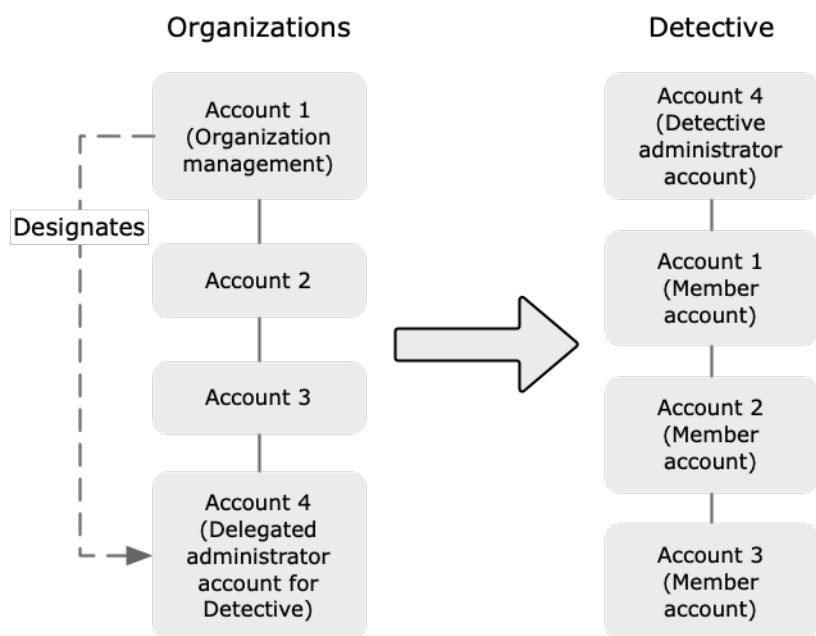
将 Detective 管理员帐户设置为委托管理员帐户 — Detective 管理员帐户也将成为 Detective 的委托管理员帐户 AWS Organizations。例外情况是组织管理帐户将自己指定为 Detective 管理员帐户。组织管理帐户不能是 Organizations 中的委托管理员。

在 Organizations 中设置委托管理员账户后，组织管理账户只能选择委托管理员账户或自己的账户作为 Detective 管理员账户。我们建议在所有区域选择委托管理员账户。

创建和管理组织行为图 — 当组织管理帐户选择 Detective 管理员帐户时，Detective 会为该帐户创建一个新的行为图表。该行为图就是组织行为图。

如果 Detective 管理员账户是现有行为图的管理员账户，则该行为图就会成为组织行为图。

Detective 管理员账户在组织行为图中选择要作为成员账户启用的组织账户。



Detective 管理员账户还可以向不属于该组织的账户发送邀请。有关更多信息，请参阅[the section called “管理组织成员账户”](#)和[the section called “管理受邀成员账户”](#)。

配置 Detective 管理员帐户所需的权限 — 为确保组织管理帐户能够配置 Detective 管理员帐户，您可以将[AmazonDetectiveOrganizationsAccess托管策略](#)附加到您的 AWS Identity and Access Management (IAM) 实体。

指定 Detective 管理员

组织管理账户可以使用 Detective 控制台来指定 Detective 管理员账户。

要管理 Detective 管理员账户，无需启用 Detective。您可以从启用 Detective 页面管理 Detective 管理员账户。

Enable Detective page (Console)

要从“启用侦探”页面指定 Detective 管理员，请按照以下步骤操作。

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 选择开始。
3. 在管理员账户所需权限面板中，为选择的账户授予必要的权限，使其能够作为 Detective 管理员的身份进行操作，并完全有权访问 Detective 中的所有操作。要以管理员身份进行操作，我们建议将 AmazonDetectiveFullAccess 策略附加到主体。

4. 从中选择附加策略IAM可直接在IAM控制台中查看推荐的策略。
5. 根据您在IAM控制台中是否拥有权限，请按以下步骤操作：
 - 如果您有权在IAM控制台中进行操作，请将推荐的策略附加到您用于 Detective 的主体。
 - 如果您无权在IAM控制台中进行操作，请复制策略的 Amazon 资源名称 (ARN) 并将其提供给您IAM管理员。然后，他们就可以代表您附加策略。
6. 在委托管理员下，选择 Detective 管理员账户。

可用的选项取决于是否拥有 Detective in Organizations 的委托管理员账户。

- 如果您没有 Detective in Organizations 的委托管理员账户，请输入该账户的账户标识符，将其指定为 Detective 管理员账户。

您可能已经拥有管理员账户，并通过手动邀请程序获得了行为图。如果是这样，我们建议将该账户指定为 Detective 管理员账户。

如果您在 Organizations for Amazon 中拥有委托管理员账户 GuardDuty，AWS Security Hub，或 Amazon Macie，然后 Detective 会提示你选择其中一个账户。也可以输入不同的账户。

- 如果您拥有 Detective in Organizations 的委托管理员账户，则系统会提示选择该账户或您的账户。我们建议在所有区域选择委托管理员账户。

7. 选择委托。

如果已启用 Detective，或者是现有行为图中的成员账户，则可以从常规页面指定 Detective 管理员账户。

General page (Console)

要从“常规”页面指定 Detective 管理员，请按照以下步骤操作。

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中的设置下，选择常规。
3. 在托管式策略面板中，您可以进一步了解 Detective 支持的所有托管式策略。您可以根据希望用户在 Detective 中执行的操作，向账户授予必要的权限。要以管理员身份进行操作，我们建议将 AmazonDetectiveFullAccess 策略附加到主体。
4. 根据您在IAM控制台中是否拥有权限，请按以下步骤操作：
 - 如果您有权在IAM控制台中进行操作，请将推荐的策略附加到您用于 Detective 的主体。

- 如果您无权在IAM控制台中进行操作，请复制策略的 Amazon 资源名称 (ARN) 并将其提供给您IAM管理员。然后，他们就可以代表您附加策略。

可用的选项取决于是否拥有 Detective in Organizations 的委托管理员账户。

- 如果您没有 Detective in Organizations 的委托管理员账户，请输入该账户的账户标识符，将其指定为 Detective 管理员账户。

您可能已经拥有管理员账户，并通过手动邀请程序获得了行为图。如果是这样，则我们建议将该账户指定为 Detective 管理员账户。

如果您在 Organizations for Amazon 中拥有委托管理员账户 GuardDuty，AWS Security Hub，或 Amazon Macie，然后 Detective 会提示你选择其中一个账户。也可以输入不同的账户。

- 如果您拥有 Detective in Organizations 的委托管理员账户，则系统会提示选择该账户或您的账户。我们建议在所有区域选择委托管理员账户。

5. 选择委托。

Detective API, AWS CLI

要指定 Detective 管理员帐户，您可以使用API呼叫或 AWS Command Line Interface。您必须使用组织管理账户证书。

如果已经拥有 Detective in Organizations 委托管理员账户，则必须选择该账户或您的账户，我们建议选择委托管理员账户。

要指定 Detective 管理员帐户 (DetectiveAPI，AWS CLI)

- D@@@ etectiveAPI：使用该[EnableOrganizationAdminAccount](#)操作。你必须提供 AWS Detective 管理员帐户的帐户标识符。要获取账户标识符，请执行 [ListOrganizationAdminAccounts](#) 操作。
- AWS CLI: 在命令行中，运行该[enable-organization-admin-account](#)命令。

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

示例

```
aws detective enable-organization-admin-account --account-id 777788889999
```

删除 Detective 管理员账号

组织管理账户可以删除区域中当前的 Detective 管理员账户。删除 Detective 管理员账户时，Detective 只会将其从当前区域中删除。它不会更改 Organizations 中的委托管理员账户。

当组织管理账户删除某个区域中的 Detective 管理员账户时，Detective 会删除组织行为图。已删除的 Detective 管理员账户已禁用 Detective。

要移除 Detective 当前委派的管理员帐户，请使用 Organizations API。删除 Detective in Organizations 委托管理员账户后，Detective 会删除所有委托管理员账户为 Detective 管理员账户的组织行为图。使用组织管理账户作为 Detective 管理员账户的组织行为图不会受到影响。

Console

可以从 Detective 控制台删除 Detective 管理员账户。

删除 Detective 管理员账户后，将对该账户禁用 Detective，并删除组织行为图。仅在当前区域中删除 Detective 管理员账户。

Important

删除 Detective 管理员账户不会影响 Organizations 中的委托管理员账户。

要删除 Detective 管理员账户（启用 Detective 页面）

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 选择开始。
3. 在授权管理员下，选择禁用 Amazon Detective。
4. 在确认对话框中，输入 **disable**，然后选择禁用 Amazon Detective。

要删除 Detective 管理员账户（常规页面）

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。

2. 在 Detective 导航窗格中的设置下，选择常规。
3. 在授权管理员下，选择禁用 Amazon Detective。
4. 在确认对话框中，输入 **disable**，然后选择禁用 Amazon Detective。

Detective API, AWS CLI

要删除 Detective 管理员帐户，您可以使用API调用或 AWS CLI。您必须使用组织管理账户证书。

删除 Detective 管理员账户后，将对该账户禁用 Detective，并删除组织行为图。

Important

删除 Detective 管理员账户不会影响 Organizations 中的委托管理员账户。

要移除 Detective 管理员帐户 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用该[DisableOrganizationAdminAccount](#)操作。

当你使用 Detective API 移除 Detective 管理员帐户时，只有在发出API呼叫或发出命令的地区才会将其删除。

- AWS CLI: 在命令行中，运行该[disable-organization-admin-account](#)命令。

```
aws detective disable-organization-admin-account
```

移除委派管理员账号

删除 Detective 管理员账户不会自动删除 Organizations 中的授权管理员账户。要移除 Detective 的委托管理员帐户，你可以使用 Organizations API。

删除授权管理员账户时，这会删除授权管理员账户为 Detective 管理员账户的所有组织行为图。它还会禁用这些区域中账户的 Detective 功能。

要移除委派管理员账号 (Organization API s , AWS CLI)

- 组织API：使用该[DeregisterDelegatedAdministrator](#)操作。必须提供 Detective 管理员账户的账户标识符和 Detective 的服务主体，即 `detective.amazonaws.com`。

- AWS CLI: 在命令行中，运行该[deregister-delegated-administrator](#)命令。

```
aws organizations deregister-delegated-administrator --account-id <Detective administrator account ID> --service-principal <Detective service principal>
```

示例

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --service-principal detective.amazonaws.com
```

账户的可用操作

管理员和成员账户可以访问以下 Detective 操作。表中的数值具有以下含义：

- 任何——该账户可对同一 Detective 管理员账户下的所有账户执行操作。
- 自身——该账户只能对自身的账户执行操作。
- 破折号 (-)——该账户不能执行操作。

在组织行为图中，Detective 管理员账户决定将哪些组织账户启用为成员账户。他们可以配置 Detective 将新组织账户自动启用为成员账户，也可以手动启用组织账户。

管理员账户可以邀请账户成为行为图中的成员账户。当成员账户接受邀请并启用后，Amazon Detective 就会开始采集成员账户的数据并将其提取到行为图中。

对于组织行为图以外的行为图，所有成员账户都是受邀账户。

下表列出了管理员和成员账户的默认权限。您可以使用自定义IAM策略进一步限制对 Detective 特性和功能的访问。

操作	管理员账户（组织）	管理员账户（邀请）	成员（组织）	成员（邀请）
查看账户	任何	任何	自身（查看管理员账户）	自身（查看管理员账户）
删除成员账户	任何 已删除受邀账户	任何	—	自身

操作	管理员账户（组织）	管理员账户（邀请）	成员（组织）	成员（邀请）
	已解除组织账户关联			
添加或删除可选的数据来源包	任何（设置适用于所有成员账户）	任何（设置适用于所有成员账户）	—	—
禁用 Detective	自身	自身	—	—
查看行为图数据	任何	任何	—	—
启用或禁用可选的数据来源包	全部	全部	—	—

查看账户列表

管理员帐户可以使用 Detective 控制台或API查看帐户列表。该列表可能包括：

- 管理员账户邀请加入行为图的账户。这些账户的类型为按邀请。
- 对于组织行为图，即组织中的所有账户。这些账户的类型为按组织。

结果不包括拒绝邀请或管理员账户已从行为图中删除的受邀成员账户。它仅包括具有以下状态的账户。

正在验证

对于受邀账户，Detective 会在发送邀请之前验证账户的电子邮件地址。

对于组织账户，Detective 正在验证该账户是否属于该组织。Detective 还会验证是否是 Detective 管理员账户启用了该账户。

验证失败

验证失败。邀请未发送，或者组织账户未启用为成员。

已邀请

适用于受邀账户。邀请已发送，但成员账户尚未回复。

不是数字

组织行为图中的组织账户。该组织账户目前不是成员账户。它不会向组织行为图提供数据。

已启用

对于受邀账户，成员账户接受邀请并向行为图提供数据。

对于组织行为图中的组织账户，Detective 管理员账户会将该账户启用为成员账户。该账户向组织行为图提供数据。

未启用

对于受邀账户，成员账户接受了邀请，但无法启用。

对于组织行为图中的组织账户，Detective 管理员账户试图启用该账户，但无法启用。

对于受邀账户，Detective 会检查成员账户的数量。行为图的最大成员账户数为 1200 个。如果行为图已经包含 1,200 个成员帐户，则无法启用新帐户。

Detective 会检查你的数据量是否在侦探配额之内。流入行为图的数据量必须小于 Detective 允许的最大值。如果当前摄取的容量超过行为图数据量每天 10 TB 的限制，则 Detective 将不允许您添加其他成员帐户。

列出账户（控制台）

您可以使用 AWS Management Console 来查看和筛选您的账户列表。

要显示账户列表（控制台）

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在 Detective 导航窗格中，选择账户管理。

成员账户列表包含以下账户：

- 您的账户
- 您邀请向行为图提供数据的账户
- 在组织行为图中，所有的组织账户

对于每个账户，列表会显示以下信息：

- AWS 账户标识符。
- 对于组织账户，即账户名称。
- 账户类型（按邀请或按组织）。
- 对于受邀账户，即账户根用户电子邮件地址。
- 账户状态。
- 账户的每日数据量。Detective 无法检索未启用为成员账户的账户的数据量。
- 上次更新账户状态的日期。

可以使用表格顶部的选项卡，根据成员账户状态筛选列表。每个选项卡都显示匹配的成员账户数量。

- 选择全部，查看所有成员账户。
- 选择已启用可查看状态为已启用的账户。
- 选择未启用可查看状态不是已启用的账户。

还可以在成员账户列表中添加其他筛选条件。

要向行为图中的账户列表添加筛选器（控制台）

1. 选择筛选器框。
2. 选择用于筛选列表的列。
3. 对于指定的列，选择要用于筛选的值。
4. 要删除筛选器，请选择右上角的 x 图标。
5. 要使用最新状态信息更新列表，请选择右上角的刷新图标。

列出你的会员账号（DetectiveAPI，AWS CLI）

您可以使用API呼叫或 AWS Command Line Interface 在行为图中查看成员帐户列表。

要在ARN请求中使用您的行为图，请使用[ListGraphs](#)操作。

要检索成员账户列表（DetectiveAPI，AWS CLI）

- D@@ etectiveAPI：使用该[ListMembers](#)操作。要识别预期的行为图，请指定行为图ARN。

请注意，对于组织行为图，[ListMembers](#) 不会返回未启用为成员账户的组织账户或从行为图中解除关联的组织账户。

- AWS CLI：在命令行处，运行 [list-members](#) 命令。

```
aws detective list-members --graph-arn <behavior graph ARN>
```

例如：

```
aws detective list-members --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

在行为图中检索有关特定成员账户的详细信息 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用该[GetMembers](#)操作。为成员账户指定行为图ARN和账户标识符列表。
- AWS CLI：在命令行处，运行 [get-members](#) 命令。

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior graph ARN>
```

例如：

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

以 Detective 成员账户的身份管理组织账户

在组织行为图中，Detective 管理员账户决定将哪些组织账户启用为成员账户。默认情况下，新组织账户不会作为成员账户启用。他们的身份是非成员。Detective 管理员账户可以配置 Detective 在组织行为图中自动启用新组织账户作为成员账户。

Detective 管理员可以将 Detective 配置为自动启用新的组织帐户作为成员帐户。如果选择自动启用组织账户，则当新账户添加到组织时，Detective 就会开始将其作为成员账户启用。Detective 不会启用尚未启用的现有组织账户。

如果您不想自动启用新的组织帐户，Detective 可以手动启用组织帐户作为成员帐户。他们还可以手动启用已取消关联的组织帐户。如果组织行为图已经启用了最多 1,200 个帐户，则 Detective 管理员无法将组织帐户启用为成员帐户。在这种情况下，组织账户的状态仍为非成员。

Detective 管理员还可以取消组织帐户与组织行为图的关联。要停止从组织行为图中的组织账户摄取数据，可以解除与该账户的关联。该账户的现有数据将保留在行为图中。

内容

- [启用新的组织账户作为 Detective 成员账户](#)
- [启用组织账户作为 Detective 成员账户](#)
- [取消组织账户与 Detective 成员账户的关联](#)

启用新的组织账户作为 Detective 成员账户

Detective 管理员账户可以配置 Detective 在组织行为图中自动启用新组织账户作为成员账户。

新账户添加到组织后，它们会被添加到账户管理页面的列表中。对于组织账户，类型为按组织。

默认情况下，新组织账户不会作为成员账户启用。他们的身份是非成员。

如果选择自动启用组织账户，则当新账户添加到组织时，Detective 就会开始将其作为成员账户启用。Detective 不会启用尚未启用的现有组织账户。

只有当行为图的最大成员帐户数为 1,200 时，Detective 才能启用组织帐户作为成员帐户。如果行为图中已包含 1200 个成员账户，则无法启用新账户。

Console

在账户管理页面上，自动启用新组织账户设置决定是否在账户被添加到组织时自动启用这些账户。

要将新组织账户自动启用为成员账户

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 将自动启用新组织账户切换到开启位置。

DetectiveAPI/AWS CLI

要确定是否自动启用新的组织帐户作为 Detective 成员帐户，管理员帐户可以使用 Detective API 或 AWS Command Line Interface。

要查看和管理配置，必须提供行为图ARN。要获取ARN，请使用[ListGraphs](#)操作。

要查看自动启用组织账户的当前配置

- **Detective API**：使用该[DescribeOrganizationConfiguration](#)操作。

在回复中，如果自动启用了新组织账户，则 `AutoEnable` 为 `true`。

- **AWS CLI**：在命令行处，运行 [describe-organization-configuration](#) 命令。

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

示例

