



使用者指南

# Amazon Detective



# Amazon Detective: 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 Detective ? .....	1
Amazon Detective 的功能 .....	1
存取 Amazon Detective .....	3
Amazon Detective 定價 .....	4
Detective 如何運作? .....	4
誰在使用 Detective? .....	5
相關服務 .....	5
概念和術語 .....	7
開始使用 .....	11
設定 .....	11
註冊 AWS 帳戶 .....	11
建立具有管理存取權的使用者 .....	12
先決條件 .....	13
授予必要的 Detective 許可 .....	13
支援的 AWS Command Line Interface 版本 .....	13
建議 .....	14
建議與 GuardDuty 和 對齊 AWS Security Hub CSPM .....	14
建議更新 GuardDuty CloudWatch 的通知頻率 .....	14
啟用 Detective .....	15
檢查 Detective 是否正在擷取資料 .....	16
行為圖表中的資料 .....	18
Detective 如何填入行為圖表 .....	18
Detective 如何處理來源資料 .....	19
Detective 擷取 .....	19
Detective 分析 .....	19
新行為圖表的訓練期間 .....	19
行為圖表資料結構概觀 .....	20
行為圖表資料結構中元素的類型 .....	20
行為圖表資料結構中的實體類型 .....	21
行為圖表中使用的來源資料 .....	26
Detective 中核心資料來源的類型 .....	26
Detective 中選用的資料來源的類型 .....	27
Amazon EKS 稽核日誌 .....	28
AWS 安全調查結果 .....	29

Detective 如何擷取和儲存來源資料 .....	30
Detective 如何強制執行行為圖表的資料量配額 .....	30
「摘要」儀表板 .....	32
調查 .....	32
新觀察到的地理位置 .....	33
過去 7 天內作用中的調查結果群組 .....	33
具有最大 API 呼叫量的角色和使用者 .....	33
具有最大流量的 EC2 執行個體 .....	34
具有最多 Kubernetes Pod 的容器叢集 .....	34
近似值通知 .....	35
Detective 如何用於調查 .....	36
調查階段 .....	36
Detective 調查的起點 .....	36
GuardDuty 偵測到的調查結果 .....	37
AWS Security Hub CSPM 彙總的安全性調查結果 .....	37
從 Detective 來源資料擷取的實體 .....	37
Detective 調查流程 .....	37
Detective 調查 .....	39
執行 Detective 調查 .....	39
檢閱 Detective Investigations 報告 .....	42
了解 Detective Investigations 報告 .....	42
Detective Investigations 報告摘要 .....	43
下載 Detective Investigations 報告 .....	44
封存 Detective Investigations 報告 .....	45
分析問題清單 .....	46
調查結果概觀 .....	46
用於調查結果概觀的範圍時間 .....	46
調查結果詳細資訊 .....	47
相關實體 .....	47
故障診斷「找不到頁面」 .....	47
尋找群組 .....	48
了解調查結果群組頁面 .....	49
調查結果群組中的資訊調查結果 .....	50
調查結果群組設定檔 .....	51
調查結果群組視覺化 .....	52
調查結果群組摘要 .....	55

檢閱調查結果群組摘要 .....	55
選擇退出問題清單群組摘要 .....	57
啟用調查結果群組摘要 .....	57
跨區域推論 .....	58
支援的區域 .....	58
封存 GuardDuty 調查結果 .....	59
分析實體 .....	60
使用實體設定檔 .....	60
實體設定檔的範圍時間 .....	60
實體識別符和類型 .....	61
涉及的調查結果 .....	61
與此實體相關的調查結果群組 .....	61
包含實體詳細資訊和分析結果的設定檔 .....	61
在實體設定檔中導覽 .....	62
設定檔面板 .....	62
設定檔面板上的資訊類型 .....	62
設定檔面板視覺化類型 .....	65
設定檔面板的偏好設定 .....	69
導覽至實體設定檔 .....	70
從其他主控台錨定 .....	70
透過 URL 導覽 .....	72
向 Splunk 新增 Detective 調查結果的 URL .....	76
錨定至其他主控台 .....	76
錨定至另一實體設定檔 .....	76
瀏覽活動詳細資訊 .....	76
整體 API 呼叫量 .....	77
地理位置 .....	84
整體 VPC 流量 .....	87
整體 Kubernetes API 呼叫量 .....	91
管理範圍時間 .....	95
設定特定開始和結束日期及時間 .....	96
編輯範圍時間的時間長度 .....	96
將範圍時間設定為調查結果時間範圍 .....	97
在摘要頁面上設定範圍時間 .....	97
檢視實體的調查結果 .....	97
大量實體 .....	98

什麼是大量實體？ .....	98
檢視設定檔上的大量實體通知 .....	99
檢視當前範圍時間的大量實體清單 .....	99
搜尋調查結果或實體 .....	101
完成搜尋 .....	101
對搜尋結果進行排序 .....	103
搜尋疑難排解 .....	103
管理帳戶 .....	104
限制與建議 .....	104
成員帳戶的數目上限 .....	104
帳戶和區域 .....	105
管理員帳戶與 Security Hub CSPM 和 GuardDuty 的一致性 .....	105
授予管理員帳戶所需的許可 .....	105
反映組織在 Detective 中的更新 .....	105
使用 Organizations 管理行為圖表帳戶 .....	106
為組織指定 Detective 管理員帳戶 .....	106
啟用組織帳戶作為成員帳戶 .....	107
指定 Detective 管理員帳戶 .....	107
指定 Detective 管理員 .....	108
移除 Detective 管理員帳戶 .....	111
帳戶的可用動作 .....	113
檢視帳戶清單 .....	114
列出帳戶 (主控台) .....	115
列出您的成員帳戶 (Detective API AWS CLI) .....	117
管理組織成員帳戶 .....	118
啟用新的組織帳戶 .....	118
將組織帳戶啟用為 Detective 成員帳戶 .....	120
取消組織帳戶的關聯 .....	121
管理受邀成員帳戶 .....	122
邀請個別帳戶加入行為圖表 .....	123
邀請成員帳戶清單至行為圖表 .....	125
啟用未啟用的成員帳戶 .....	127
移除成員帳戶 .....	128
針對成員帳戶：管理邀請和成員資格 .....	129
成員帳戶的 IAM 政策 .....	130
檢視行為圖表的邀請 .....	131

回應行為圖表邀請 .....	132
從行為圖表中移除帳戶 .....	133
帳戶動作的影響 .....	134
Detective 遭到停用 .....	134
成員帳戶遭到從行為圖表中移除 .....	134
成員帳戶離開組織 .....	135
AWS 帳戶已暫停 .....	135
AWS 帳戶已關閉 .....	135
Amazon Detective Python 指令碼 .....	136
enableDetective.py 指令碼概觀 .....	136
disableDetective.py 指令碼概觀 .....	137
指令碼的必要許可 .....	137
為 Python 指令碼設置執行環境 .....	138
建立要新增或移除的成員帳戶 .csv 清單 .....	140
執行 enableDetective.py .....	140
執行 disableDetective.py .....	142
與 Security Lake 的偵測整合 .....	144
啟用整合 .....	144
開始之前 .....	146
步驟 1：在 Detective 中建立 Security Lake 訂閱者 .....	146
步驟 2：新增必要的 IAM 許可 .....	147
步驟 3：接受資源共享 ARN 邀請 .....	149
變更 Detective 整合組態 .....	156
支援 AWS 的區域 .....	157
在 Detective 中查詢原始日誌 .....	158
查詢 AWS 角色的原始日誌 .....	162
查詢 Amazon EKS 叢集的原始日誌 .....	163
查詢 Amazon EC2 執行個體的原始日誌 .....	163
停用整合 .....	163
刪除 CloudFormation 堆疊 .....	164
預測和監控成本 .....	166
關於行為圖表的免費試用 .....	166
選用的資料來源的免費試用 .....	167
管理員帳戶用量和費用 .....	167
為每個帳戶擷取的資料量 .....	168
行為圖表的預計成本 .....	168