```
aws detective describe-organization-configuration --graph-arn  
arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

要自动启用新组织账户

- **Detective API**：使用该[UpdateOrganizationConfiguration](#)操作。要自动启用新组织账户，请将 `AutoEnable` 设置为 `true`。
- **AWS CLI**：在命令行处，运行 [update-organization-configuration](#) 命令。

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN>  
--auto-enable | --no-auto-enable
```

示例

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-  
east-1:111122223333:graph:123412341234 --auto-enable
```

启用组织账户作为 Detective 成员账户

如果您没有自动启用新组织账户，则可以手动启用这些账户。您还必须手动启用已解除关联的账户。

确定是否可以启用账户

如果组织行为图中已启用账户的上限为 1200 个，则无法将组织账户启用为成员账户。在这种情况下，组织账户的状态仍为非成员。该账户不向行为图提供数据。

一旦成员账户可以启用，Detective 就会自动将成员账户状态更改为已启用。例如，如果管理员帐户删除其他成员帐户以便为帐户腾出空间，则成员帐户的状态将更改为“已启用”。

Console

在账户管理页面，可以将组织账户作为成员账户启用。

要启用组织账户作为成员账户

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 要查看当前未启用的账户列表，请选择未启用。
4. 您可以选择特定的组织账户，也可以启用所有组织账户。

要启用选定的组织账户：

- a. 选择要启用的每个组织账户。
- b. 选择启用账户。

要启用所有组织账户，请选择启用所有组织账户。

Detective API/AWS CLI

您可以使用 Detective API 或 AWS Command Line Interface，在组织行为图中启用组织帐户作为成员帐户。要在ARN请求中使用您的行为图，请使用[ListGraphs](#)操作。

要启用组织账户作为成员账户

- Detective API：使用该[CreateMembers](#)操作。您必须提供图表ARN。

为每个账户指定账户标识符。组织行为图中的组织账户不会收到邀请。您无需提供电子邮件地址或其他邀请信息。

- AWS CLI：在命令行处，运行 [create-members](#) 命令。

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-arn <behavior graph ARN>
```

示例

```
aws detective create-members --accounts AccountId=444455556666
AccountId=123456789012 --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

取消组织账户与 Detective 成员账户的关联

要停止从组织行为图中的组织账户摄取数据，可以解除与该账户的关联。该账户的现有数据将保留在行为图中。

解除组织账户的关联后，状态将更改为非成员。Detective 会停止从该账户摄取数据，但该账户仍保留在列表中。

Console

在账户管理页面，您可以解除组织账户作为成员账户的关联。

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 要显示已启用的账户列表，请选择已启用。
4. 选择要解除关联的每个账户的复选框。
5. 选择操作。然后选择禁用账户。

已解除关联账户的账户状态更改为非成员。

Detective API/AWS CLI

要在ARN请求中使用您的行为图，请使用[ListGraphs](#)操作。

取消组织账户与组织行为图的关联

- Detective API：使用该[DeleteMembers](#)操作。为要取消关联的成员账户指定图表ARN和账户标识符列表。
- AWS CLI：在命令行处，运行 [delete-members](#) 命令。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
graph ARN>
```

示例

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

在 Detective 中管理受邀成员账户

Detective 管理员账号可以在行为图中邀请账号成为成员账号。一张行为图最多可以包含 1200 个成员账户。当成员账户接受邀请并启用后，Amazon Detective 就会开始采集成员账户的数据并将其提取到行为图中。

要邀请个人账户，你可以手动指定要邀请的成员账号将其数据贡献到行为图中。如果要添加成员账户列表，可以选择提供一个.csv 文件，其中包含要邀请加入行为图的成员账户列表。

对于组织行为图以外的行为图，所有成员账户都是受邀账户。Detective 管理员账户也可以邀请非组织账户的账户加入组织行为图。

简而言之，邀请账户加入行为图的流程如下。

1. 对于要添加的每个成员帐户，管理员帐户都提供 AWS 帐户标识符和根用户电子邮件地址。
2. Detective 验证此电子邮件地址是否为帐户的根用户电子邮件地址。如果帐户信息有效，Detective 就会向成员账户发送邀请。

Detective 不会执行此验证，也不会向以下地区的成员账户发送电子邮件邀请：

- AWS GovCloud（美国东部）区域
- AWS GovCloud（美国西部）区域

对于其他区域，你可以DisableEmailNotification使用 Detective 的[CreateMembers](#)操作 API。如果设置DisableEmailNotification为 true，则 Detective 将不会向成员账户发送邀请。对于集中管理的账户，这是一个非常有用的设置。

3. 成员账户接受或拒绝邀请。

即使管理员账户不发送邀请电子邮件，成员账户也必须回复邀请。

4. 成员账户接受邀请后，Detective 开始将成员账户中的数据提取到行为图中。
5. 一旦成员账户符合启用条件，Detective 就会自动将成员账户状态更改为已启用。

例如，如果管理员帐户删除其他成员帐户以便为帐户腾出空间，则成员帐户的状态将更改为“已启用”。

如果多个账户处于未启用状态，则 Detective 会按照邀请顺序启用这些账户。检查是否启用任何未启用账户的程序每小时运行一次。

管理员账户还可以手动启用账户，而不必等待自动流程。例如，管理员账户可能想要选择要启用的账户。有关如何启用成员账户的信息，请参阅[the section called “启用未启用的成员账户”](#)。

请注意，Detective 于 2021 年 5 月 12 日开始自动启用未启用的账户。在此之前未启用的账户不会自动启用。管理员账户必须手动启用它们。

管理员账户可以从行为图中删除受邀成员账户。Detective 不会从行为图中删除任何现有数据，因为行为图汇总了各成员账户的数据。

内容

- [邀请个人账号加入行为图表](#)
- [邀请成员账号列表加入行为图表](#)
- [启用未启用的成员账户](#)
- [从行为图中移除成员账户](#)

邀请个人账号加入行为图表

可以手动指定要邀请为行为图提供数据的成员账户。

Console

使用 Detective 控制台手动选择要邀请的成员账户。

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 选择操作。然后选择邀请账户。
4. 在添加账户下，选择添加个人账户。
5. 要将成员账户添加到邀请列表，请执行以下步骤。
 - a. 选择添加账户。

- b. 在AWS 账户 ID 中，输入 AWS 账户 ID。
- c. 对于电子邮件地址，输入根用户账户的电子邮件地址。
6. 要从列表中删除某个账户，请为该账户选择删除。
7. 在个性化邀请电子邮件下，添加要包含在邀请电子邮件中的自定义内容。

例如，可以使用该区域提供联系信息。或者使用它来提醒成员账号，他们需要将所需的IAM策略附加到其用户或角色，然后才能接受邀请。

8. 成员账户IAM政策包含成员账户所需IAM政策的文本。电子邮件邀请中包含此策略文本。要复制策略文本，请选择复制。
9. 选择邀请。

Detective API/AWS CLI

你可以使用 Detective API 或 the AWS Command Line Interface 邀请成员账户将其数据贡献到行为图中。要获取要在ARN请求中使用的行为图，请使用[ListGraphs](#)操作。

邀请成员账号访问行为图表 (DetectiveAPI , AWS CLI)

- **DetectiveAPI** : 使用该[CreateMembers](#)操作。您必须提供图表ARN。为每个账户指定账户标识符和根用户电子邮件地址。

如果不想向成员账户发送邀请电子邮件，请将 `DisableEmailNotification` 设置为 `true`。默认 `DisableEmailNotification` 为 `false`。

如果要发送邀请电子邮件，则可以选择提供自定义文本添加到邀请电子邮件中。

- **AWS CLI** : 在命令行处，运行 `create-members` 命令。

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --message "<Custom message text>"
```

示例

```
aws detective create-members --accounts
AccountId=444455556666,EmailAddress=mmajor@example.com
AccountId=123456789012,EmailAddress=jstyles@example.com --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This
is Paul Santos. I need to add your account to the data we use for security"
```

```
investigation in Amazon Detective. If you have any questions, contact me at  
psantos@example.com."
```

要表示不向成员账户发送邀请电子邮件，请包含--disable-email-notification。

```
aws detective create-members --accounts AccountId=<AWS account  
ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --  
disable-email-notification
```

示例

```
aws detective create-members --accounts  
AccountId=444455556666,EmailAddress=mmajor@example.com  
AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn  
arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-  
notification
```

邀请成员账号列表加入行为图表

可以从 Detective 控制台提供一份 .csv 文件，其中包含要邀请加入行为图的成员账户列表。

文件的第一行是标题行。然后将每个账户单独列一行。每个成员账户条目都包含 AWS 账户 ID 和账户的 root 用户电子邮件地址。

例如：

```
Account ID,Email address  
111122223333,srodriguez@example.com  
444455556666,rroe@example.com
```

Detective 在处理文件时，会忽略已邀请的账户，除非账户状态为验证失败。该状态表明，为该账户提供的电子邮件地址与该账户根用户电子邮件地址不匹配。在这种情况下，Detective 会删除原始邀请，然后再次尝试验证电子邮件地址并发送邀请。

该选项还提供了可用于创建账户列表的模板。

从 .csv 列表（控制台）邀请成员账户

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。

2. 在 Detective 导航窗格中，选择账户管理。
3. 选择操作。然后选择邀请账户。
4. 在添加账户下，选择从 .csv 添加。
5. 要下载要使用的模板文件，请选择下载 .csv 模板。
6. 要选择包含账户列表的文件，请选择选择 .csv 文件。
7. 在查看成员账户下，验证 Detective 在文件中检测到的成员账户列表。
8. 在个性化邀请电子邮件下，添加要包含在邀请电子邮件中的自定义内容。

例如，您可以提供联系信息，或提醒会员账号遵守所需的IAM政策。

9. 成员账户IAM政策包含成员账户所需IAM政策的文本。电子邮件邀请中包含此策略文本。要复制策略文本，请选择复制。
10. 选择邀请。

添加跨区域的成员账户列表

Detective 在中 GitHub 提供了一个开源 Python 脚本，允许你执行以下操作：

- 在指定的区域列表中，将指定的成员账户列表添加到管理员账户的行为图中。
- 如果管理员账户在某个区域中没有行为图，则该脚本也会启用 Detective 并在该区域中创建行为图。
- 向成员账号发送邀请电子邮件。
- 自动接受成员账户的邀请。

有关如何配置和使用 GitHub 脚本的信息，请参阅[the section called “亚马逊 Detective Python 脚本”](#)。

启用未启用的成员账户

会员账户接受邀请后，Amazon Detective 会检查成员账户的数量。行为图的最大成员账户数为 1200 个。如果行为图中已包含 1200 个成员账户，则无法启用新账户。如果 Detective 无法启用成员账户，则会将成员账户状态设置为未启用。

未启用的成员账户不会为行为图提供数据。

Detective 会根据行为图自动启用账户。

也可以尝试手动启用未启用成员账户的成员账户。例如，可以删除现有的成员账户，以减少数据量。与其等待自动程序启用账户，不如尝试启用未启用的成员账户。

Console

成员账户列表包含一个选项，可启用未启用的选定成员账户。

要启用未启用的成员账户

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 在我的成员账户下，选中要启用的每个成员账户对应的复选框。

只能启用状态为未启用的成员账户。

4. 选择启用账户。

Detective 决定是否可以启用成员账户。如果可以启用成员账户，则状态将更改为已启用。

Detective API/CLI

您可以使用API呼叫或启用未启用的单个成员帐户。AWS Command Line Interface 要获取要在 ARN请求中使用的行为图，请使用[ListGraphs](#)操作。

要启用未启用的成员账户

- Detective API：使用该[StartMonitoringMember](#) API操作。您必须提供行为图ARN。要识别成员账户，请使用 AWS 账户标识符。
- AWS CLI: 运行[start-monitoring-member](#)命令。

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account ID>
```

例如：

```
start-monitoring-member --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --account-id 444455556666
```

从行为图中移除成员账户

管理员账户可以随时从行为图中移除受邀成员账户。

Detective 会自动删除终止于 AWS GovCloud (美国东部) 和 AWS GovCloud (美国西部) 地区的成员账户。

从行为图中删除受邀成员账户时，会发生以下情况。

- 该成员账户已从我的成员账户中删除。
- Amazon Detective 会停止从已删除的账户提取数据。

Detective 不会从行为图中删除任何现有数据，因为行为图汇总了各成员账户的数据。

Console

您可以使用 AWS Management Console 将受邀成员账户从行为图中移除。

要删除成员账户 (控制台)

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 在账户列表中，选择要删除的每个成员账户的复选框。

无法从列表中删除自己的账户。

4. 选择操作。然后选择禁用账户。

Detective API/CLI

你可以使用 Detective API 或 AWS Command Line Interface 将受邀成员账户从行为图中移除。要获取要在ARN请求中使用的行为图，请使用[ListGraphs](#)操作。

要从行为图中移除受邀成员账号 (DetectiveAPI, AWS CLI)

- DetectiveAPI：使用该[DeleteMembers](#)操作。为要移除的成员账户指定图表ARN和账户标识符列表。
- AWS CLI：在命令行处，运行 [delete-members](#) 命令。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

例如：

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Python script

Detective 在中提供了一个开源脚本 GitHub。可以使用此脚本从管理员账户的行为图表中删除指定区域列表中的指定成员账户列表。

有关如何配置和使用 GitHub 脚本的信息，请参阅[the section called “亚马逊 Detective Python 脚本”](#)。

对于成员账号：管理行为图邀请和成员资格

Amazon Detective 会向每个成员账户摄取其提供的每个行为图所摄取的数据费用。

账户管理页面允许成员账户查看其所属的行为图的管理员账户。

受邀访问行为图的成员账号可以查看和回复他们的邀请。他们还可以从行为图中删除自己的账户。

对于组织行为图，组织账户无法控制其账户是否为成员账户。Detective 管理员账户可选择启用或禁用组织账户作为成员账户。

内容

- [会员账户必需的IAM政策](#)
- [查看行为图邀请列表](#)
- [回复行为图邀请](#)
- [从行为图中删除账户](#)

会员账户必需的IAM政策

在成员账户可以查看和管理邀请之前，必须将所需的IAM政策附加到其委托人身上。主体可以是现有用户或角色，也可以创建新的用户或角色供 Detective 使用。

理想情况下，管理员帐户会让其IAM管理员附加所需的策略。

会员账户IAM政策允许访问成员在 Amazon Detective 中进行账户操作。为行为图做出贡献的电子邮件邀请包括该IAM政策的文本。

要使用此策略，请 *<behavior graph ARN>* 替换为图表ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
      ],
      "Resource": "*"
    }
  ]
}
```

请注意，组织行为图中的组织账户不会收到邀请，也无法取消其账户与组织行为图的关联。如果它们不属于其他行为图，则只需获得 ListInvitations 权限。ListInvitations 允许他们查看行为图的管理员账户。管理邀请和取消关联成员资格的权限仅适用于通过邀请获得的成员资格。

查看行为图邀请列表

在 Amazon Detective 控制台API中 AWS Command Line Interface , Detective 或的会员账户可以看到他们的行为图表邀请。

查看行为图邀请（控制台）

您可以从中查看行为图邀请 AWS Management Console。

要查看行为图邀请 (控制台)

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在 Detective 导航窗格中，选择账户管理。

在账户管理页面上，我的管理员账户包含在当前区域中已打开和已接受的行为图邀请。对于组织账户，我的管理员账户还包含组织行为图。

如果账户目前处于免费试用期，该页面还会显示免费试用期的剩余天数。

该列表中不包含拒绝的邀请、退出的成员资格或管理员账户删除的成员资格。

每个邀请都会显示管理员账号、接受邀请的日期以及邀请的当前状态。

- 对于尚未回复的邀请，状态为已邀请。
- 对于已接受的邀请，状态为已启用或未启用。

如果状态为已启用，则账户会向行为图提供数据。

如果状态为未启用，则账户不会向行为图提供数据。

您的账户状态最初设置为“未启用”，而 Detective 会检查您是否已 GuardDuty 启用，如果启用，则检查您的账户是否会导致行为图的数据量超过 Detective 配额。

如果账户不会导致行为图超出配额，Detective 会将账户状态更新为已启用。否则，状态将保持为未启用。

当行为图能够容纳账户的数据量时，Detective 会自动将其更新为已启用。例如，管理员账户可能会删除其他成员账户，以便启用账户。管理员账户也可以手动启用账户。

查看行为图邀请 (DetectiveAPI , AWS CLI)

您可以列出来自 Detective API 或 AWS Command Line Interface。

检索行为图的开放和已接受邀请列表 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用该[ListInvitations](#)操作。
- AWS CLI：在命令行处，运行 [list-invitations](#) 命令。

```
aws detective list-invitations
```

回复行为图邀请

在你接受邀请后，Detective 会检查成员账户的数量。行为图的最大成员账户数为 1200 个。如果行为图中已包含 1200 个成员账户，则无法启用新账户。

接受邀请后，您的帐户中将启用 Detective。Detective 会检查你的数据量是否在 Detective 配额之内。流入行为图的数据量必须小于 Detective 允许的最大值。如果当前摄取的容量高于每天 10 TB 的限制，则无法添加更多帐户，Detective 将禁止进一步摄取数据。Detective 控制台会显示一条通知，指出数据量太大且状态仍为“未启用”。

如果拒绝邀请，则该邀请就会从邀请列表中删除，Detective 也不会行为图中使用账户数据。

回复行为图邀请（控制台）

您可以使用回复电子邮件邀请，其中包含指向 Detective 控制台的链接。AWS Management Console 只能回复状态为已邀请的邀请。

要回复行为图邀请（控制台）

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 在我的管理员账户下，要接受邀请并开始向行为图提供数据，请选择接受邀请。

要拒绝邀请并将其从列表中删除，请选择拒绝。

回应行为图的邀请（DetectiveAPI，AWS CLI）

您可以回复 Detective API 或... 的行为图邀请 AWS Command Line Interface。

要接受行为图的邀请（DetectiveAPI，AWS CLI）

- DetectiveAPI：使用该 [AcceptInvitation](#) 操作。必须指定图表ARN。
- AWS CLI：在命令行处，运行 [accept-invitation](#) 命令。