行為圖表的預計成本 .....	168
來源套件擷取的資料量 .....	169
成員帳戶用量追蹤 .....	169
每個行為圖表的擷取量 .....	169
跨行為圖表的預計成本 .....	170
Detective 如何計算預計成本 .....	170
安全 .....	172
資料保護 .....	172
金鑰管理 .....	173
身分與存取管理 .....	174
目標對象 .....	174
使用身分來驗證 .....	174
使用政策管理存取權 .....	175
Amazon Detective 如何搭配 IAM 運作 .....	177
身分型政策範例 .....	181
AWS 受管政策 .....	187
使用服務連結角色 .....	197
對身分與存取進行疑難排解 .....	199
法規遵循驗證 .....	201
恢復能力 .....	201
基礎架構安全 .....	202
VPC 端點 (AWS PrivateLink) .....	202
Detective VPC 端點的考量事項 .....	202
建立 Detective 的介面 VPC 端點 .....	203
為 Detective 建立 VPC 端點政策 .....	203
共用子網路 .....	204
安全最佳實務 .....	204
Detective 管理員帳戶的最佳實務 .....	204
成員帳戶最佳實務 .....	204
記錄API通話 .....	205
中的偵測資訊 CloudTrail .....	205
了解 Detective 日誌檔案項目 .....	206
區域和配額 .....	208
Detective 區域與端點 .....	208
Detective 配額 .....	208
不支援 Internet Explorer 11 .....	208

---

管理標籤 .....	209
檢視行為圖的標籤 .....	209
將標籤新增至行為圖 .....	210
從行為圖中移除標籤 .....	211
停用 Amazon Detective .....	212
停用 Detective (主控台) .....	212
停用 Detective (Detective API) AWS CLI .....	212
停用跨區域的 Detective (GitHub 上的 Python 指令碼) .....	213
文件歷史紀錄 .....	214
.....	CCXXXIV

# 什麼是 Amazon Detective ？

Amazon Detective 會協助您分析、調查並快速識別安全調查結果或可疑活動的根本原因。Detective 會自動從您的AWS資源收集日誌資料。Detective 接著會使用機器學習、統計分析和圖論來產生視覺化內容，協助您更快地進行有效率的安全調查。Detective 提供預先建置的資料彙總、摘要和內容，可協助您快速分析並判斷潛在安全問題的本質和範圍。

使用 Detective ，您可以訪問長達一年的歷史事件資料。此資料可透過一組視覺化取得，視覺化可顯示已選取時間範圍內活動類型和數目的變化。Detective 將此類變更連結至 GuardDuty 調查結果。如需 Detective 中來源資料的詳細資訊，請參閱 [the section called “行為圖表中使用的來源資料”](#)。

透過自動彙總資料並提供視覺化工具，Amazon Detective 可讓您更快、更有效率地進行安全調查。您可以快速分析潛在問題，並判斷安全威脅的範圍。

## 主題

- [Amazon Detective 的功能](#)
- [存取 Amazon Detective](#)
- [Amazon Detective 定價](#)
- [Detective 如何運作？](#)
- [誰在使用 Detective ？](#)
- [相關服務](#)

## Amazon Detective 的功能

以下是 Amazon Detective 有助於調查AWS環境中可疑活動和分析資源以識別安全問題根本原因的一些重要方式。

### Detective 調查結果群組

[Detective 調查結果群組](#)可讓您檢查與潛在安全事件相關的多個活動。您可以使用調查結果群組來分析高嚴重性 GuardDuty 調查結果的根本原因。如果威脅行為者嘗試入侵您的AWS環境，他們通常會執行一系列動作，產生多個安全調查結果和異常行為。

Detective 中的調查結果群組頁面會顯示從您的行為圖表擷取的所有相關調查結果群組。如需如何利用調查結果群組來分析安全調查結果根本原因的詳細資訊，請參閱 [Detective 中的分析調查結果群組](#)。

Detective 提供每個調查結果群組的互動式視覺化，協助您更快速且更徹底地調查安全問題。視覺化旨在顯示與安全事件相關的實體和調查結果，讓您更輕鬆地了解連線和根本原因。可協助您更快速、更徹底地調查問題，而不需費力。[問題清單群組視覺化](#)面板會顯示問題清單群組中涉及的問題清單和實體。