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

例如：

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

要拒绝行为图邀请 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用该[RejectInvitation](#)操作。必须指定图表ARN。
- AWS CLI：在命令行处，运行 [reject-invitation](#) 命令。

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

例如：

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

从行为图中删除账户

接受邀请后，可以随时从行为图中删除账户。从行为图中删除账户时，Amazon Detective 会停止从账户向行为图中摄取数据。现有数据仍保留在行为图中。

只有受邀账户才能从行为图中删除自己的账户。组织账户不能从组织行为图中删除自己的账户。

从行为图中删除账户 (控制台)

您可以使用 AWS Management Console 将您的账户从行为图表中移除。

要从行为图中删除账户 (控制台)

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中，选择账户管理。
3. 在我的管理员账户下，针对要退出的行为图，选择退出。

从行为图中删除你的账户 (DetectiveAPI , AWS CLI)

你可以使用 Detective API 或 AWS Command Line Interface 将你的账户从行为图中移除。

要将你的账号从行为图中移除 (DetectiveAPI , AWS CLI)

- D@ detecteAPI : 使用该[DisassociateMembership](#)操作。必须指定图表ARN。
- AWS CLI : 在命令行处，运行 [disassociate-membership](#) 命令。

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

例如：

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

账户操作对行为图的影响

这些操作会对 Amazon Detective 的数据和访问产生以下影响。

Detective 已禁用

当管理员账户禁用 Detective 时，会出现以下情况：

- 删除行为图。
- Detective 停止从管理员账户和该行为图的成员账户中摄取数据。

成员账户已从行为图中删除

从行为图中删除成员账户后，Detective 会停止从该账户摄取数据。

行为图中的现有数据不受影响。

对于受邀账户，该账户将从我的成员账户列表中删除。

对于组织行为图中的组织账户，账户状态更改为非成员。

成员账户退出组织

当成员账户退出组织时，会发生以下情况：

- 该账户已从组织行为图的我的成员账户列表中删除。

- Detective 会停止从该账户摄取数据。

行为图中的现有数据不受影响。

AWS 账户已暂停

管理员帐户在中被暂停后 AWS，该帐户将失去在 Detective 中查看行为图的权限。Detective 停止向行为图输入数据。

当会员帐户在中被暂停时 AWS，Detective 会停止提取该帐户的数据。

90 天后，该账户将被停用或重新激活。管理员账户被重新激活后，其 Detective 权限将恢复。Detective 会恢复从该账户摄取数据。成员账户被重新激活后，Detective 会恢复从该账户中摄取数据。

AWS 账户已关闭

AWS 账户关闭后，Detective 会对关闭做出如下回应。

- 对于管理员账户，Detective 会删除行为图。
- 对于成员账户，Detective 会将该账户从行为图中删除。

AWS 自管理员账户关闭生效之日起，将账户的政策数据保留 90 天。在 90 天期限结束时，AWS 永久删除该账户的所有保单数据。

- 要将调查发现保留 90 天以上，可以将策略存档。您还可以使用带有 EventBridge 规则的自定义操作将发现结果存储在 S3 存储桶中。
- 只要 AWS 保留策略数据，当您重新打开已关闭的账户时，就会将该账户重新 AWS 分配为服务管理员并恢复该账户的服务策略数据。
- 有关更多信息，请参阅[关闭账户](#)。

Important

对于 AWS GovCloud (US) 各地区的客户：

- 在关闭账户前，备份并删除账户资源。关闭账户后，将不再拥有其访问权限。

使用 Detective Python 脚本管理账户

Amazon Detective 在 GitHub 存储库中提供了一组开源 Python 脚本[amazon-detective-multiaccount-scripts](https://github.com/aws-samples/amazon-detective-multiaccount-scripts)。这些脚本需要 Python 3。

您可以使用它们执行以下任务：

- 启用跨区域的管理员账户 Detective。

启用 Detective 后，您就可以向行为图分配标签值。

- 在跨区域中，将成员账户添加到管理员账户的行为图中。
- 可选择向成员账号发送邀请电子邮件。您还可以将请求配置为不发送邀请电子邮件。
- 在跨区域中，从管理员账户的行为图中删除成员账户。
- 禁用跨区域的管理员账户 Detective。当管理员账户禁用 Detective 时，每个区域中管理员账户的行为图都会被禁用。

enableDetective.py 脚本概述

enableDetective.py 脚本执行以下操作：

1. 在每个指定区域为管理员账户启用 Detective，前提是管理员账户尚未在该区域启用 Detective。

使用脚本启用 Detective 后，您就可以向行为图分配标签值。

2. 可选择从管理员账户向每个行为图的指定成员账户发送邀请。

邀请电子邮件消息使用默认消息内容，无法自定义。

您还可以将请求配置为不发送邀请电子邮件。

3. 自动接受成员账户的邀请。

由于脚本会自动接受邀请，因此成员账户可以忽略这些消息。

我们建议直接联系成员账户，通知他们自动接受邀请。

disableDetective.py 脚本概述

disableDetective.py 脚本会删除指定区域内管理员账户行为图中的指定成员账户。

此外，还提供了在指定区域内禁用管理员账户 Detective 的选项。

脚本所需的权限

这些脚本需要管理员帐户以及您添加或删除的所有成员帐户中预先存在的 AWS 角色。

Note

所有账户中的角色名称必须相同。

IAM政策[建议的最佳做法](#)是使用作用域最小的角色。要执行脚本中[创建图表](#)、[创建成员](#)和[向图中添加成员](#)的工作流程，所需的权限是：

- 侦探：CreateGraph
- 侦探：CreateMembers
- 侦探：DeleteGraph
- 侦探：DeleteMembers
- 侦探：ListGraphs
- 侦探：ListMembers
- 侦探：AcceptInvitation

角色信任关系

角色信任关系必须允许实例或本地凭证代入该角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果您没有包含所需权限的通用角色，则必须在每个成员账户中创建一个至少具有这些权限的角色。您还必须在管理员账户中创建角色。

创建角色时，请确保执行以下操作：

- 在每个账户中使用相同的角色名称。
- 在上面添加所需的权限（推荐）或选择[AmazonDetectiveFullAccess](#)托管策略。
- 如上所述，添加角色信任关系模块。

要自动执行此过程，您可以使用EnableDetective.yaml AWS CloudFormation 模板。由于该模板只创建全局资源，因此可以在任何区域运行。

为 Python 脚本设置运行环境

您可以从EC2实例或本地计算机运行脚本。

启动和配置实例EC2例

运行脚本的一种选择是从EC2实例运行脚本。

启动和配置EC2实例

1. 使用您的管理员账户启动EC2实例。有关如何启动EC2实例的详细信息，请参阅亚马逊EC2用户指南中的 [Amazon EC2 Linux 实例入门](#)。
2. 为实例附加一个有权允许实例在管理员账户AssumeRole中调IAM用的角色。

如果您使用该EnableDetective.yaml AWS CloudFormation 模板，则会创建配置文件名EnableDetective为的实例角色。

否则，有关创建实例角色的信息，请参阅博客文章 [“使用EC2控制台轻松替换IAM角色或将角色附加到现有EC2实例”](#)。

3. 安装所需的软件：

- APT: `sudo apt-get -y install python3-pip python3 git`
- RPM: `sudo yum -y install python3-pip python3 git`
- Boto (最低版本 1.15) : `sudo pip install boto3`

4. 将存储库克隆到EC2实例。

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

配置本地计算机来运行脚本

您也可以在本地计算机上运行脚本。

要配置本地计算机来运行脚本

1. 确保已在本地计算机上设置了管理员账户凭证，该凭证具有调用 AssumeRole 的权限。
2. 安装所需的软件：
 - Python 3
 - Boto (最低版本 1.15)
 - GitHub 脚本

平台	安装说明
Windows	1. 安装 Python 3 (tho https://www.py.org/download s/windows/). 2. 打开命令提示符。 3. 要安装 Boto，请运行：pip install boto3 4. 从 GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) 下载脚本源代码。
Mac	1. 安装 Python 3 (tho https://www.py.org/download s/mac-osx/). 2. 打开命令提示符。 3. 要安装 Boto，请运行：pip install boto3 4. 从 GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts) 下载脚本源代码。
Linux	1. 要安装 Python 3，请运行以下命令之一： • sudo apt-get -y install python3-pip python3 git

平台	安装说明
	• <code>sudo yum install git python</code> 2. 要安装 Boto , 请运行 : <code>sudo pip install boto3</code> 3. 从中克隆脚本源代码https://github.com/aws-samples/amazon-detective-multiaccount-scripts。

创建要添加或删除的 .csv 成员账户列表

为确定要添加到行为图或从行为图中删除的成员账户，您需要提供一个包含账户列表的 .csv 文件。

将每个账户单独列一行。每个成员账户条目都包含 AWS 账户 ID 和账户的 root 用户电子邮件地址。

请参见以下示例：

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

运行 enableDetective.py

您可以从 EC2 实例或本地计算机运行 enableDetective.py 脚本。

运行 enableDetective.py

1. 将 .csv 文件复制到您的 EC2 实例或本地计算机上的 amazon-detective-multiaccount-scripts 目录中。
2. 切换到 amazon-detective-multiaccount-scripts 目录。
3. 运行 enableDetective.py 脚本。

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
--input_file inputFileName --tags tagValueList --enabled_regions regionList --
disable_email
```

运行脚本时，请替换以下值：

administratorAccountID

管理员 AWS 账户的账户 ID。

roleName

要在管理员账户和每个成员账户中 AWS 扮演的角色的名称。

inputFileName

包含要添加到管理员账户行为图的成员账户列表的 .csv 文件的名称。

tagValueList

(可选) 以逗号分隔的标签值列表，用于为新行为图分配标签值。

每个标签值的格式为 *key=value*。例如：

```
--tags Department=Finance,Geo=Americas
```

regionList

(可选) 以逗号分隔的区域列表，用于将成员账户添加到管理员账户的行为图中。例如：

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

管理员账户可能尚未在某个区域中启用 Detective。在这种情况下，该脚本会启用 Detective 并为管理员账户创建新的行为图。

如果您未提供区域列表，则该脚本将在 Detective 支持的所有区域内运行。

--disable_email

(可选) 如果包含，Detective 不会向成员账户发送邀请电子邮件。

运行 **disableDetective.py**

您可以从 EC2 实例或本地计算机运行 `disableDetective.py` 脚本。

运行 **disableDetective.py**

1. 将 .csv 文件复制到 `amazon-detective-multiaccount-scripts` 目录。
2. 要使用 .csv 文件删除指定区域列表中管理员账户行为图中列出的成员账户，请按以下步骤运行 `disableDetective.py` 脚本：

```
disabledetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList
```

3. 要在所有区域禁用管理员账户的 Detective，请运行带有 `--delete-master` 标志的 `disableDetective.py` 脚本。

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
--input_file inputFileName --disabled_regions regionList --delete_master
```

运行脚本时，请替换以下值：

administratorAccountID

管理员 AWS 账户的账户 ID。

roleName

要在管理员账户和每个成员账户中 AWS 扮演的角色的名称。

inputFileName

包含要从管理员账户行为图中删除的成员账户列表的 .csv 文件的名称。

即使禁用了 Detective，您也必须提供 .csv 文件。

regionList

(可选) 以逗号分隔的区域列表，用于执行以下操作之一：

- 从管理员账户的行为图中删除成员账户。
- 如果包含 `--delete-master` 标志，请禁用 Detective。

例如：

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

如果您未提供区域列表，则该脚本将在 Detective 支持的所有区域内运行。

Amazon Detective 与亚马逊安全湖集成

Amazon Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动将来自 AWS 环境、SaaS 提供商、本地资源、云源和第三方来源的安全数据集中到存储在您账户中的专用数据湖中。AWS Security Lake 可以帮助您分析安全数据，让您更全面地了解整个组织的安全状况。借助 Security Lake，您还可以改善对工作负载、应用程序和数据的保护。

Amazon Detective 与 Amazon Security Lake 集成，这意味着您可以查询和检索 Security Lake 存储的原始日志数据。

使用此集成，您可以从 Security Lake 原生支持的以下来源收集日志和事件。Detective 最多支持源版本 2 (OCSF 1.1.0)。

- AWS CloudTrail 管理事件版本 1.0 及更高版本
- 亚马逊 Virtual Private Cloud (亚马逊 VPC) 流日志 1.0 及更高版本
- 亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 审核日志版本 2.0。— 要使用 Amazon EKS 审计日志作为来源，您必须添加 `ram:ListResources` 到 IAM 权限中。有关更多详细信息，请参阅[向您的账户添加所需的 IAM 权限](#)。

有关 Security Lake 如何自动将来自原生支持的 AWS 服务的日志和事件转换为 OCSF 架构的详细信息，请参阅 [Amazon Security Lake 用户指南](#)。

将 Detective 与 Security Lake 集成后，Detective 开始从安全湖中提取与 AWS CloudTrail 管理事件和 Amazon VPC 流日志相关的原始日志。有关更多详细信息，请参阅[查询原始日志](#)。

启用 Detective 与安全湖的集成

要将 Detective 与 Security Lake 集成，你必须完成以下步骤。

1. [开始之前](#)

使用 Organizations 管理账户来为您的组织指定一个委托的 Security Lake 管理员。确保安全湖已启用，并确认安全湖正在从 AWS CloudTrail 管理事件和亚马逊虚拟私有云 (Amazon VPC) 流日志中收集日志和事件。

为了与安全参考架构保持一致，Detective 建议使用日志存档帐户，并推迟使用安全工具帐户进行 Security Lake 部署。

2. [创建安全湖订阅者](#)

要使用来自 Amazon Security Lake 的日志和事件，您必须为 Security Lake 订阅用户。按照以下步骤向 Detective 账户管理员授予查询权限。

3. 为您的 IAM 身份添加所需的 AWS Identity and Access Management (IAM) 权限。

- 添加以下权限以创建 Detective 与 Security Lake 集成：
 - 将这些 AWS 身份和访问管理 (IAM) 权限附加到您的 IAM 身份。有关详细信息，请参阅[向您的账户添加所需的 IAM 权限](#)部分。
 - 将此 IAM 策略添加到您计划用于传递 AWS CloudFormation 服务角色的 IAM 委托人中。有关更多详细信息，请参阅向您的 [IAM 委托人添加权限](#)部分。
 - 如果您已经将 Detective 与 Security Lake 集成，则要使用集成，请将这些 (IAM) 权限附加到您的 IAM 身份。有关详细信息，请参阅[向您的账户添加所需的 IAM 权限](#)部分。

4. [接受资源共享 ARN 邀请并启用集成](#)

使用 AWS CloudFormation 模板设置创建和管理 Security Lake 订阅者的查询访问权限所需的参数。有关创建堆栈的详细步骤，请参阅[使用 AWS CloudFormation 模板创建堆栈](#)。创建完堆栈后，启用集成。

要演示如何使用 Detective 控制台将 Amazon Detective 与 Amazon Security Lake 集成，请观看以下视频：[Amazon Detective 与亚马逊安全湖集成——如何设置](#)-->

在开始将 Detective 与 Security Lake

本主题介绍初步步骤，例如为您的组织委派 Security Lake 管理员、为您的 Detective 管理员帐户启用 Security Lake 以及验证 Security Lake 是否正在收集日志和事件。

Security Lake 与 AWS Organizations 集成，可管理组织中多个账户的日志收集。要为组织使用 Security Lake，您的 AWS Organizations 管理账户必须先为您的组织指定一名委派的 Security Lake 管理员。然后，委托的 Security Lake 管理员必须启用 Security Lake，并为组织中的成员账户启用日志和事件收集。

在将 Security Lake 与 Detective 集成之前，请确保已为 Detective 管理员帐户启用 Security Lake。您必须先配置数据湖设置，然后使用 Security Lake 控制台启用 Security Lake 来设置日志收集。有关如何启用 Security Lake 的详细步骤，请参阅《Amazon Security Lake 用户指南》中的[入门](#)。

此外，请验证 Security Lake 是否正在从 AWS CloudTrail 管理事件和亚马逊虚拟私有云 (Amazon VPC) 流日志中收集日志和事件。有关安全湖中日志收集的更多详细信息，请参阅 Amazon Security Lake 用户指南中的[从 AWS 服务收集数据](#)。

第 1 步：在 Detective 中创建安全湖订阅者

本主题介绍如何使用 Detective 控制台创建 Security Lake 订阅者。

要使用来自 Amazon Security Lake 的日志和事件，您必须为 Security Lake 订阅用户。订阅用户可以查询和访问 Security Lake 收集的数据。具有查询权限的订阅者可以使用诸如亚马逊 Athena 之类的服务直接在亚马逊简单存储服务 (Amazon S3) 存储桶中查询 AWS Lake Formation 表。要成为订阅用户，Security Lake 管理员必须为您提供允许您查询数据湖的订阅用户访问权限。有关管理员如何执行此操作的信息，请参阅《Amazon Security Lake 用户指南》中的[创建具有查询权限的订阅用户](#)。

按照以下步骤创建 Security Lake 订阅者，以便向 Detective 管理员帐户授予查询权限。

在 Security Lake 中创建 Detective 订阅用户

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择集成。
3. 在 Security Lake 订阅用户窗格中，记下账户 ID 和外部 ID 值。

让 Security Lake 管理员 IDs 使用它们来：

- 在 Security Lake 中为您创建 Detective 订阅用户。
- 将订阅用户配置为具有查询权限。
- 要确保创建具有 Lake Formation 权限的 Security Lake 查询订阅用户，请在 Security Lake 控制台中选择 Lake Formation 作为数据访问方式。

当 Security Lake 管理员为您创建订阅用户时，Security Lake 会为您生成一个 Amazon 资源共享 ARN。要求管理员将此 ARN 发送给您。

4. 在 Security Lake 订阅用户窗格中输入 Security Lake 管理员提供的资源共享 ARN。
5. 收到 Security Lake 管理员的资源共享 ARN 后，在 Security Lake 订阅用户窗格的资源共享 ARN 框中输入 ARN。

第 2 步：在 Detective 中向你的账户添加所需的 IAM 权限

本主题说明了您必须添加到您的 IAM 身份的 AWS Identity and Access Management (IAM) 权限策略的详细信息。

要启用 Detective 与 Security Lake 的集成，您必须将以下 AWS Identity and Access Management (IAM) 权限策略附加到您的 IAM 身份。