## 分類問題清單的偵測調查

透過 [Detective 調查](#)，您可以使用入侵指標調查 IAM 使用者和 IAM 角色，這可協助您判斷資源是否涉及安全事件。入侵指標 (IOC) 指在網路、系統或環境中或在網路、系統或環境上觀察到的成品，可以 (具有高可信度) 識別惡意活動或安全事件。透過 Detective 調查，您可以最大化效率、專注於安全威脅，並強化事件回應功能。

Detective Investigation 使用機器學習模型和威脅情報，僅顯示最關鍵、可疑的問題，讓您專注於高階調查。它會自動分析您AWS環境中的資源，以識別入侵或可疑活動的潛在指標。這可讓您識別模式，並了解哪些資源受到安全事件的影響，提供主動的威脅識別和緩解方法。

您可以透過執行 Detective 調查，從 Detective 主控台啟動 [Detective 調查](#)。若要以程式設計方式執行調查，請使用 Detective API 的 [StartInvestigation](#) 操作。若要使用AWS Command Line Interface(AWS CLI) 執行調查，請執行 [start-investigation](#) 命令。

## Detective 與 Amazon Security Lake 整合

[Detective 與 Amazon Security Lake 整合](#)，這表示您可以查詢和擷取 Security Lake 存放的原始日誌資料。透過此整合，您可以從 Security Lake 原生支援的下列來源收集日誌和事件。

- AWS CloudTrail管理事件 1.0 版及更新版本
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌 1.0 版及更新版本
- Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌 2.0 版

將 Detective 與 Security Lake 整合之後，Detective 會開始從 Security Lake 提取與AWS CloudTrail 管理事件和 Amazon VPC 流程日誌相關的原始日誌。您可以[查詢原始日誌](#)以檢視 Detective 中的日誌和事件。

## 調查 VPC 流量

透過 Detective，您可以互動方式檢查 Amazon Elastic Compute Cloud ([Amazon EC2](#)) 執行個體和 [Kubernetes Pod 的虛擬私有雲端 \(VPC\) 網路流程的活動詳細資訊](#)。Amazon EC2 Detective 會自動從您的受監控帳戶收集 VPC 流程日誌、依 EC2 執行個體彙總它們，並呈現這些網路流程的視覺化摘要和分析。

針對 EC2 執行個體，整體 VPC 流量的活動詳細資訊會顯示所選時間範圍內 EC2 執行個體和 IP 地址之間的互動。

針對 Kubernetes Pod，整體 VPC 流量會針對所有目的地 IP 地址，顯示 Kubernetes Pod 指派之 IP 地址的進出整體位元組量。

## 存取 Amazon Detective

Amazon Detective 適用於大多數 AWS 區域。如需目前可使用 Detective 的區域清單，請參閱《》中的 [Amazon Detective 端點和配額](#) AWS 一般參考。如需有關管理 AWS 區域的資訊 AWS 帳戶，請參閱《AWS 帳戶管理參考指南》中的 [指定 AWS 區域您的帳戶可以使用哪些](#)。

在每個區域中，您可以透過下列任何方式使用 Detective。

### AWS 管理主控台

AWS 管理主控台是以瀏覽器為基礎的界面，可用來建立和管理 AWS 資源。作為該主控台的一部分，Amazon Detective 主控台可讓您存取 Detective 帳戶、資料和資源。您可以使用 Detective 主控台來執行任何 Detective 任務：檢閱潛在的安全威脅，並分析、調查和識別安全調查結果的根本原因。

### AWS 命令列工具

使用 AWS 命令列工具，您可以在系統的命令列發出命令，以執行 Detective 任務和 AWS 任務。使用命令列比使用主控台更快、更方便。若您想要建構執行任務的指令碼，命令列工具也非常實用。

AWS 提供兩組命令列工具：AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell。如需安裝和使用的詳細資訊 AWS CLI，請參閱 [AWS Command Line Interface](#) 《[使用者指南](#)》。如需安裝和使用 Tools for PowerShell 的相關資訊，請參閱 [AWS Tools for PowerShell 使用者指南](#)。

### AWS SDKs

AWS 提供 SDKs，其中包含適用於各種程式設計語言和平台的程式庫和範本程式碼，例如 Java、Go、Python、C++ 和 .NET。SDKs 提供 Detective 和其他的便利、程式設計存取 AWS 服務。它們也會處理諸如密碼編譯簽署請求、管理錯誤以及自動重試請求等任務。如需有關安裝和使用 AWS SDKs 的資訊，請參閱 [要建置的工具 AWS](#)。

### Amazon Detective REST API

Amazon Detective REST API 可讓您以程式設計方式存取 Detective 帳戶、資料和資源。使用此 API，您可以將 HTTPS 請求直接傳送至 Detective。不過，與 AWS 命令列工具和 SDKs 不同，使用

此 API 需要您的應用程式處理低階詳細資訊，例如產生雜湊來簽署請求。如需此 API 的相關資訊，請參閱 [Detective API 參考](#)。

## Amazon Detective 定價

如同其他AWS產品，使用 Amazon Detective 沒有合約或最低承諾。

Detective 定價基於多個維度 - 並針對所有資料收取每 GB 的分層固定費率，無論來源為何。如需詳細資訊，請參閱 [Amazon Detective 定價](#)。

為了協助您了解和預測使用 Detective 的成本，Detective 為您的帳戶提供預估的使用成本。您可以在 Amazon Detective 主控台上[檢閱這些預估值](#)，並使用 [Amazon Detective API 存取這些預估值](#)。視您使用服務的方式而定，使用其他AWS 服務搭配某些 Detective 功能可能會產生額外費用，例如 Security Lake 整合和 Detective Investigations。

當您第一次啟用 Detective 時，您的AWS 帳戶會自動註冊 Detective 的 30 天免費試用。這包括在中啟用做為組織一部分的個別帳戶AWS Organizations。在免費試用期間，在適用的中使用 Detective 無需付費AWS 區域。

為了協助您了解和預測免費試用結束後使用 Detective 的成本，Detective 會根據您在試用期間使用 Detective 的情況，為您提供預估的使用成本。您的用量資料也會指出免費試用結束前剩餘的時間量。您可以在 [Amazon Detective 主控台上檢閱 Detective 帳戶的用量相關資料](#)，並使用 Amazon Detective API 存取資料。

## Detective 如何運作？

Detective 會自動從 和 Amazon VPC 流程日誌擷取以時間為基礎的事件，例如登入嘗試、API 呼叫 AWS CloudTrail和網路流量。它還會擷取 GuardDuty 偵測到的調查結果。

透過此類事件，Detective 使用機器學習和視覺化來建立資源行為的統一互動式檢視，以及它們之間在一段時間後的互動。您可以探索此行為圖表，以檢查潛在的惡意動作，例如失敗的登入嘗試或可疑的 API 呼叫。您也可以查看這些動作如何影響AWS帳戶和 Amazon EC2 執行個體等資源。您可以針對各種任務調整行為圖表的範圍和時間軸：

- 快速調查任何超出規範的活動。
- 識別可能表示安全問題的模式。
- 了解所有受調查結果影響的資源。

Detective 量身訂做的視覺化可為帳戶資訊提供基準並進行摘要。此類調查結果可以幫助回答「這是否為對此角色的異常 API 呼叫」等問題嗎？或「這是預期來自此執行個體的流量激增嗎」？

透過 Detective，您就無需再整理任何資料，也無需再開發、設定或調整自己的查詢和演算法。沒有前期成本，您僅需為分析的事件付費，不再需要部署其他軟體或訂閱其他摘要。

## 誰在使用 Detective？

當帳戶啟用 Detective 後，它會成為行為圖表的管理員帳戶。行為圖表是從一或多個AWS帳戶擷取和分析資料的一組連結。管理員帳戶邀請成員帳戶將其資料提供至管理員帳戶的行為圖表。

Detective 也與 整合AWS Organizations。組織管理帳戶會指定組織的 Detective 管理員帳戶。Detective 管理員帳戶會在組織行為圖表中啟用組織帳戶作為成員帳戶。