将下面的内联策略附加到角色。如果您想使用自己的 Amazon S3 存储桶来存储 Athena 查询结果，请将 `athena-results-bucket` 替换为您的 Amazon S3 存储桶名称。如果您希望 Detective 自动生成 Amazon S3 存储桶来存储 Athena 查询结果，请从 IAM 策略中删除全部 `S3ObjectPermissions`。

如果您没有将此策略附加到您的 IAM 身份所需的权限，请联系您的 AWS 管理员。如果您拥有所需权限但出现问题，请参阅 IAM 用户指南中的[排除访问被拒绝错误消息](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "athena:BatchGetQueryExecution",
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:GetQueryRuntimeStatistics",
      "athena:GetWorkGroup",
      "athena:ListQueryExecutions",
      "athena:StartQueryExecution",
      "athena:StopQueryExecution",
      "lakeformation:GetDataAccess",
      "ram:ListResources"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:GetParametersByPath"
    ],
    "Resource": [
      "arn:aws:ssm:*<ACCOUNT ID>:parameter/Detective/SLI"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation:GetTemplateSummary",
      "iam:ListRoles"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [

```

```
        "securitylake.amazonaws.com"  
      ]  
    }  
  }  
}  
]  
}
```

步骤 3：接受资源共享 ARN 邀请

本主题介绍使用 AWS CloudFormation 模板接受资源共享 ARN 邀请的步骤，这是启用 Detective 与 Security Lake 集成之前的必需步骤。

要从 Security Lake 访问原始数据日志，您必须接受 Security Lake 管理员创建的 Security Lake 账户发出的资源共享邀请。您还需要设置跨账户表共享的 AWS Lake Formation 权限。此外，您还必须创建可接收原始查询日志的 Amazon Simple Storage Service (Amazon S3) 存储桶。

在下一步中，您将使用 AWS CloudFormation 模板为以下内容创建堆栈：接受资源共享 ARN 邀请、创建所需 AWS Glue 爬网程序 资源和授予 AWS Lake Formation 管理员权限。

接受资源共享 ARN 邀请并启用集成

1. 使用 CloudFormation 模板创建新 CloudFormation 堆栈。有关更多详细信息，请参阅 [使用 AWS CloudFormation 模板创建堆栈](#)。
2. 创建完堆栈后，选择“启用集成”以启用 Detective 与 Security Lake 的集成。

使用 AWS CloudFormation 模板创建堆栈

Detective 提供了一个 AWS CloudFormation 模板，您可以使用该模板来设置创建和管理 Security Lake 订阅者的查询访问权限所需的参数。

步骤 1：创建 AWS CloudFormation 服务角色

必须创建 AWS CloudFormation 服务角色才能使用 AWS CloudFormation 模板创建堆栈。如果您没有创建服务角色所需的权限，请联系 Detective 管理员账户的管理员。有关 AWS CloudFormation 服务角色的更多信息，请参阅 [AWS CloudFormation 服务角色](#)。

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

2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 对于选择可信实体，选择 AWS 服务。
4. 选择 AWS CloudFormation。然后选择下一步。
5. 输入角色的名称。例如 CFN-DetectiveSecurityLakeIntegration。
6. 将下面的内联策略附加到角色。<Account ID>替换为您的 AWS 账户 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudFormationPermission",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateChangeSet"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:aws:transform/*"
      ]
    },
    {
      "Sid": "IamPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:PassRole",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::<ACCOUNT ID>:role/*",
        "arn:aws:iam::<ACCOUNT ID>:policy/*"
      ]
    }
  ],
}
```

```

{
  "Sid": "S3Permissions",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:DeleteBucket*",
    "s3:PutBucket*",
    "s3:GetBucket*",
    "s3:GetObject",
    "s3:PutEncryptionConfiguration",
    "s3:GetEncryptionConfiguration"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ]
},
{
  "Sid": "LambdaPermissions",
  "Effect": "Allow",
  "Action": [
    "lambda:CreateFunction",
    "lambda:DeleteFunction",
    "lambda:GetFunction",
    "lambda:TagResource",
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
  ]
},
{
  "Sid": "CloudwatchPermissions",
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup",
    "logs:DeleteLogGroup",
    "logs:DescribeLogGroups"
  ],
  "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
},
{
  "Sid": "KmsPermission",
  "Effect": "Allow",
  "Action": [

```

```

        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
    }
  ]
}

```

第 2 步：为您的 IAM 委托人添加权限。

您需要以下权限才能使用您在上一步中创建的 CloudFormation 服务角色创建堆栈。将以下 IAM 策略添加到您计划用于传递 CloudFormation 服务角色的 IAM 委托人。您将假设这个 IAM 主体来创建堆栈。如果您没有添加 IAM 策略所需的权限，请联系 Detective 管理员账户的管理员。

Note

在以下策略中，本策略中使用的 CFN-DetectiveSecurityLakeIntegration 是指您在前面的 Creating an AWS CloudFormation 服务角色步骤中创建的角色。如果不一致，请将其更改为您在之前步骤中输入的角色名称。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration"
    },
    {
      "Sid": "RestrictCloudFormationAccess",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
    "Condition": {
        "StringEquals": {
            "cloudformation:RoleArn": [
                "arn:aws:iam:*:<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
            ]
        }
    }
},
{
    "Sid": "CloudformationDescribeStack",
    "Effect": "Allow",
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetStackPolicy"
    ],
    "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
},
{
    "Sid": "CloudformationListStacks",
    "Effect": "Allow",
    "Action": [
        "cloudformation:ListStacks"
    ],
    "Resource": "*"
},
{
    "Sid": "CloudWatchPermissions",
    "Effect": "Allow",
    "Action": [
        "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
}
]
}

```

步骤 3：在 AWS CloudFormation 控制台中指定自定义值

1. 从 Detective 进入 AWS CloudFormation 控制台。

2. (可选) 输入堆栈名称。堆栈名称是自动填充的。您可以将堆栈名称更改为与现有堆栈名称不冲突的名称。
3. 输入以下参数。

- AthenaResultsBucket— 如果您不输入值，则此模板会生成一个 Amazon S3 存储桶。如果您想使用自己的存储桶，请输入要存储 Athena 查询结果的存储桶名称。如果您使用自己的存储桶，请确保存储桶与资源共享 ARN 位于同一区域。如果您使用自己的存储桶，请确保您选择的 LakeFormationPrincipals 具有向存储桶写入对象和从存储桶读取对象的权限。有关存储桶权限的更多详细信息，请参阅《Amazon Athena 用户指南》中的[查询结果和最近查询](#)。
- DTRegion— 此字段已预先填写。请不要更改此字段中的值。
- LakeFormationPrincipals— 输入您想要授予使用安全湖集成的权限的 IAM 委托人 (例如，IAM 角色 ARN) 的 ARN，以逗号分隔。这些可能是你的安全分析师和使用 Detective 的安全工程师。

您只能使用之前在步骤 [Step 2: Add the required IAM permissions to your account] 中附加了 IAM 权限的 IAM 主体。

- ResourceShareARN-此字段已预先填写。请不要更改此字段中的值。

4. 权限

IAM 角色：选择您在 Creating an AWS CloudFormation Service Role 步骤中创建的角色。或者，可以将其留空 (如果您的当前 IAM 角色具有 Creating an AWS CloudFormation Service Role 步骤中的所有必需权限)。

5. 查看并选中所有我确认复选框，然后单击创建堆栈按钮。有关更多详细信息，请查看将要创建的以下 IAM 资源。

```
* ResourceShareAcceptorCustomResourceFunction
  - ResourceShareAcceptorLambdaRole
  - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
  - SsmParametersLambdaRole
  - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
  - GlueDatabaseLambdaRole
  - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
  - GlueTablesLambdaRole
  - GlueTablesLogsAccessPolicy
```

第 4 步：将 Amazon S3 存储桶策略添加到 IAM 委托人 **LakeFormationPrincipals**

(可选) 如果您让此模板为您生成 AthenaResultsBucket，则必须将以下策略附加到 LakeFormationPrincipals 中的 IAM 主体。

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

athena-results-bucket 替换为 AthenaResultsBucket 名称。AthenaResultsBucket 可以在 AWS CloudFormation 控制台上找到：

1. 在 <https://console.aws.amazon.com/cloudformation> 上打开 AWS CloudFormation 控制台。
2. 单击您的堆栈。
3. 单击资源选项卡。
4. 搜索逻辑 ID AthenaResultsBucket 并复制其物理 ID。

更改 Detective 集成配置

如果要更改用于将 Detective 与 Security Lake 集成的任何参数，可以对其进行编辑，然后再次启用集成。您可以编辑 AWS CloudFormation 模板以在以下情况下重新启用此集成：

- 要更新 Security Lake 订阅，您可以创建新的订阅用户，也可以让 Security Lake 管理员更新现有订阅的数据来源。
- 指定用于存储原始查询日志的其他 Amazon S3 存储桶。
- 指定其他 Lake Formation 主体。

重新启用 Detective 与 Security Lake 的集成时，您可以编辑资源共享 ARN，并查看 IAM 权限。要编辑 IAM 权限，您可以从 Detective 转到 IAM 控制台。您也可以编辑先前在 AWS CloudFormation 模板中输入的值。您必须删除现有 CloudFormation 堆栈并重新创建它才能重新启用集成。

重新启用 Detective 与 Security Lake 的集成

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择集成。
3. 您可以使用以下任一步骤编辑集成：
 - 在 Security Lake 窗格中，选择编辑。
 - 在 Security Lake 窗格中，选择视图。在视图页面中，选择编辑。
4. 输入新的资源共享 ARN，以访问区域中的数据来源。
5. 查看当前 IAM 权限，并转到 IAM 控制台（如果您想编辑 IAM 权限）。
6. 编辑 CloudFormation 模板中的值。
 1. 在创建新堆栈之前，请先删除现有堆栈。如果您不删除现有堆栈并尝试在同一区域创建新堆栈，则您的请求将失败。有关更多详细信息，请参阅[删除堆 CloudFormation 栈](#)。
 1. 创建新 CloudFormation 堆栈。有关更多详细信息，请参阅[使用 AWS CloudFormation 模板创建堆栈](#)。
7. 选择启用集成。

支持将 Detective 与安全湖集成的 AWS 区域

您可以在以下 AWS 区域将 Detective 与 Security Lake 集成。

区域名称	区域	终端节点	协议
美国东部（俄亥俄州）	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS

区域名称	区域	终端节点	协议
美国西部 (加利福尼亚北部)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
美国西部 (俄勒冈州)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
亚太地区 (孟买)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
亚太地区 (首尔)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
亚太地区 (新加坡)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
亚太地区 (悉尼)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
亚太地区 (东京)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
加拿大 (中部)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
欧洲地区 (法兰克福)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
欧洲地区 (爱尔兰)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
欧洲地区 (伦敦)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
欧洲地区 (巴黎)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
欧洲地区 (斯德哥尔摩)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS

区域名称	区域	终端节点	协议
南美洲（圣保罗）	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

在 Detective 中查询原始日志

将 Detective 与 Security Lake 集成后，Detective 开始从安全湖提取与 AWS CloudTrail 管理事件和亚马逊虚拟私有云（亚马逊 VPC）流日志相关的原始日志。

Note

在 Detective 中查询原始日志不会产生额外费用。包括亚马逊 Athena 在内的其他 AWS 服务的使用费仍按公布费率收取。

AWS CloudTrail 管理事件适用于以下配置文件：

- AWS 账户
- AWS 用户
- AWS 角色
- AWS 角色会话
- 亚马逊 EC2 实例
- Amazon S3 存储桶
- IP 地址
- Kubernetes 集群
- Kubernetes 吊舱
- Kubernetes 主题
- IAM 角色
- IAM 角色会话
- IAM 用户

Amazon VPC FLOW 日志适用于以下配置文件：

- 亚马逊 EC2 实例
- Kubernetes 容器组 (pod)

要演示如何使用 Detective 控制台将 Amazon Detective 与 Amazon Security Lake 集成，请观看以下视频：[Amazon Detective 与亚马逊 Security Lake 集成——如何使用-->](#)

查询 AWS 账户的原始日志

1. 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择搜索，然后搜索 AWS account。
3. 在 API 调用总量部分中，选择显示范围时间的详细信息。
4. 在此处，您可以开始查询原始日志。

The screenshot shows the Amazon Detective console interface. At the top, the breadcrumb navigation is 'Detective > Search > AwsAccount/714603721603'. Below this, the account ID '714603721603' is displayed with an 'AWS account' label and an 'Info' link. To the right, the 'Scope time' is set to '12/21/2023 18:00 UTC > 12/22/2023 18:00 UTC'. The main content area shows 'Activity for time window: 12/21/2023 18:00 UTC - 12/22/2023 18:00 UTC'. Below this, there are three tabs: 'Observed IP addresses' (selected), 'API method by service', and 'Resource'. A search bar is present with the placeholder text 'Search'. On the right side of the activity window, a button labeled 'Query raw logs' is highlighted with a red rectangular box. Below the tabs, a table displays the search results. The table has five columns: 'IP address', 'Successful calls', 'Failed calls', 'Location', and 'Actions'. There are three rows of data, each with a play button icon in the 'IP address' column.

IP address ▼	Successful calls ▼	Failed calls ▼	Location ▼	Actions
▶ [redacted]	6	2	[redacted]	
▶ [redacted]	2	1	-	
▶ [redacted]	1	0		

在原始日志预览表中，您可以查看通过查询 Security Lake 数据检索到的日志和事件。有关原始事件日志的更多详细信息，您可以查看 Amazon Athena 中显示的数据。

Raw log preview: CloudTrail

View raw event logs that were retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Athena.

Raw log preview (500+)

< 1 2 3 4 5 6 7 ... 50 >

date_time	requestor_arn	account_id	region	source_ip	service	api_
2023-12-22 09:58:38.000 UTC			us-east-1		s3.amazonaws.com	GetE
2023-12-22 09:59:49.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		ec2.amazonaws.com	Desc
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		iam.amazonaws.com	GetI
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	GetC
2023-12-22 10:00:13.000 UTC			us-east-1		autoscaling.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc

Close

Cancel query request

See results in Athena

Download results

在查询原始日志表中，您可以取消查询请求，在 Amazon Athena 中查看结果，并下载结果 [下载为逗号分隔值 (.csv) 文件]。

如果您在 Detective 中看到日志，但查询未返回任何结果，则可能是由于以下原因而引起的。

- 原始日志可能会先在 Detective 中可用，然后才显示在 Security Lake 日志表中。请稍后重试。
- Security Lake 中可能缺少日志。如果您等待了很长时间，则表示 Security Lake 中缺少日志。要解决该问题，请联系您的 Security Lake 管理员。

示例

- [查询 AWS 角色的原始日志](#)
- [查询 Amazon EKS 集群的原始日志](#)
- [查询 Amazon EC2 实例的原始日志](#)

查询 AWS 角色的原始日志

如果您想了解新地理位置中 AWS 角色的活动，可以在 Detective 控制台中进行操作。

查询 AWS 角色的原始日志

- 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。

- 在 Detective Summary 页面的“新观察到的地理位置”部分，记下该 AWS 角色。
- 在导航窗格中，选择搜索，然后搜索 AWS role。
- 对于该 AWS 角色，展开资源以显示该资源从该 IP 地址发出的特定 API 调用。
- 选择要调查的 API 调用旁边的放大镜图标，以打开原始日志预览表。

Activity for time window:

Q Query raw logs

Observed IP addresses

API method by service

Resource

Q Search

< 1 >

IP address ▼	Successful calls ▼	Failed calls ▼	Location ▼	Actions
▶ 10.0.0.0/24	289	284	-	
▶ 10.0.0.0/24	63	0	10.0.0.0/24	
▶ 10.0.0.0/24	42	0	10.0.0.0/24	
▶ 10.0.0.0/24	21	0	10.0.0.0/24	

查询 Amazon EKS 集群的原始日志

- 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
- 从 Detective 摘要页面创建的 pod 最多的容器集群部分，导航到 Amazon EKS 集群。
- 在 Amazon EKS 集群详情页面中，选择 Kubernetes API 活动选项卡。
- 在涉及此 Amazon EKS 集群的整体 Kubernetes API 活动部分中，选择范围时间的显示详情。
- 在此处，您可以开始查询原始日志。

查询 Amazon EC2 实例的原始日志

- 打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
- 在导航窗格中，选择搜索，然后搜索 Amazon EC2 instance。
- 在 VPC 的总流量部分，选择要调查的 API 调用旁边的放大镜图标，以打开原始日志预览表。
- 在此处，您可以开始查询原始日志。

Activity for time window: 11/21/2023 11:00 (UTC-08:00) - 11/22/2023 11:00 (UTC-08:00) ↗

Toggle overall traffic

Query raw logs

☐	IP address ▾	Local port ▾	Remote port ▾	Inbound traffic ▾	Outbound traffic ▾	Protocol ▾	Directionality ▾	Accept / Reject ▾	Actions
☐		22	-	44.7 kB	57.7 kB	TCP	Inbound	Accept	
☐		22	-	240 B	480 B	TCP	Inbound	Accept	
☐		22	-	61.1 kB	75 kB	TCP	Inbound	Accept	
☐		22	-	59.6 kB	70.8 kB	TCP	Inbound	Accept	
☐		22	-	240 B	540 B	TCP	Inbound	Accept	

在原始日志预览表中，您可以查看通过查询 Security Lake 数据检索到的日志和事件。有关原始事件日志的更多详细信息，您可以查看 Amazon Athena 中显示的数据。

在查询原始日志表中，您可以取消查询请求，在 Amazon Athena 中查看结果，并下载结果 [下载为逗号分隔值 (.csv) 文件]。

禁用 Detective 与安全湖的集成

如果您禁用 Detective 与 Security Lake 的集成，则无法再从 Security Lake 中查询日志和事件数据。

禁用 Detective 与 Security Lake 的集成

1. 打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在导航窗格中，选择集成。
3. 删除现有堆栈。有关更多详细信息，请参阅 [删除堆 CloudFormation 栈](#)。
4. 在禁用 Security Lake 集成窗格中，选择禁用。

删除堆 CloudFormation 栈

如果您不删除现有堆栈，则在同一区域创建新堆栈将失败。您可以使用 CloudFormation 控制台或使用 AWS CLI 删除 CloudFormation 堆栈。

删除 AWS CloudFormation 堆栈 (控制台)

1. 在 <https://console.aws.amazon.com/cloudformat> ion 上打开 AWS CloudFormation 控制台。
2. 在 CloudFormation 控制台的堆栈页面上，选择要删除的堆栈。该堆栈当前必须处于运行状态。

3. 在堆栈详细信息窗格中，选择删除。
4. 在系统提示时，选择删除堆栈。

 Note

堆栈删除开始后，就无法停止堆栈删除操作。堆栈进入 DELETE_IN_PROGRESS 状态。

堆栈删除过程完成之后，堆栈将处于 DELETE_COMPLETE 状态。

排查堆栈删除错误

如果您在单击Delete按钮Failed to delete stack后看到该消息出现权限错误，则表示您的 IAM 角色无 CloudFormation 权删除堆栈。请联系您的账户管理员以删除堆栈。

删除 CloudFormation 堆栈 (AWS CLI)

在 AWS CLI 界面中输入以下命令：

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

CFN-DetectiveSecurityLakeIntegration 是您在 Creating an AWS CloudFormation Service Role 步骤中创建的服务角色。

预测和监控 Detective 成本

为了帮助您跟踪 Detective 活动，使用情况页面显示了数据摄取量和预计费用。

- 对于管理员账户，使用情况页面显示整个行为图中的数据量和预计费用。
- 对于成员账户，使用情况页面显示了他们提供的行为图中其账户的数据量和预计费用。

Detective 还支持 AWS CloudTrail 日志记录。

内容

- [行为图免费试用简介](#)
- [监控 Detective 管理员帐户的使用情况](#)
- [监控 Detective 成员账户的使用情况](#)
- [Amazon Detective 如何计算预计费用](#)

行为图免费试用简介

Amazon Detective 为每个区域的每个账户提供 30 天的免费试用。某个账户的免费试用从首次发生以下操作之一时开始。

- 某个账户启用 Detective 后，就会成为行为图的管理员账户。
- 某个账户被指定为 AWS Organizations 组织的 Detective 管理员账户，并且首次启用了 Detective。
- 如果 Detective 管理员账户在被指定之前已经启用了 Detective，则该账户不会开始新的 30 天免费试用。
- 账户接受邀请成为行为图中的成员账户，并作为成员账户启用。
- 该组织账户由 Detective 管理员账户作为成员账户启用。

从那时起，免费试用期为 30 天。该账户无需为该期间处理的任何数据付费。试用期结束后，Detective 开始向账户收取其为行为图提供的数据。有关如何跟踪 Detective 活动、监控使用情况和查看预计费用的更多信息，请参阅[预测和监控 Detective 成本](#)。有关定价的更多信息，请参阅[Detective 定价](#)。

该区域的所有行为图都使用相同的 30 天周期。例如，一个账户被启用为行为图的成员账户。这就开始了 30 天的免费试用。10 天后，该账户将启用同一区域的第二个行为图。对于第二个行为图，该账户将获得 20 天的免费数据。

免费试用提供多种好处：

- 管理员账户可以浏览 Detective 的特征和功能，以验证其价值。
- 管理员和成员账户可以在 Detective 开始向他们收费之前，监控数据量和预估费用。请参阅[the section called “管理员账户使用情况和费用”](#)和[the section called “成员账户使用情况跟踪”](#)。

可选数据来源的免费试用

Detective 还为可选数据来源提供 30 天的免费试用。该免费试用与首次启用 Detective 时为核心 Detective 数据来源提供的免费试用不同。

Note

如果客户在启用可选数据来源包后 7 天内将其禁用，如果再次启用，Detective 会一次性自动重置该数据来源包的免费试用。

要启用或禁用可选的数据来源，请参阅[Detective 中可选数据来源的类型](#)。

监控 Detective 管理员帐户的使用情况

Amazon Detective 会向每个账户收取该账户所属的每个行为图中使用的数据的费用。无论数据来源如何，Detective 对所有数据按每 GB 分级统一费率收费。

对于管理员账户，通过 Detective 控制台的使用情况页面，可以查看过去 30 天内按数据来源或按账户摄取的数据量。管理员账户还可以查看其账户和整个行为图在典型 30 天内的预计费用。

要查看 Detective 的使用情况信息

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为<https://console.aws.amazon.com/detective/>。
2. 在 Detective 导航窗格中的设置下，选择使用情况。
3. 选择一个选项卡，在按数据来源或按账户查看使用情况之间进行选择。

每个账户摄取的数据量

按成员账户划分的摄取量会列出行为图中的活跃账户。它不会列出已删除的成员账户。

对于每个账户，摄取的流量列表提供以下信息。

- AWS 账户标识符和 root 用户电子邮件地址。
- 账户开始为行为图表提供数据的日期。

对于管理员账户，这是该账户启用 Detective 的日期。

对于成员账户，这是账户接受邀请后启用为成员账户的日期。

- 该账户在过去 30 天内摄取的数据量。总量包括所有来源类型。
- 该账户当前是否处于免费试用期。对于当前处于免费试用期的账户，列表会显示剩余天数。

如果所有账户都不在免费试用期内，则不显示免费试用状态栏。

行为图的预计费用

该账户的预计费用显示管理员账户 30 天数据的预计费用。预计费用基于管理员账户的每日平均流量。

Important

这一数额只是预计费用。它预测了典型的 30 天时间段内管理员账户数据的总费用。它是根据前 30 天的使用情况计算出来的。请参阅 [the section called “Detective 如何计算预计费用”](#)。

行为图的预计费用

所有账户的预计费用显示了整个行为图 30 天数据的预计总费用。预计费用是根据每个账户的每日平均流量计算的。

Important

这一数额只是预计费用。它预测了典型的 30 天时间段内行为图数据的总费用。它是根据前 30 天的使用情况计算出来的。预计费用不包括从行为图中删除的成员账户。请参阅 [the section called “Detective 如何计算预计费用”](#)。

源包摄取的数据量

选择按源包查看行为图中启用的不同源包所列出的数据摄取量。

所有账户都可以查看自己账户的这些数据。管理员账户可以查看更多面板，按源包列出每个成员的使用情况。它不会列出已删除的成员账户。

Detective 核心

Detective 核心面板显示了过去 30 天内从 Detective 核心来源（日志 CloudTrail、VPC 流日志和 GuardDuty 调查结果）摄取的数据量。

EKS 审计日志

EKS 审核日志面板显示过去 30 天内从 EKS 审计日志源提取的数据量。只有为行为图启用了 EKS 审核日志后，此源包的面板才可用。

监控 Detective 成员账户的使用情况

Amazon Detective 会向每个账户收取该账户所属的每个行为图中使用的数据的费用。无论数据来源如何，Detective 对所有数据按每 GB 分级统一费率收费。

对于成员账户，使用情况页面仅显示该账户的数据量和预计的 30 天费用。

要查看 Detective 的使用情况信息

1. 登录到 AWS Management Console。然后打开 Detective 控制台，网址为 <https://console.aws.amazon.com/detective/>。
2. 在 Detective 导航窗格中的设置下，选择使用情况。

每个行为图的摄取量

该账户的摄取量列出了该成员账户提供的行为图。它不包含您退出的成员资格或管理员账户删除的成员资格。

对于每个行为图，该列表会包含以下信息：

- 管理员账户的账户编号
- 在过去 30 天内从该成员账户摄取的数据量。总量包括所有来源类型。
- 启用行为图的成员账户的日期。

各行为图的预计费用

该账户的预计费用显示了该成员账户在其提供的所有行为图中 30 天数据的预计费用。预计费用是根据成员账户的每日平均数据量计算的。

Important

这一数额只是预计费用。它预测了典型的 30 天时间段内管理员账户数据的总费用。它是根据前 30 天的使用情况计算出来的。请参阅 [the section called “Detective 如何计算预计费用”](#)。

Amazon Detective 如何计算预计费用

要计算在使用情况页面上显示的预计费用值，Detective 会执行以下操作。

1. 要在行为图中获取个人账户的预计费用，Detective 执行了以下操作。
 - a. 计算每天的平均数据量。它将所有活跃天数的数据量相加，然后除以账户的活跃天数。

如果该账户在 30 天前启用，则天数为 30。如果该账户在不到 30 天前启用，则为自接受之日起的天数。

例如，如果该账户在 12 天前启用，则 Detective 会将这 12 天摄取的数据量相加，然后将其除以 12。
 - b. 将该账户的日平均值乘以 30。这是该账户 30 天的预计使用量。
 - c. 使用其定价模型计算预计 30 天使用量的预计 30 天费用。
2. 要获得行为图的预计总费用，Detective 会执行以下操作：
 - a. 合并行为图中所有账户的预计 30 天使用量。
 - b. 使用其定价模型计算预计 30 天使用量的预计 30 天总费用。
3. 要在行为图中获取成员账户的预计总费用，Detective 会执行以下操作：
 - a. 合并所有行为图中预计的 30 天使用量。
 - b. 使用其定价模型计算的预计 30 天使用量的预计 30 天总费用。
4. 如果您使用的是共享 Amazon VPC，则 Detective 会根据监控活动计算预计成本。我们建议您查看特定于您环境的调查的预计成本。
 - a. 如果 Detective 成员账户拥有共享 Amazon VPC，且还有其他非 Detective 账户使用该共享 VPC，则 Detective 将监控来自该 VPC 的所有流量。使用量和成本将增加，Detective 将提供 VPC 内所有流量的可视化。

- b. 如果您在共享 Amazon VPC 内有一个 EC2 实例，且共享所有者不是 Detective 成员，则 Detective 将不会监控来自该 VPC 的任何流量，而且使用量和成本将降低。如果您想查看 VPC 内的流量，则必须将 Amazon VPC 所有者添加为 Detective 图的成员。

Amazon Detective 中的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。[责任共担模式](#)将其描述为云的安全性 和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。AWS 还为您提供可以安全使用的服务。

作为[AWS 合规性计划](#)的一部分，第三方审核人员将定期测试和验证安全性的有效性。

要了解适用于 Amazon Detective 的合规性计划，请参阅 [AWS 合规性计划范围内的服务](#)。

- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您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 Detective 时应用责任共担模式。以下主题说明如何配置 Detective 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Detective 资源。

内容

- [Amazon Detective 中的数据保护](#)
- [Amazon Detective 的身份和访问管理](#)
- [Amazon Detective 的合规性验证](#)
- [Amazon Detective 中的故障恢复能力](#)
- [Amazon Detective 中的基础架构安全性](#)
- [Detective 的安全最佳实践](#)

Amazon Detective 中的数据保护

这些区域有：AWS [分担责任模型](#)分适用于 Amazon Detective 中的数据保护。如本模型所述，AWS 负责保护运行所有内容的全球基础设施 AWS 云。您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，请参阅[数据隐私FAQ](#)。有关欧洲数据保护的信息，请参阅 [AWS 责任共担模型和GDPR](#)博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您进行保护 AWS 账户凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用SSL/TLS与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。有关使用 CloudTrail 轨迹捕获的信息 AWS 活动，请参阅[使用中的 CloudTrail 轨迹](#) AWS CloudTrail 用户指南。
- 使用 AWS 加密解决方案，以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅[联邦信息处理标准 \(FIPS\) 140-3](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你与 Detective 或其他人合作时 AWS 服务使用控制台，API，AWS CLI，或 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

Detective 对其处理和存储的所有静态和传输数据进行加密。

内容

- [Amazon Detective 的密钥管理](#)

Amazon Detective 的密钥管理

由于 Detective 不存储任何可识别个人身份的客户数据，因此它使用 AWS 托管式密钥。

这种类型的 KMS 密钥可以在多个账户中使用。请参阅《[AWS Key Management Service 开发者指南](#)》[中对 AWS 自有密钥的描述](#)。

这种类型的 KMS 密钥每年（大约 365 天）自动轮换。请参阅《[AWS Key Management Service 开发人员指南](#)》[中对密钥轮换的描述](#)。

Amazon Detective 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Detective 资源。IAM无需支付额外费用即可使用。AWS 服务

内容

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [Amazon Detective 是如何使用的 IAM](#)
- [Amazon Detective 基于身份的策略示例](#)
- [AWS Amazon Detective 的托管政策](#)
- [使用 Detective 的服务相关角色](#)
- [对 Amazon Detective 身份和访问进行故障排除](#)

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你在 Detective 中所做的工作。

服务用户 – 如果使用 Detective 服务来完成作业，则管理员会提供所需的凭证和权限。使用更多 Detective 特征来完成工作时，可能需要额外权限。了解如何管理访问权限有助于向管理员请求适合的权限。如果无法访问 Detective 中的特征，请参阅[对 Amazon Detective 身份和访问进行故障排除](#)。

服务管理员 – 如果您在公司负责管理 Detective 资源，则您可能具有 Detective 的完全访问权限。您有责任确定服务用户应访问哪些 Detective 特征和资源。然后，您必须向IAM管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何与 Detective IAM 配合使用，请参阅[Amazon Detective 是如何使用的 IAM](#)。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写策略来管理 Detective 的访问权限。要查看可在中使用的基于身份的 Detective 策略示例IAM，请参阅。[Amazon Detective 基于身份的策略示例](#)

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户、IAM 用户身份或通过担任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。AWS IAM Identity Center（IAM 身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用 IAM 角色设置了联合身份。当您使用联合访问 AWS 时，您就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的[如何登录到您 AWS 账户](#)的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的[API 请求 AWS 签名版本 4](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的[多因素身份验证](#)和 AWS IAM Identity Center 用户指南 IAM 中的[AWS 多因素身份验证](#)。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的[需要根用户凭据的 IAM 任务](#)。

IAM 用户和群组

[IAM 用户](#)是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的 IAM 用户。但是，如果您有需要 IAM 用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[定期轮换需要长期凭证的用例的访问密钥](#)。

[IAM 群组](#)是指定 IAM 用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins 并授予该群组管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅用户指南中的IAM用户[用例](#)。

IAM角色

[IAM角色](#)是您内部具有特定权限 AWS 账户 的身份。它与IAM用户类似，但与特定人员无关。要在中临时扮演角色 AWS Management Console，可以[从用户切换到IAM角色（控制台）](#)。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的[代入角色的方法](#)。

IAM具有临时证书的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的[为第三方身份提供商（联合）创建角色](#)。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅 AWS IAM Identity Center 用户指南中的 [权限集](#)。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
- 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。
- 服务角色-服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。
- 服务相关角色-服务相关角色是一种链接到的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

- 在 Amazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS，当与身份或资源关联时，它会定义其权限。AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档结构和内容的更多信息，请参阅 [《IAM 用户指南》中的 JSON 策略概述](#)。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对其所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以将 IAM 策略添加到角色中，用户可以代入这些角色。

IAM 无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的[使用客户托管策略定义自定义 IAM 权限](#)。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组 and 角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行[选择，请参阅《IAM 用户指南》中的在托管策略和内联策略之间进行选择](#)。

基于资源的策略

基于资源的 JSON 策略是您附加到资源的策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人 (账户成员、用户或角色) 有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的[访问控制列表 \(ACL\) 概述](#)。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体 (IAM用户或角色) 授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的[IAM实体的权限边界](#)。
- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。对成员账户中的实体 (包括每个实体) 的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 资源控制策略 (RCPs) — RCPs 这些JSON策略可用于设置账户中资源的最大可用权限，而无需更新附加到您拥有的每项资源的IAM策略。这会RCP限制成员账户中资源的权限，并可能影响身份 (包括身份) 的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息RCPs，包括 AWS 服务 该支持的列表RCPs，请参阅《AWS Organizations 用户指南》中的[资源控制策略 \(RCPs\)](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的[策略评估逻辑](#)。

Amazon Detective 是如何使用的 IAM

默认情况下，用户和角色没有创建或修改 Amazon Detective 资源的权限。他们也无法使用 AWS Management Console AWS CLI、或执行任务 AWS API。Detective 管理员必须拥有 AWS Identity and Access Management (IAM) 策略，授予IAM用户和角色对他们所需的指定资源执行特定API操作的权限。然后，管理员必须将这些策略附加到需要这些权限的主体。

Detective 使用IAM基于身份的策略为以下类型的用户和操作授予权限：

- 管理员账户 - 管理员账户是行为图的所有者，行为图使用其账户中的数据。管理员账户可以邀请成员账户为行为图提供数据。管理员帐户还可以使用行为图来分类和调查与这些帐户关联的发现和资源。

可以设置策略，允许管理员账户以外的用户执行不同类型的任务。例如，管理员账户中的用户可能只具有管理成员账户的权限。其他用户可能只拥有使用行为图进行调查的权限。

- 成员账户 — 成员账户是受邀向行为图提供数据的账户。成员账号对邀请作出回应。接受邀请后，成员账户可以从行为图中删除其账户。

要全面了解 Detective 和其他人是如何 AWS 服务 使用的IAM，请参阅 [《IAM用户指南》中JSON选项卡上的“创建策略”](#)。

Detective 基于身份的策略

使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。Detective 支持特定的操作、资源和条件键。

要了解您在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

操作

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

策略语句必须包含 Action 或 NotAction 元素。Action 元素列出了策略允许的操作。NotAction 元素列出了不允许的操作。

为 Detective 定义的操作反映了可以使用 Detective 执行的任务。Detective 中的策略操作具有以下前缀：detective:。

例如，要授予使用该CreateMembersAPI操作邀请成员账户访问行为图的权限，您需要将该detective:CreateMembers操作包含在他们的策略中。

要在单个语句中指定多项操作，请使用逗号将它们隔开。例如，对于成员账户，该策略包括一组与管理邀请相关的操作：

```
"Action": [
    "detective:ListInvitations",
    "detective:AcceptInvitation",
    "detective:RejectInvitation",
    "detective:DisassociateMembership"
]
```

可以使用通配符 (*) 指定多个操作。例如，要管理行为图中使用的数据，Detective 中的管理员账户必须能够执行以下任务：

- 查看他们的成员账户列表 (ListMembers)。
- 获取有关所选成员账户的信息 (GetMembers)。
- 邀请成员账号查看其行为图 (CreateMembers)。
- 将成员从其行为图中删除 (DeleteMembers)。

可以授予对所有以 Members 词结尾的操作的访问权限，而不必单独列出这些操作。这方面的政策可能包括以下操作：