如需 Detective 如何使用行為圖表帳戶中來源資料的相關資訊，請參閱 [the section called “行為圖表中使用的來源資料”](#)。

如需管理員帳戶如何管理行為圖表的相關資訊，請參閱 [管理帳戶](#)。如需成員帳戶如何管理其行為圖表邀請和成員資格的相關資訊，請參閱 [the section called “針對成員帳戶：管理邀請和成員資格”](#)。

管理員帳戶使用行為圖表產生的分析和視覺化來調查AWS資源和 GuardDuty 調查結果。使用 Detective 與 GuardDuty 整合AWS Security Hub CSPM，您可以將這些服務中的 GuardDuty 調查結果直接轉向 Detective 主控台。

Detective 調查著重於與所涉AWS資源相關的活動。有關 Detective 中調查過程的概觀，請參閱《Detective 使用者指南》中的 [Amazon Detective 如何用於調查](#)。

## 相關服務

若要進一步保護 中的資料、工作負載和應用程式AWS，請考慮使用下列AWS 服務搭配 Amazon Detective。

### AWS Security Hub CSPM

AWS Security Hub CSPM可讓您全面檢視AWS資源的安全狀態，並協助您根據安全產業標準和最佳實務檢查AWS環境。這部分是透過取用、彙總、組織和排定來自多個AWS 服務 (包括 Detective) 和支援AWS合作夥伴網路 (APN) 產品的安全性調查結果優先順序來執行。Security Hub CSPM 可協助您分析安全趨勢，並識別整個AWS環境中最優先的安全問題。

若要進一步了解 Security Hub CSPM，請參閱 [AWS Security Hub CSPM使用者指南](#)。

## Amazon GuardDuty

Amazon GuardDuty 是一種安全監控服務，可分析和處理特定類型的AWS日誌，例如 Amazon S3 和 CloudTrail 管理事件日誌AWS CloudTrail的資料事件日誌。它使用威脅情報摘要，例如惡意 IP 地址和網域的清單，以及機器學習，來識別AWS環境中非預期和可能未經授權的惡意活動。

若要進一步了解 GuardDuty，請參閱 [Amazon GuardDuty 使用者指南](#)。

## Amazon Security Lake

Amazon Security Lake 是完全受管的安全資料湖服務。您可以使用 Security Lake，將來自AWS環境、SaaS 提供者、內部部署來源、雲端來源和第三方來源的安全資料，自動集中到存放在您AWS帳戶中的專用資料湖。Security Lake 可協助您分析安全資料，讓您更全面地了解整個組織的安全狀態。透過 Security Lake，您還可以改善工作負載、應用程式和資料的保護。

若要進一步了解 Security Lake，請參閱 [Amazon Security Lake 使用者指南](#)。若要進一步了解如何同時使用 Detective 和 Security Lake，請參閱 [與 Security Lake 的偵測整合](#)。

若要了解其他AWS安全服務，請參閱 [上的安全、身分和合規AWS](#)。

# Amazon Detective 概念和術語

以下術語和概念相當重要，能協助您了解 Amazon Detective 及其運作方式。

## 管理員帳戶

AWS 帳戶擁有行為圖表並使用行為圖表進行調查的。

管理員帳戶會邀請成員帳戶將其資料提供至行為圖表。如需詳細資訊，請參閱[the section called “管理受邀成員帳戶”](#)。

對於組織行為圖表，管理員帳戶是組織管理帳戶指定的 Detective 管理員帳戶。如需詳細資訊，請參閱 [the section called “指定 Detective 管理員帳戶”](#)。Detective 管理員帳戶可以在組織行為圖表中將任何組織帳戶作為成員帳戶啟用。如需詳細資訊，請參閱 [the section called “管理組織成員帳戶”](#)。

管理員帳戶也可以檢視行為圖表的資料用量，並從行為圖表中移除成員帳戶。

## 自治系統組織 (ASO)

被分配了自治系統的標題組織。該自主系統是異質網路或一組使用類似路由邏輯和政策的網路。

## 行為圖表

從傳入來源資料產生的連結資料集，該資料與一個或多個AWS 帳戶相關聯。

每個行為圖表都使用相同的調查結果、實體和關係。

## 委派管理員帳戶 (AWS Organizations)

在組織中，服務的委派管理員帳戶能夠管理組織服務的使用情況。

在 Detective 中，Detective 管理員帳戶也是委派的管理員帳戶，除非 Detective 管理員帳戶是組織管理帳戶。組織管理帳戶無法成為委派的管理員帳戶。