```
"Action": "detective:*Members"
```

要查看 Detective 操作的列表，请参阅《服务授权参考》中的 [Amazon Detective 定义的操作](#)。

资源

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON 策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 [Amazon 资源名称 \(ARN\)](#) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*" 
```

有关格式的更多信息 ARNs，请参阅 [Amazon 资源名称 \(ARNs\)](#) 和 [AWS 服务命名空间](#)。

对于 Detective，唯一的资源类型是行为图。Detective 中的行为图资源具有以下内容 ARN：

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

例如，行为图具有以下值：

- 行为图的区域是 us-east-1。
- 管理员账户 ID 的账户 ID 是 111122223333。
- 行为图的图 ID 是 027c7c4610ea4aacaf0b883093cab899。

要在 Resource 语句中识别此行为图，您可以使用以下内容 ARN：

```
"Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899" 
```

要在 Resource 语句中指定多个资源，请使用逗号分隔它们。

```
"Resource": [
    "resource1",
    "resource2"
]
```

例如，在多个行为图中，可能会邀请同 AWS 一个账户成为成员账户。在该成员账户的政策中，Resource 语句将列出他们受邀访问的行为图。

```
"Resource": [  
    "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899",  
    "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"  
]
```

某些 Detective 操作（例如创建行为图、列出行为图和列出行为图邀请）不会在特定行为图上执行。要执行这些操作，Resource 语句必须使用通配符 (*)。

```
"Resource": "*"
```

对于管理员账户操作，Detective 始终会验证发出请求的用户是否属于受影响行为图的管理员账户。对于成员账户操作，Detective 始终会验证提出请求的用户是否属于成员账户。即使 IAM 策略授予访问行为图的权限，如果用户不属于正确的账户，用户也无法执行操作。

对于在特定行为图表上执行的所有操作，IAM 策略应包含该图表 ARN。该图表 ARN 可以稍后添加。例如，当一个账户首次启用 Detective 时，初始 IAM 策略使用图表 ARN 的通配符提供对所有 Detective 操作的访问权限。这样，用户就可以立即开始管理成员账户，并在其行为图中进行调查。创建行为图后，您可以更新策略以添加该图表 ARN。

条件键

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑 OR 运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在资源上标有 IAM 用户的用户名时，您才能向 IAM 用户授予访问该资源的权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM 策略元素：变量和标签](#)。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

Detective 不定义自己的一组条件键。它确实支持使用全局条件键。要查看所有 AWS 全局条件键，请参阅IAM用户指南中的[AWS 全局条件上下文密钥](#)。

要了解可以对哪些操作和资源使用条件键，请参阅 [Amazon Detective 定义的操作](#)。

示例

要查看 Detective 基于身份的策略的示例，请参阅[Amazon Detective 基于身份的策略示例](#)。

Detective 基于资源的策略（不受支持）

Detective 不支持基于资源的策略。

基于 Detective 行为图标签的授权

可以为每个行为图分配标签值。可以在条件语句中使用这些标签值来管理对行为图的访问。

标签值的条件语句使用以下格式。

```
{"StringEquals":{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

例如，当 Department 标签的值为 Finance 时，使用以下代码来允许或拒绝操作。

```
{"StringEquals":{"aws:ResourceTag/Department": "Finance"}}
```

有关使用资源标签值的策略示例，请参阅[the section called “管理员账户：根据标签值限制访问”](#)。

Detective IAM 角色

[IAM角色](#)是您的 AWS 账户中具有特定权限的实体。

使用 Detective 的临时凭证

您可以使用临时证书通过联合身份登录、代入IAM角色或担任跨账户角色。您可以通过调用[AssumeRole](#)或之类的 AWS STS API操作来获取临时安全证书[GetFederationToken](#)。

Detective 支持使用临时凭证。

服务相关角色

[服务相关角色](#)允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在您的IAM账户中，并归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Detective 服务相关角色的详细信息，请参阅[the section called “使用服务相关角色”](#)。

服务角色 (不支持)

此特征允许服务代表您代入[服务角色](#)。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在您的IAM账户中，并归该账户所有。这意味着IAM管理员可以更改此角色的权限。但是，这样做可能会中断服务的功能。

Detective 不支持服务角色。

Amazon Detective 基于身份的策略示例

默认情况下，IAM用户和角色无权创建或修改 Detective 资源。他们也无法使用 AWS Management Console AWS CLI、或执行任务 AWS API。

IAM管理员必须创建IAM策略，授予用户和角色对其所需的指定资源执行特定API操作的权限。然后，管理员将这些策略附加到需要这些权限的IAM用户或群组。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的在[JSON选项卡上创建策略](#)。

主题

- [策略最佳实践](#)
- [使用 Detective 控制台](#)
- [允许用户查看他们自己的权限](#)
- [管理员账户：在行为图中管理成员账户](#)
- [管理员账户：使用行为图进行调查](#)
- [成员账号：管理行为图邀请和成员资格](#)
- [管理员账户：根据标签值限制访问](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除账户中的 Detective 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针

对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM用户指南》中的[AWS 托管策略或工作职能托管策略](#)。

- 应用最低权限原则-使用IAM策略设置权限时，仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限IAM的更多信息，请参阅IAM用户指南IAM[中的策略和权限](#)。
- 使用IAM策略中的条件进一步限制访问权限-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅IAM用户指南中的使用 A [IAMccess Analyzer 验证策略](#)。
- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》MFA中的使用[进行安全API访问](#)。

有关最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM[中的安全最佳实践](#)。

使用 Detective 控制台

要使用 Amazon Detective 控制台，用户或角色必须有权访问与中的相应操作相匹配的相关操作API。

要启用 Detective 并成为行为图的管理员账户，必须向用户或角色授予 CreateGraph 操作权限。

要使用 Detective 控制台执行任何管理员账户操作，必须向用户或角色授予 ListGraphs 操作权限。这就授予了他们作为管理员账户检索行为图的权限。还必须向他们授予执行特定管理员账户操作的权限。

管理员账户最基本的操作是在行为图中查看成员账户列表，并使用行为图进行调查。

- 要查看行为图中的成员账户列表，必须向主体授予 ListMembers 操作的权限。
- 要在行为图中进行调查，必须向主体授予 SearchGraph 操作的权限。

要使用 Detective 控制台执行任何成员账户操作，必须向用户或角色授予 ListInvitations 操作的权限。这会授予查看行为图邀请的权限。然后就可以授予他们特定成员账户操作的权限。

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用或以编程方式完成此操作的 AWS CLI 权限。AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam: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": "*"
    }
  ]
}
```

管理员账户：在行为图中管理成员账户

此示例策略适用于仅负责管理行为图中使用的成员账户的管理员账户用户。该策略还允许用户查看使用信息并停用 Detective。该策略未授予使用行为图进行调查的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:ListMembers", "detective:CreateMembers", "detective:DeleteMembers", "detective:DeleteGraph",
        "Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899"
      ],
    },
    {
      "Effect": "Allow",
      "Action": ["detective:CreateGraph", "detective:ListGraphs"],
      "Resource": "*"
    }
  ]
}
```

管理员账户：使用行为图进行调查

此示例策略适用于仅使用行为图进行调查的管理员账户用户。他们无法在行为图中查看或编辑成员账户列表。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["detective:SearchGraph"],
      "Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899"
    },
    {
      "Effect": "Allow",
      "Action": ["detective:ListGraphs"],
      "Resource": "*"
    }
  ]
}
```

成员账号：管理行为图邀请和成员资格

此示例策略适用于属于成员账户的用户。在示例中，成员账户属于两个行为图。该策略授予回复邀请和从行为图中删除成员账户的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation", "detective:RejectInvitation", "detective:DisassociateMembership",
        "Resource": [
          "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899",
          "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"
        ]
      },
    },
    {
      "Effect": "Allow",
      "Action": ["detective:ListInvitations"],
      "Resource": "*"
    }
  ]
}
```

管理员账户：根据标签值限制访问

如果行为图的 SecurityDomain 标签与用户的 SecurityDomain 标签匹配，则以下策略允许用户使用行为图进行调查。

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": ["detective:SearchGraph"],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": ["detective:ListGraphs"],
    "Resource": "*"
  } ]
}
```

```
}
```

如果行为图的 SecurityDomain 标签值为 Finance，则以下策略禁止用户使用行为图进行调查。

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Deny",
    "Action": ["detective:SearchGraph"],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {
      "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
    }
  } ]
}
```

AWS Amazon Detective 的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的[客户管理型策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)。

AWS 托管策略：AmazonDetectiveFullAccess

您可以将 AmazonDetectiveFullAccess 策略附加到 IAM 身份。

此策略授予管理权限，允许主体完全访问所有 Amazon Detective 操作。可以在主体为其账户启用 Detective 之前，将该策略附加到主体。它还必须附加到用于运行 Detective Python 脚本以创建和管理行为图的角色。

拥有这些权限的主体可以管理成员账户，为其行为图添加标签，并使用 Detective 进行调查。他们还可以对 GuardDuty 发现结果进行存档。该策略提供了 Detective 控制台显示其中账户的账户名所需的权限 AWS Organizations。

权限详细信息

该策略包含以下权限：

- **detective**— 允许主体完全访问所有 Detective 操作。
- **organizations**— 允许主体从 AWS Organizations 获取有关组织内账户的信息。如果账户属于某个组织，则这些权限允许 Detective 控制台显示账户名称和账号。
- **guardduty**— 允许校长从 Detective 内部获取和存档 GuardDuty 调查结果。
- **securityhub**— 允许主体从 Detective 内部获取 Security Hub 的调查发现。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings"
      ],
      "Resource": "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
    },
  ],
}
```

```
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "securityHub:GetFindings"
        ],
        "Resource": "*"
      }
    ]
  }
}
```

AWS 托管策略 : AmazonDetectiveMemberAccess

可以将 AmazonDetectiveMemberAccess 策略附加到您的 IAM 实体。

该策略为成员提供对 Amazon Detective 的访问权限并限定对控制台的访问权限。

可以通过此策略：

- 查看 Detective 图成员资格邀请并接受或拒绝这些邀请。
- 在使用情况页面上查看在 Detective 中的活动如何影响使用该服务的费用。
- 在图中退出成员资格。

该策略授予只读权限，允许在一定范围内访问 Detective 控制台。

权限详细信息

该策略包含以下权限：

- `detective`— 允许成员访问 Detective。

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

```
{
  "Effect": "Allow",
  "Action": [
    "detective:AcceptInvitation",
    "detective:BatchGetMembershipDatasources",
    "detective:DisassociateMembership",
    "detective:GetFreeTrialEligibility",
    "detective:GetPricingInformation",
    "detective:GetUsageInformation",
    "detective:ListInvitations",
    "detective:RejectInvitation"
  ],
  "Resource": "*"
}
```

AWS 托管策略 : AmazonDetectiveInvestigatorAccess

可以将 AmazonDetectiveInvestigatorAccess 策略附加到您的 IAM 实体。

该策略为调查人员提供对 Detective 服务的访问权限并限定对 Detective 控制台 UI 依赖项的访问权限。此策略授予在 Detective 中为 IAM 用户和 IAM 角色启用 Detective 调查的权限。您可以通过调查确定漏洞指标，例如使用调查报告的调查发现，该报告提供有关安全指标的分析 and 见解。该报告按严重程度进行排序，严重程度是使用 Detective 的行为分析和机器学习确定的。您可以使用该报告来确定资源修复的优先级。

权限详细信息

该策略包含以下权限：

- **detective**：允许主体调查人员访问 Detective 操作，启用 Detective 调查并启用调查发现组摘要。
- **guardduty**— 允许校长从 Detective 内部获取和存档 GuardDuty 调查结果。
- **securityhub**— 允许主体从 Detective 内部获取 Security Hub 的调查发现。
- **organizations**— 允许委托人从 AWS Organizations 中检索有关组织中帐户的信息。如果帐户属于某个组织，则这些权限允许 Detective 控制台显示帐户名称和账号。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",

```

```
    "Effect": "Allow",
    "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubPermissions",
    "Effect": "Allow",
    "Action": [
        "securityHub:GetFindings"
    ],
    "Resource": "*"
}
]
```

AWS 托管策略：AmazonDetectiveOrganizationsAccess

可以将 AmazonDetectiveOrganizationsAccess 策略附加到您的 IAM 实体。

该策略授予在组织内启用和管理 Amazon Detective 的权限。可以在整个组织内启用 Detective 并确定 Detective 的授权管理员账户。

权限详细信息

该策略包含以下权限：

- **detective**— 允许主体访问 Detective 操作。
- **iam**— 指定在 Detective 调用 EnableOrganizationAdminAccount 时创建服务相关角色。
- **organizations**— 允许委托人从 AWS Organizations 中检索有关组织中帐户的信息。如果帐户属于某个组织，则这些权限允许 Detective 控制台显示帐户名称和账号。支持 AWS 服务集成，允许将指定成员帐户注册为委托管理员和注销其他“安全服务”，并允许委托人检索其他安全服务（例如 Amazon Detective、Amazon GuardDuty、Amazon Macie 和) 中的委托管理员账户。AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "detective.amazonaws.com",
                "guardduty.amazonaws.com",
                "macie.amazonaws.com",
                "securityhub.amazonaws.com"
            ]
        }
    }
}
]
}
}

```

AWS 托管策略：AmazonDetectiveServiceLinkedRole

无法将 AmazonDetectiveServiceLinkedRole 策略附加到 IAM 实体。此附加到服务相关角色的策略允许 Detective 代表您执行操作。有关更多信息，请参阅 [the section called “使用服务相关角色”](#)。

该策略授予管理权限，允许服务相关角色检索组织的账户信息。

权限详细信息

该策略包含以下权限：

- organizations— 检索组织的账户信息。

```
{
```

```
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    }
  ]
}
```

Detective 对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来 Detective AWS 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅 [文档历史记录页面](#) 上的 RSS 信息源。

更改	描述	日期
AmazonDetectiveInvestigatorAccess ：对现有策略的更新	在 AmazonDetectiveInvestigatorAccess 策略中新增了 Detective 调查和调查发现组摘要操作。 这些操作允许启动、检索和更新 Detective 调查；以及从 Detective 内部获取调查发现组的摘要。	2023 年 11 月 26 日
AmazonDetectiveFullAccess 和 AmazonDetectiveInvestigatorAccess – 现有策略更新	Detective 在 AmazonDetectiveFullAccess 和 AmazonDetectiveInvestigatorAccess 策略中添加了 Security Hub GetFindings 操作。 这些操作允许从 Detective 中获取 Security Hub 的调查发现。	2023 年 5 月 16 日

更改	描述	日期
AmazonDetectiveOrganizationsAccess : 新策略	Detective 增加了 AmazonDetectiveOrganizationsAccess 策略。 该策略授予在组织内启用和管理 Detective 的权限	2023 年 3 月 2 日
AmazonDetectiveMemberAccess : 新策略	Detective 添加了 AmazonDetectiveMemberAccess 策略。 该策略为成员提供对 Detective 的访问权限并限定对控制台 UI 依赖项的访问权限。	2023 年 1 月 17 日
AmazonDetectiveFullAccess – 对现有策略的更新	Detective 在 AmazonDetectiveFullAccess 政策中添加了 GuardDuty GetFindings 行动。 这些操作允许从 Detective 内部获取 GuardDuty 调查结果。	2023 年 1 月 17 日
AmazonDetectiveInvestigatorAccess : 新策略	Detective 添加了 AmazonDetectiveInvestigatorAccess 策略。 该策略允许主体在 Detective 中进行调查。	2023 年 1 月 17 日
AmazonDetectiveServiceLinkedRole : 新策略	Detective 为其服务相关角色添加了一项新策略。 该策略允许服务相关角色检索有关组织中账户的信息。	2021 年 12 月 16 日
Detective 开始跟踪更改情况	Detective 开始跟踪其 AWS 托管策略的变化。	2021 年 5 月 10 日

使用 Detective 的服务相关角色

Amazon Detective 使用 AWS Identity and Access Management (IAM) [服务相关角色](#)。服务关联角色是一种与 Detective 直接相关的独特 IAM 角色类型。服务相关角色由 Detective 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使 Detective 的设置变得更容易，因为不必手动添加所需权限。Detective 定义其服务相关角色的权限，除非另外定义，否则只有 Detective 可以代入该角色。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。

只有在首先删除相关资源后，您才能删除服务相关角色。这样可以保护 Detective 资源，因为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[与 IAM 配合使用的 AWS 服务](#)，并查找服务相关角色列设为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

Detective 的服务相关角色权限

Detective 使用名为 AWSServiceRoleForDetective— 允许侦探代表你访问 AWS Organizations 信息的服务相关角色。

AWSServiceRoleForDetective 服务相关角色信任以下服务来代入该角色：

- `detective.amazonaws.com`

AWSServiceRoleForDetective 服务相关角色使用托管策略[AmazonDetectiveServiceLinkedRolePolicy](#)。

有关AmazonDetectiveServiceLinkedRolePolicy政策更新的详细信息，请参阅 [Amazon Detective 对 AWS 托管策略的更新](#)。要获得有关本政策变更的自动提醒，请订阅 Detective [文档历史记录页面上的](#) RSS 提要。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的[服务相关角色权限](#)。

创建 Detective 的服务相关角色

无需手动创建服务相关角色。当您在 AWS Management Console、或 AWS API 中为组织指定 Detective 管理员账户时 AWS CLI，Detective 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。为某个组织指定 Detective 管理员账户时，Detective 会再次创建服务相关角色。

编辑 Detective 的服务相关角色

Detective 不允许你编辑 AWSServiceRoleForDetective 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。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 Detective 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，我们建议删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

Note

如果在试图删除资源时 Detective 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 Detective 使用的 Detective 资源 AWSServiceRoleForDetective

1. 删除 Detective 管理员账户。请参阅 [the section called “指定 Detective 管理员账户”](#)。
2. 在指定 Detective 管理员账户的每个区域重复该过程。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForDetective 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](#)。

Detective 服务相关角色的受支持区域

Detective 支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 [AWS 区域和端点](#)。

对 Amazon Detective 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Detective 时可能遇到的常见问题 IAM。如果您在使用 AWS Identity and Access Management (IAM) 时遇到访问被拒绝问题或类似困难，请查阅《IAM 用户指南》中的[故障排除 IAM](#) 主题。