在 Detective 中，允許自我委派。組織管理帳戶可以委派自己的帳戶成為 Detective 的委派管理員，但這只能在 Detective 的範圍內註冊或記住，並不是適用於組織。

## Detective 管理員帳戶

組織管理帳戶指定為區域中組織行為圖表的管理員帳戶的帳戶。如需詳細資訊，請參閱 [the section called “指定 Detective 管理員帳戶”](#)。

Detective 建議組織管理帳戶選擇其帳戶以外的帳戶。

如果帳戶非組織管理帳戶，則 Detective 管理員帳戶也組織中 Detective 的委派管理員帳戶。

## Detective 來源資料

來自以下摘要類型的已處理、結構化資訊版本：

- 來自AWS服務的日誌，例如AWS CloudTrail日誌和 Amazon VPC 流程日誌
- GuardDuty 調查結果

Detective 使用 Detective 來源資料來填入行為圖表。Detective 也會儲存 Detective 來源資料的副本，以支援其分析。

## 實體

從擷取資料中擷取的項目。

每個實體都有一個類型，用來識別它所代表的物件類型。實體類型的範例包括 IP 地址、Amazon EC2 執行個體和AWS使用者。

實體可以是您管理AWS的資源，或是已與您的資源互動的外部 IP 地址。

針對每個實體，來源資料也會用來填入實體屬性。屬性值可以直接從來源記錄中擷取，也可以跨多個記錄彙總。

## 問題清單

Amazon GuardDuty 偵測到的安全問題。

## 調查結果群組

可能與相同事件或安全問題相關的相關調查結果、實體和證據的集合。Detective 會根據內建的機器學習模型產生調查結果群組。

## Detective 證據

Detective 會根據您在過去 45 天內收集的行為圖表中的資料，識別與調查結果群組相關的其他證據。此證據顯示為嚴重性值為資訊性的調查結果。證據會提供支援資訊，反白顯示在調查結果群組中檢視時，可能可疑的異常活動或未知行為。該範例可能是在調查結果的範圍內新觀察到的地理位置或觀察到的 API 呼叫。目前，這些調查結果只能在 Detective 中檢視，而不會傳送至 Security Hub CSPM。

## 尋找概觀

提供調查結果資訊摘要的單一頁面。

調查結果概觀包含調查結果的相關實體清單。從清單中，您可以錨定至實體的設定檔。

調查結果概觀也包含含有調查結果屬性的詳細資訊面板。

## 大量實體

在時間間隔內與大量其他實體之間有連線或來自大量其他實體的實體。例如，EC2 執行個體可能具有來自數百萬個 IP 地址的連線。連線數目超過 Detective 可容納的臨界值。

當目前的範圍時間包含大量的時間間隔時，Detective 會通知使用者。

如需詳細資訊，請參閱《Amazon Detective 使用者指南》中的[檢視大量實體的詳細資訊](#)。

## 調查

分類可疑或有趣活動，確定其範圍，取得其基礎來源或原因，然後確定如何繼續的過程。

## 成員帳戶

AWS 帳戶管理員帳戶受邀將資料貢獻至行為圖表的。在組織行為圖表中，成員帳戶可以是 Detective 管理員帳戶已啟用為成員帳戶的組織帳戶。

受邀成員帳戶可以回應行為圖表邀請，並從行為圖表中移除其帳戶。如需詳細資訊，請參閱 [the section called “針對成員帳戶：管理邀請和成員資格”](#)。

組織帳戶無法在組織行為圖表中變更其成員資格。

所有成員帳戶也可以在提供資料的行為圖表中檢視其帳戶的用量資訊。

他們沒有對行為圖表的其他存取。

## 組織行為圖表

Detective 管理員帳戶所擁有的行為圖表。組織管理帳戶會指定 Detective 管理員帳戶。如需詳細資訊，請參閱 [the section called “指定 Detective 管理員帳戶”](#)。