我无权在 Detective 中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当mateojacksonIAM用户尝试使用控制台接受邀请成为行为图的成员账户但没有detective:AcceptInvitation权限时，就会出现以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 detective:AcceptInvitation 操作访问 arn:aws:detective:us-east-1:444455556666:graph:567856785678 资源。

我无权执行 iam : PassRole

如果收到错误提示，表明您无权执行 iam:PassRole 操作，则必须更新策略，允许向 Detective 传递角色。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的IAM用户marymajor尝试使用控制台在 Detective 中执行操作时，会出现以下示例错误。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 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的人访问我的 Detective 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Detective 是否支持这些特征，请参阅[Amazon Detective 是如何使用的 IAM](#)。
- 要了解如何提供对您拥有的资源的[访问权限](#)，请参阅《IAM用户指南》中的[AWS 账户 向其他IAM用户 提供访问权限](#)。AWS 账户
- 要了解如何向第三方提供对您的资源的[访问权限 AWS 账户](#)，请参阅IAM用户指南中的[向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的[向经过外部身份验证的用户提供访问权限 \(联合身份验证 \)](#)。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。

Amazon Detective 的合规性验证

Amazon Detective 属于 AWS 保障计划的范围。有关更多信息，请参阅 [Health Information Trust Alliance 通用安全框架 \(HITRUST\) CSF](#)。

有关特定合规计划范围内的 AWS 服务列表，请参阅按合规计划划分的[范围内的AWS](#)[AWS服务按合规计划](#)。有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅在 Artifact 中[下载报告在 AWS Ar](#)。

AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#) — 安全与合规性指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点的基准环境的步骤 AWS。
- [使用AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- [AWS Security Hub](#) — 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准 and 最佳实践。

Amazon Detective 中的故障恢复能力

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

除了 AWS 全球基础设施外，Detective 还利用亚马逊 DynamoDB 和亚马逊简单存储服务 (Amazon S3) 中内置的弹性。有关更多信息，请参阅 [Amazon DynamoDB 中的弹性和灾难恢复以及亚马逊简单存储服务中的弹性](#)。

Detective 架构还能够抵御单个可用区的故障。这种故障恢复能力内置在 Detective 中，不需要任何配置。

Amazon Detective 中的基础架构安全性

作为一项托管服务，Amazon Detective 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅[AWS 云安全](#)。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 [AWS security Pillar Well-Architected Framework](#) 中的[基础设施保护](#)。

您可以使用 AWS 已发布的 API 呼叫通过网络访问 Detective。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic C DHE urve Ephemeral Diffie-Hellman)。ECDHE 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的私有访问密钥对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

Detective 的安全最佳实践

Detective 提供了在您开发和实施自己的安全策略时需要考虑的大量安全特征。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

对于 Detective 来说，安全最佳实践与在行为图中管理账户关联。

Detective 管理员帐户的最佳做法

邀请成员账号加入 Detective 行为图时，请仅邀请您监督的账号。

限制访问行为图。拥有该[AmazonDetectiveFullAccess](#)策略的用户可以授予对所有 Detective 操作的访问权限。拥有这些权限的主体可以管理成员账户，为其行为图添加标签，并使用 Detective 进行调查。

当用户有权访问行为图时，他们可以查看成员账户的所有调查发现。这样的调查发现可能会暴露敏感的安全信息。

成员账户的最佳实践

当您收到行为图的邀请时，请务必验证邀请的来源。

检查发送邀请的管理员账户的账户标识符。AWS 确认您知道该账户属于谁，并且邀请账户有正当理由监控您的安全数据。

使用 Amazon Detective 记录API通话 AWS CloudTrail

Detective 与 AWS CloudTrail 一项服务集成，该服务提供用户、角色或 AWS 服务在 Detective 中采取的操作的记录。CloudTrail 将 Detective 的所有API通话记录为事件。捕获的呼叫包括来自 Detective 控制台的调用和对侦探API操作的代码调用。

- 如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Detective 的事件。
- 如果您未配置跟踪，您仍然可以在 CloudTrail控制台的“事件历史记录”中查看最新的事件。

使用收集的信息 CloudTrail，您可以确定以下内容：

- 向 Detective 发出的请求
- 发出请求的 IP 地址
- 发出请求的人员
- 发出请求的时间
- 有关该请求的其他详细信息

要了解更多信息 CloudTrail，请参阅[AWS CloudTrail 用户指南](#)。

中的 Detective 信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Detective 中发生活动时，该 CloudTrail 活动与其他 AWS 服务事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅[使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录 AWS 账户中的事件，包括 Detective 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。

预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。您还可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。

有关更多信息，请参阅下列内容：

- [创建跟踪概述](#)

- [CloudTrail 支持的服务和集成](#)
- [为以下各项配置亚马逊SNS通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)和[接收来自多个账户的 CloudTrail 日志文件](#)

CloudTrail 记录所有 Detective 操作，这些操作记录在《[侦探API参考](#)》中。

例如，对CreateMembersAcceptInvitation、和DeleteMembers操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用 root 还是 AWS Identity and Access Management (IAM) 用户凭证发出
- 请求是使用角色还是联合用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅[CloudTrail userIdentity元素](#)。

了解 Detective 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。

事件表示来自任何源的单个请求。事件包括有关请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共API调用的有序堆栈跟踪，因此条目不会按任何特定的顺序出现。

以下示例显示了演示该AcceptInvitation操作的 CloudTrail 日志条目。

```
{
  "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
  "Username": "JaneRoe",
  "EventTime": 1571956406.0,
  "CloudTrailEvent": {"eventVersion": "1.05", "userIdentity": {
    "type": "AssumedRole", "principalId": "AR0AJZARKEP6WKJ5JHSUS:JaneRoe", "arn": "arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe", "accountId": "111122223333", "accessKeyId": "AKIAIOSFODNN7EXAMPLE", "sessionContext": {
      "attributes": {"mfaAuthenticated": "false", "creationDate": "2019-10-24T21:54:56Z"}
    }, "sessionIssuer": {
      "type": "Role", "principalId": "AR0AJZARKEP6WKJ5JHSUS", "arn": "arn:aws:iam::111122223333:role/1A4R5SKSPGG9V", "accountId":
```

```
\ "111122223333\", \"userName\": \"JaneRoe\" } } }, \"eventTime\": \"2019-10-24T22:33:26Z\", \"eventSource\": \"detective.amazonaws.com\", \"eventName\": \"AcceptInvitation\", \"awsRegion\": \"us-east-2\", \"sourceIPAddress\": \"192.0.2.123\", \"userAgent\": \"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/AWS_Lambda_java8\", \"errorCode\": \"ValidationException\", \"requestParameters\": { \"masterAccount\": \"111111111111\" }, \"responseElements\": { \"message\": \"Invalid request body\" }, \"requestID\": \"8437ff99-5ec4-4b1a-8353-173be984301f\", \"eventID\": \"f2545ee3-170f-4340-8af4-a983c669ce37\", \"readOnly\": false, \"eventType\": \"AwsApiCall\", \"recipientAccountId\": \"111122223333\" }, { \"eventName\": \"AcceptInvitation\", \"eventSource\": \"detective.amazonaws.com\", \"resources\": [] },
```

Amazon Detective 区域和配额

使用 Amazon Detective 时，请注意这些配额。

Detective 区域和端点

要查看 Detective 可用 AWS 区域 位置的列表，请参阅 [Detective 服务端点](#)。

Detective 配额

Detective 有以下配额，这些配额无法配置。

资源	限额	注释
成员账户数	1,200	管理员账户可以添加到行为图中的成员账户的数量。
行为图数据量——数据量警告	每天 9 TB	如果行为图数据量每天大于 9 TB，则 Detective 会显示一条警告，提示行为图已接近允许的最大数据量。
行为图数据量——无新账户	每天 10 TB	如果行为图数据量每天大于 10 TB，则无法在行为图中添加新的成员账户。
行为图数据量——停止向行为图中摄取数据	每天 15 TB	如果行为图数据量每天大于 15 TB，则 Detective 就会停止向行为图中摄取数据。 每天 15 TB 既反映了正常的数据量，也反映了数据量的峰值。 要重新启用数据摄取，您必须联系 支持。

不支持 Internet Explorer 11 浏览器

您不能将 Detective 与 Internet Explorer 11 浏览器一起使用。

管理行为图的标签

标签是一个可选标签，您可以定义并分配给 AWS 资源，包括某些类型的 Detective 资源。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来应用策略、分配成本、区分资源版本，或识别支持特定合规性要求或工作流的资源。

您可以为行为图分配标签。然后，您可以使用 IAM 策略中的标签值来管理对 Detective 中行为图函数的访问权限。请参阅 [the section called “基于 Detective 行为图标签的授权”](#)。

您也可以将标签用作费用报告工具。例如，要跟踪与安全相关的成本，您可以为 Detective 行为图、AWS Security Hub 中心资源和 Amazon 探 GuardDuty 测器分配相同的标签。然后 AWS Cost Explorer，您可以在中搜索该标签以查看这些资源的成本的合并视图。

查看行为图的标签

您可以从常规页面管理行为图的标签。

Console

要查看分配给行为图的标签列表

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在导航窗格中的设置下，选择常规。

Detective API, AWS CLI

您可以使用 Detective API 或 the AWS Command Line Interface 来获取行为图的标签列表。

要获取行为图的标签列表 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用该 [ListTagsForResource](#) 操作。您必须提供您的 ARN 行为图表。
- AWS CLI：在命令行处，运行 `list-tags-for-resource` 命令。

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

示例

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

向行为图添加标签

Console

您可以在常规页面的标签列表中将标签值添加到行为图中。

要向行为图添加标签

1. 选择添加新标签。
2. 对于键，输入标签的名称。
3. 对于值，输入标签的值。

Detective API, AWS CLI

您可以使用 Detective API 或 AWS CLI，将标签值添加到行为图中。

向行为图添加标签 (DetectiveAPI，AWS CLI)

- DetectiveAPI：使用该[TagResource](#)操作。您可以提供行为图ARN和要添加的标签值。
- AWS CLI：在命令行处，运行 `tag-resource` 命令。

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph ARN> --tags '{"TagName":"TagValue"}
```

示例

```
aws detective tag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}
```

从行为图中移除标签

Console

要从常规页面的列表中删除标签，请为该标签选择删除选项。

Detective API, AWS CLI

您可以使用 Detective AWS CLI 或 API 从行为图中删除标签值。

要从行为图中移除标签 (DetectiveAPI , AWS CLI)

- DetectiveAPI : 使用该[UntagResource](#)操作。您可以提供行为图ARN以及要移除的标签的名称。
- AWS CLI : 在命令行处，运行 `untag-resource` 命令。

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys  
"TagName"
```

示例

```
aws detective untag-resource --resource-arn arn:aws:detective:us-  
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

禁用 Amazon Detective

行为图的管理员账户可以从 Detective 控制台、Detective API 或 AWS Command Line Interface 中禁用 Amazon Detective。禁用 Detective 时，行为图及其关联的 Detective 数据将被删除。

行为图一旦被删除，就无法恢复。

内容

- [禁用 Detective \(控制台 \)](#)
- [禁用 Detective \(侦探 API , AWS CLI \)](#)
- [禁用跨区域侦探 \(Python 脚本已开启 GitHub \)](#)

禁用 Detective (控制台)

您可以从 AWS Management Console 中禁用 Amazon Detective。

禁用 Amazon Detective (控制台)

1. 通过 <https://console.aws.amazon.com/detective/> 打开 Amazon Detective 控制台。
2. 在 Detective 导航窗格中的设置下，选择常规。
3. 在“常规”页面的“禁用 Amazon Detective”下，选择“禁用 Amazon Detective”。
4. 出现提示时，键入 **disable**。
5. 选择禁用 Amazon Detective。

禁用 Detective (侦探 API , AWS CLI)

您可以通过 Detective API 或 AWS Command Line Interface 禁用 Amazon Detective。要获取要在请求中使用的行为图的 ARN，请使用 [ListGraphs](#) 操作。

要禁用 Detective (侦探 API , AWS CLI)

- Detective API：使用 [DeleteGraph](#) 操作。您必须提供图 ARN。
- AWS CLI：在命令行处，运行 [delete-graph](#) 命令。

```
aws detective delete-graph --graph-arn <graph ARN>
```

例如：

```
aws detective delete-graph --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

禁用跨区域侦探 (Python 脚本已开启 GitHub)

Detective 在中提供了一个开源脚本 GitHub ，允许您在指定的区域列表中为管理员帐户禁用 Detective。

有关如何配置和使用 GitHub 脚本的信息，请参阅[the section called “亚马逊 Detective Python 脚本”](#)。

Detective 用户指南的文档历史记录

下表列出了自 Detective 上一次发布以来对文档所做的重要更改。如需对此文档更新的通知，可以订阅 RSS 信息源。

- 最新文档更新：2025 年 2 月 20 日

变更	说明	日期
增加了对 Amazon GuardDuty 攻击序列发现的支持	Detective 增加了对查找与 GuardDuty 扩展威胁检测相关的类型的支持。GuardDuty 当由多个操作组成的特定序列（例如 API 活动和 GuardDuty 发现检测）与潜在的可疑活动一致时，检测攻击序列。有关扩展威胁检测和攻击序列发现类型的信息，请参阅 Amazon GuardDuty 用户指南中的 扩展威胁检测 。	2025 年 2 月 20 日
增加了 GuardDuty 对 Amazon IAM 查找的支持	Detective 增加了对新 GuardDuty 查找类型的支持，当使用为环境 AWS 账户中列出的用户创建的受限用户凭据向发出请求时，该类型会提醒您 AWS 服务。有关更多信息，请参阅 Policy: IAMUser/ShortTermRotationCredentialUsage 在《亚马逊 GuardDuty 用户指南》中。	2025 年 2 月 4 日
新特征	在 Detective 调查组可视化中添加了 时间轴布局 。引入了播放按钮功能和基于严重性的搜索结果筛选。这些增强功能可以	2024 年 12 月 27 日

帮助您更好地了解事件进展，确定关键问题的优先顺序，并进行更有效的安全调查。

[增加了对 Amazon GuardDuty 调查结果的支持](#)

Detective 增加了对以下三种 GuardDuty 查找类型的支持，当对您 AWS 环境中的 Amazon EC2 实例或容器工作负载执行可疑命令时，它们会通知您：

2024 年 11 月 6 日

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

[增加了对 Amazon GuardDuty 调查结果的支持](#)

Detective 现在为以下[GuardDuty 运行时监控查找类型](#)提供支持。

2024 年 8 月 27 日

- Execution:Runtime/SuspiciousShell
- PrivilegeEscalation:Runtime/ElevationToRoot

[增加了对 Amazon GuardDuty 调查结果的支持](#)

Detective 现在支持 [S3 的 GuardDuty 恶意软件防护](#)。这可以帮助您扫描新上传到 Amazon S3 存储桶中的对象，以查找潜在的恶意软件和可疑上传，并在它们被摄入下游进程之前采取措施将其隔离。

2024 年 7 月 9 日

更新了功能	Detective 在 查找组“可视化”面板 中添加了新的径向布局，以提供改进的可视化效果，便于数据解释。	2024 年 6 月 26 日
新的安全湖源版本	除了源版本 1 (OCSF 1.0.0-rc.2) 之外，Detective 现在还会从源版本 2 (OCSF 1.1.0) 中为侦探支持的 Security Lake 源提取数据。	2024 年 5 月 15 日
新的安全湖日志源	您可以使用 Detective 与 Security Lake 的集成，从 Amazon EKS 审核日志中收集日志 和事件。	2024 年 5 月 15 日
文档更新	《亚马逊侦探管理指南》中的内容现已合并到《亚马逊侦探用户指南》中。《Amazon Detective 管理指南》的标准支持将于 2024 年 5 月 8 日结束。	2024 年 4 月 15 日

增加了对 Amazon GuardDuty 调查结果的支持	Detective 现在为以下GuardDuty 运行时监控查找类型提供支持。 • Execution:Runtime/MaliciousFileExecuted • Execution:Runtime/SuspiciousTool • DefenseEvasion:Runtime/PtraceAntiDebugging • Execution:Runtime/SuspiciousCommand • DefenseEvasion:Runtime/SuspiciousCommand	2024 年 4 月 5 日
移除了 Amazon GuardDuty 会员资格要求	您无需再成为 GuardDuty 客户即可启用 Amazon Detective。取消了在 GuardDuty 启用 Detective 之前在账户中启用 48 小时的要求。	2024 年 2 月 2 日
增加了对 Amazon GuardDuty 调查结果的支持	Detective 将对GuardDuty EC2 运行时监控查找类型的支持扩展到 ECS 和 EC2 资源。	2024 年 1 月 30 日

[更新了功能](#)

现在，您可以从“调查”页面对要调查的特定资源进行 Detective 调查。Detective 根据其在调查发现和调查发现组中的活动来建议资源。Det@@[ective Investigations 允许您使用泄露指标调查](#) IAM 用户和 IAM 角色，这可以帮助您确定安全事件中是否涉及资源。

2024 年 1 月 16 日

[更新了功能](#)

现在，您可以针对推荐的资源从“调查”页面运行 Detective 调查。Detective 根据其在调查发现和调查发现组中的活动来建议资源。Det@@[ective Investigations 允许您使用泄露指标调查](#) IAM 用户和 IAM 角色，这可以帮助您确定安全事件中是否涉及资源。

2023 年 12 月 26 日

[Detective 读取共享流量的方式发生了变化 VPCs](#)

如果您使用的是共享 Amazon VPC，则可能会看到 Detective 监控的流量发生了变化。我们建议您查看[VPC 总流量的活动详细信息](#)中的变化，以了解其对您覆盖范围的潜在影响，并查看[Detective 如何计算预计成本](#)，以了解这会如何影响您的服务成本。

2023 年 12 月 20 日

[区域可用性](#)

将欧洲（斯德哥尔摩）、欧洲（巴黎）和加拿大（中部）地区添加到可用 Det@@[ective 与 Security Lake 集成的 AWS](#)区域列表中。

2023 年 12 月 8 日

新特征	Detective 调查 允许您使用漏洞指标调查 IAM 用户和 IAM 角色，这有助于您确定安全事件中是否涉及某个资源。	2023 年 11 月 26 日
新特征	默认情况下，Detective 自动为调查发现组生成 调查发现组摘要 ，由生成式人工智能（生成式 AI）提供支持。调查发现组摘要，快速分析调查发现与受影响资源之间的关系，然后采用自然语言总结潜在威胁。	2023 年 11 月 26 日
新特征	Detective 与 Security Lake 的集成 ，使您可以查询和检索 Security Lake 存储的原始日志数据。使用此集成，您可以从 CloudTrail 管理事件和 Amazon Virtual Private Cloud（Amazon VPC）流日志中收集日志和事件。	2023 年 11 月 26 日
在“安全性”一章中新增了有关托管策略的信息	在 AmazonDetectiveInvestigatorAccess 策略中新增了 Detective 调查和调查发现组摘要操作。	2023 年 11 月 26 日
查看调查发现概述	如果某个调查发现与较大的活动相关，Detective 现在会通知您导航到该调查发现群组。	2023 年 9 月 18 日
Amazon Detective 端点和配额	Detective 现已在以色列（特拉维夫）区域推出。	2023 年 8 月 25 日

增强调查发现群组可视化	Detective 调查发现组可视化现在包括带有汇总调查发现的调查发现组，从而能够更高效地分析相关证据、实体和调查发现。	2023 年 8 月 8 日
增强调查发现群组	调查发现群组现在包括来自 Amazon Inspector 的漏洞调查发现。	2023 年 6 月 13 日
增加了对亚马逊 GuardDuty Lambda 保护的支持	GuardDuty Detective 现在为 Lambda Protection 提供支持。	2023 年 5 月 26 日
将 AWS 安全发现添加为新的可选数据源包。	Detective 现在将 AWS 安全发现作为可选的数据源包提供。该可选数据来源包允许 Detective 从 Security Hub 获取数据，并将这些数据添加到行为图中。	2023 年 5 月 16 日
增加了对 Amazon GuardDuty EKS 运行时监控查找类型的支持	Detective 现在为 GuardDuty EKS 运行时监控查找类型提供支持。	2023 年 5 月 3 日
增加了对 Amazon GuardDuty RDS 保护查找类型的支持	Detective 现在为 GuardDuty RDS 保护查找类型提供支持。	2023 年 4 月 20 日
增加了对其他 Amazon GuardDuty 查找类型的支持	Detective 现在为以下其他 GuardDuty 发现类型提供了配置文件：DefenseEvasion: EC2UnusualDNSResolver DefenseEvasion: EC2UnusualDoHActivity DefenseEvasion: EC2UnusualDoTActivity	2023 年 4 月 12 日

在 Detective 控制台中添加了新的控制台面板，帮助用户根据具体使用情况选择合适的 AWS 托管式策略。	Detective 提供托管式策略，可安全地选择所需的权限。	2023 年 4 月 3 日
显示 EKS 集群的 VPC 流量	新添加了 Amazon Elastic Kubernetes Service (Amazon EKS) 集群的 Amazon Virtual Private Cloud (Amazon VPC) 流量的部分。	2023 年 3 月 2 日
调查发现群组现在包括 Detective 行为图的动态可视化表示	Detective 调查发现群组现在包括 Detective 行为图的动态可视化表示，以强调调查发现群组中实体与调查发现之间的关系。	2023 年 2 月 28 日
从 Detective 摘要页面和搜索结果页面导出数据。数据以逗号分隔值 (CSV) 格式导出。	Detective 现在提供了从 Detective 控制台将数据导出到浏览器的选项。	2023 年 2 月 7 日
添加了 EKS Amazon EKS 工作负载的 VPC 总流量	Detective 现在可从 Amazon Elastic Kubernetes Service Amazon EKS 工作负载中添加有关 Amazon 虚拟私有云 (VPC) 流量日志的可视化摘要和分析。	2023 年 1 月 19 日
在“安全性”一章中新增了有关托管式策略的信息	Detective 现在支持通过 AmazonDetectiveFullAccess 策略 GuardDuty 获取调查结果的操作。现在，安全章节提供了有关 Detective 的以下新托管策略的详细信息：AmazonDetectiveMemberAccess 和 AmazonDetectiveInvestigator Access。	2023 年 1 月 17 日

添加了数据留存功能	使用 Detective，您最多可以访问一年的历史事件数据。	2022 年 12 月 20 日
在摘要页面上添加了调整范围时间的选项。	Detective 现在提供了调整范围时间的选项，以便查看过去 365 天内任何 24 小时时间段的活动。	2022 年 10 月 5 日
搜索调查发现或实体	Detective 现在提供不区分大小写的搜索功能。	2022 年 10 月 3 日
添加了设置范围时间戳的功能	Detective 现在提供了一种配置范围时间戳格式首选项的方法。此首选项将应用于 Detective 中的所有时间戳。	2022 年 10 月 3 日
添加了与调查发现群组相关的术语	Detective 现在支持调查发现群组，可在单个显示屏中将相关调查发现关联在一起，帮助调查环境中潜在的恶意活动。在调查发现群组配置文件中，可以转到与该群组相关的实体配置文件以及调查发现概述。	2022 年 8 月 3 日
添加了与 Amazon EKS 审计日志关联的新配置文件	Detective 现在提供了配置文件，允许调查与以下容器相关的实体关联的活动：Amazon EKS 集群、容器镜像、Kubernetes 容器组 (pod) 和 Kubernetes 主题。	2022 年 7 月 26 日

添加了新的可选数据来源	Detective 现在支持将 EKS 审计日志作为可选数据来源包。管理员账户可以为其现有行为图启用这一新数据来源。默认情况下，在此日期之后创建的图表将启用此数据来源。管理员可以随时手动禁用此数据来源。	2022 年 7 月 26 日
Detective 的新服务相关角色和托管式策略	Detective 现在有一个与服务相关的角色，即 <code>AWSServiceRoleForDetective</code> 。服务相关角色用于代表您访问 Organizations 数据。该角色使用新的 <code>AmazonDetectiveServiceLinkedRolePolicy</code> 托管式策略。	2021 年 12 月 16 日
增加了与的集成 AWS Organizations	Detective 现已与 Organizations 集成。组织管理账户为组织指定了 Detective 管理员账户。Detective 管理员账户可以查看组织中的所有账户，并在组织行为图中启用这些账户作为成员账户。	2021 年 12 月 16 日
将调查发现配置文件替换为调查发现概述	调查发现配置文件包含分析相关资源活动的可视化内容。新的发现概述包含从中 GuardDuty 提取的发现细节以及相关实体的列表。可以从调查发现概述中转到相关实体的配置文件。	2021 年 9 月 20 日

[移除了对支持的 GuardDuty 查找类型的限制](#)

Detective 不再局限于一组选定的 GuardDuty 查找类型。Detective 会自动收集所有调查发现类型的调查发现详细信息，并提供对相关实体的实体配置文件的访问权限。

2021 年 9 月 20 日

[从关联的调查发现概述配置文件面板链接到调查发现详细信息](#)

在实体配置文件中，当在关联的调查发现列表中选择一项调查发现时，调查发现的详细信息将显示在右侧的面板中。范围时间设置为调查发现时间窗口。

2021 年 9 月 20 日

[在 Detective 中的可用实体类型中添加了 S3 存储桶](#)

Detective 现在提供 S3 存储桶的配置文件。S3 存储桶配置文件提供与 S3 存储桶交互的主体以及他们在 S3 存储桶上执行的 API 操作的详细信息。

2021 年 9 月 20 日

[在 Splunk URLs 中生成 Detective 的新选项](#)

Splunk Trumpet 项目允许你向 Splunk 发送 AWS 内容。该项目现在允许您添加 Detective URLs 以导航到配置文件以获取 GuardDuty 发现。

2021 年 9 月 8 日

[已 AKIDs 在账户和角色的活动详情中替换](#)

在账户资料中，“总体 API 调用量”的活动详细信息现在显示用户或角色，而不是访问密钥标识符 (AKIDs)。在角色配置文件中，“总体 API 调用量”的活动详细信息现在显示的是角色会话，而不是 AKIDs。对于在此更改之前发生的活动，调用者将被列为未知资源。

2021 年 7 月 14 日

[在有关 API 调用的信息中添加了调用服务](#)

在 Detective 控制台上，有关 API 调用的信息现在包括发出调用的服务。在关于 API 调用总量、新观察到的 API 调用和数量增加的 API 调用的列表中添加了服务列。在 API 调用总量和新观察到的地理位置的活动详细信息中，API 方法按照发出这些方法的服务进行了归类。对于在此更改之前发生的活动，API 方法归类为未知服务。

2021 年 7 月 14 日

[用户、角色和角色会话的新资源交互选项卡](#)

用户、角色和角色会话的资源交互选项卡包含涉及这些实体的角色代入活动信息。对于角色会话，这是一个新选项卡。对于用户和角色，这是一个包含新内容的现有选项卡。

2021 年 6 月 29 日

[更新了行为图数据量配额值](#)

增加了行为图的数据量配额。在每天 3.24 TB 的情况下，Detective 会发出警告。在每天 3.6 TB 的情况下，无法添加新账户。在每天 4.5 TB 的情况下，Detective 停止向行为图输入数据。

2021 年 6 月 10 日

[在 Python 脚本选项中添加了标签值](#)

使用 Detective Python 脚本 `enableDetective.py` 启用 Detective 时，您现在可以将标签值分配给行为图。

2021 年 5 月 19 日

添加了自动启用通过数据量检查的成员账户的功能	当成员账户接受邀请时，其状态为已接受（未启用），直到 Detective 确认其数据不会导致行为图数据量超过配额。如果数据量没有问题，Detective 会自动将状态更改为已接受（已启用）。请注意，当前已接受（未启用）的现有成员账户无法自动启用。	2021 年 5 月 12 日
在“安全性”一章中新增了有关托管式策略的信息	“安全性”一章中新增了一节，详细介绍了 Detective 的托管式策略。Detective 目前提供单一托管式策略，即 AmazonDetectiveFullAccess。	2021 年 5 月 10 日
更改了成员账户列表中的数据量值	在账户管理页面，成员账户列表现在会显示每个成员账户的每日数据量。此前，列表显示流量表示为允许总流量的百分比。	2021 年 4 月 29 日
修改了管理成员账户的选项	将管理账户菜单替换为操作菜单。合并了添加个人账户和从 .csv 文件添加账户的选项。将启用账户从管理账户移至操作旁边的单独选项。	2021 年 4 月 5 日
添加了行为图谱标签和基于标签的授权	启用 Detective 后，您就可以向行为图添加标签。您可以从常规页面管理行为图的标签。Detective 还支持基于标签值的授权。	2021 年 3 月 31 日

[增加了对其他 Amazon GuardDuty 查找类型的支持](#)

Detective 现在为以下其他 GuardDuty 发现类型提供配置文件：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 29 日

[为 AWS GovCloud \(US\) 区域添加了差异](#)

Detective 现已在各 AWS GovCloud (US) 地区上线。在 AWS GovCloud (美国东部) 和 AWS GovCloud (美国西部)，Detective 不会向成员账户发送邀请电子邮件。Detective 也不会自动删除在 AWS 中关闭的成员账户。

2021 年 3 月 24 日

添加了根据成员账户状态筛选成员账户列表的选项卡	成员账户列表现在显示选项卡，可以使用这些选项卡根据成员账户状态筛选列表。您可以查看所有成员账户、状态为已接受（启用）的成员账户或状态不是已接受（启用）的成员账户。	2021 年 3 月 16 日
增加了对其他 Amazon GuardDuty 查找类型的支持	Detective 现在为以下其他 GuardDuty 发现类型提供了配置文件：Backdoor:EC2/C&CActivity.B Impact:EC2/PortSweep、Impact:EC2/WinRMBruteForce、和 PrivilegeEscalation:IAMUser/AdministrativePermissions	2021 年 3 月 4 日
在 Python 脚本中添加了隐藏邀请电子邮件的选项	Detective enableDetective.py 脚本现在提供了 --disable_email 选项。加入该选项后，Detective 不会向成员账户发送邀请电子邮件。	2021 年 2 月 26 日
将“主账户”更改为“管理员账户”	术语“主账户”已更改为“管理员账户”。该术语在 Detective 控制台和 API 中也做了更改。	2021 年 2 月 25 日
将“主账户”更改为“管理员账户”	术语“主账户”已更改为“管理员账户”。该术语在 Detective 控制台和 API 中也做了更改。	2021 年 2 月 25 日

为配置文件面板“进出调查发现 IP 地址的 VPC 流量”增加了活动详细信息	配置文件面板进出调查发现 IP 地址的 VPC 流量现在可以显示活动详细信息。只有当调查发现与单个 IP 地址相关联时，才会显示活动详细信息。活动详细信息显示每个端口、协议和方向组合的流量。	2021 年 2 月 25 日
添加了不向成员账户发送邀请电子邮件的 API 选项	使用 Detective API 添加成员账户时，管理员账户可以选择不向成员账户发送邀请电子邮件。	2021 年 2 月 25 日
为 IP 地址配置文件上的“API 调用总量”配置文件面板提供新的活动详细信息	现在可以从 API 调用总量配置文件面板中显示 IP 地址的活动详细信息。活动详细信息显示从该 IP 地址发出调用的每个资源的成功和失败调用次数。	2021 年 2 月 23 日
在 IP 地址配置文件上新增“VPC 的总流量”配置文件面板	IP 地址配置文件现在包含 VPC 的总流量配置文件面板。该配置文件面板显示进出该 IP 地址的 VPC 流量。您可以显示活动详细信息以显示 IP 地址与之通信的每个 EC2 实例的音量。	2021 年 1 月 21 日
添加了 Detective 摘要页面	Detective Summary 页面包含可视化效果，可根据地理位置、API 调用次数和 Amazon EC2 流量引导分析师找到感兴趣的实体。	2021 年 1 月 21 日

[更新了从 Amazon 转向 Detective GuardDuty 的选项](#)

在中 GuardDuty，“在侦探中调查”选项已从“操作”菜单移至查找结果详细信息面板。它会显示相关实体的列表。如果是支持的调查发现类型，则列表中还包括该调查发现。然后，可以选择导航到实体配置文件或调查发现配置文件。

2021 年 1 月 15 日

[添加了将活动详细信息窗口设置为默认范围时间的选项](#)

在 API 调用总量和 VPC 的总流量的活动详细信息中，可以将活动详细信息的时间窗口设置为配置文件的默认范围时间。

2021 年 1 月 15 日

[为实体添加了处理超长时间间隔的功能](#)

添加了一条新通知，用于在实体有一个或多个超长时间间隔时显示。新的大量实体页面显示了当前范围内的所有超长时间间隔。

2020 年 12 月 18 日

[成员账户配额增加到 1200](#)

主账户现在可以邀请多达 1200 个成员账户访问其行为图谱。之前的限额为 1000。

2020 年 12 月 11 日

[增加了行为图数据量配额值](#)

更新了有关行为图数据量配额的信息，添加了具体的配额值。

2020 年 12 月 11 日

[在 API 调用总量配置文件面板上添加了活动详细信息的时间范围选择](#)

在 API 调用总量面板上，现在可以显示任何选定时间范围内的活动详细信息。面板最初会显示一个选项，用于显示范围时间的活动详细信息。

2020 年 9 月 29 日

在“VPC 的总流量”配置文件面板上添加了活动详细信息的时间区间选择	在 VPC 的总流量面板上，可以显示图表中单个时间区间的活动详细信息。要显示时间间隔的详细信息，请选择该时间间隔。	2020 年 9 月 25 日
新角色会话和联合用户实体	Detective 现在允许浏览和调查联合身份验证。可以查看每个角色由哪些资源代入，以及这些身份验证是什么时候进行的。	2020 年 9 月 17 日
范围时间管理更新	已删除锁定或解锁范围时间的选项。它始终处于锁定状态。在调查发现配置文件上，如果范围时间与调查发现时间窗口不同，则会显示警告。	2020 年 9 月 4 日
滚动浏览配置文件时，配置文件标题仍然可见	在配置文件上，当滚动浏览选项卡上的配置文件面板时，类型、标识符和范围时间仍然可见。当选项卡不可见时，可以使用页面导览痕迹中的选项卡下拉列表导航到其他选项卡。	2020 年 9 月 4 日
搜索始终显示搜索结果	进行搜索时，搜索结果会显示在搜索页面上。可以从结果中转到调查发现或实体配置文件。	2020 年 8 月 27 日
已添加到允许的搜索条件中	允许的搜索条件已经扩大。您可以按名称搜索 AWS 用户和 AWS 角色。您可以使用 ARN 搜索结果、AWS 角色、AWS 用户和 EC2 实例。	2020 年 8 月 27 日

[从配置文件面板链接到其他控制台](#)

在 EC2 实例详情配置面板上，EC2 实例标识符链接到 Amazon EC2 控制台。在用户详细信息和角色详细信息配置文件面板上，用户名和角色名称链接到 IAM 控制台。

2020 年 8 月 14 日

[VPC 流量数据的活动详细信息](#)

VPC 的总流量配置文件面板现在提供对活动详细信息的访问。活动详细信息显示选定时间段内 IP 地址和 EC2 实例之间的流量。

2020 年 7 月 23 日

[成员账户现在可以查看其使用情况和预计费用](#)

成员账户现在可以查看自己的使用信息。对于成员账户，使用情况页面会显示他们提供的每个行为图中采集的数据量。成员账户还可以查看其 30 天的预计费用。

2020 年 5 月 26 日

[免费试用现在是按账户而不是按行为图进行的](#)

现在，每个账户 Amazon Detective 都会在每个区域内获得单独的免费试用。免费试用从账户启用 Detective 或账户首次作为成员账户启用时开始。

2020 年 5 月 26 日

[开启了新的开源 Python 脚本 GitHub](#)

上的新[amazon-detective-multiaccount-scripts](#)存储库 GitHub 提供了开源 Python 脚本，您可以使用这些脚本来管理跨区域的行为图。您可以启用 Detective、添加成员账户、删除成员账户和禁用 Detective。

2020 年 1 月 21 日

[Amazon Detective 简介](#)

Detective 使用机器学习和专用可视化技术，帮助分析和调查整个 Amazon Web Services (AWS) 工作负载中的安全问题。

2019 年 12 月 2 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。