在組織行為圖表中，Detective 管理員帳戶控制組織帳戶是否為成員帳戶。組織帳戶無法從組織行為圖表中移除本身。

Detective 管理員帳戶也可以邀請其他帳戶加入組織行為圖表。

## 設定檔

提供與實體活動相關資料視覺化集合的單一頁面。

針對調查結果，設定檔可幫助分析師確定該調查結果是否為真正關注的問題還是誤報。

檔案提供資訊以支援對某項調查結果進行調查，或用於常規尋找可疑活動。

## 設定檔面板

設定檔上的單一視覺化。每個設定檔面板都旨在幫助回答特定問題，以協助分析師進行調查。

設定檔面板可以包含鍵值對、資料表、時間軸、長條圖或地理位置圖。

## 關係

個別實體之間發生的活動。也會從引入來源資料中擷取關係。

與實體類似，關係具有類型，可識別涉及的實體類型和連接方向。關係類型的範例為連接到 Amazon EC2 執行個體的 IP 地址。

## 範圍名稱

用於設定檔上顯示資料範圍的時間範圍。

調查結果的預設範圍時間會反映觀察到可疑活動的首次和末次時間。

實體設定檔的預設範圍時間為前 24 小時。

# Amazon Detective 入門

本教學課程提供 Amazon Detective 的簡介。您將了解如何為 AWS 您的帳戶啟用 Detective。您也將了解如何驗證 Detective 是否已開始將資料從 AWS 您的帳戶擷取並擷取至您的行為圖表。

當您啟用 Amazon Detective 時，Detective 會建立區域特定行為圖表，該圖表將您的帳戶作為其管理員帳戶。初始情況下，該帳戶是行為圖表中的唯一帳戶。然後，管理員帳戶可以邀請其他 AWS 帳戶將其資料貢獻至行為圖表。請參閱 [管理帳戶](#)。

首次在區域中啟用 Detective 也會開始為行為圖表提供 30 天的免費試用。如果該帳戶停用了 Detective，然後再次啟用時，則不提供免費試用。請參閱 [the section called “關於行為圖表的免費試用”](#)。

免費試用之後，會根據行為圖表中各個帳戶所提供的資料，向帳戶進行收費。管理員帳戶可以追蹤用量，並查看其整個行為圖表常規 30 天期間的總預計成本。如需詳細資訊，請參閱 [the section called “管理員帳戶用量和費用”](#)。成員帳戶可以追蹤其所屬行為圖表的用量和預計成本。如需詳細資訊，請參閱 [the section called “成員帳戶用量追蹤”](#)。

## 主題

- [設定 AWS 您的帳戶](#)
- [啟用 Detective 的先決條件](#)
- [啟用 Detective 的建議](#)
- [啟用 Detective](#)

## 設定 AWS 您的帳戶

在啟用 Amazon Detective 之前，您必須具備 AWS 帳戶。如果您沒有 AWS 帳戶，請完成下列步驟來建立帳戶。

### 註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

#### 註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。

## 2. 請遵循線上指示進行。

部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行 [需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

### 保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶您的電子郵件地址，以帳戶擁有者 [AWS 管理主控台](#) 身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的 [以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的 [為您的 AWS 帳戶根使用者（主控台）啟用虛擬 MFA 裝置](#)。

### 建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的 [使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

## 以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

## 指派存取權給其他使用者

- 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

- 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

## 啟用 Detective 的先決條件

在啟用 Detective 之前，請確定符合下列要求。

### 授予必要的 Detective 許可

啟用 Detective 之前，您必須確定 IAM 主體擁有必要的 Detective 許可。主體可以是您正在使用的現有使用者或角色，也可以建立新使用者或角色以用於 Detective。

當您註冊 Amazon Web Services (AWS) 時，您的帳戶會自動註冊所有 AWS 服務服務，包括 Amazon Detective。但若要啟用和使用 Detective，您首先必須設定許可來允許存取 Amazon Detective 主控台和 API 操作。您或您的管理員可以使用 AWS Identity and Access Management (IAM) 將[AmazonDetectiveFullAccess受管政策](#)連接至您的 IAM 主體，以授予所有 Detective 動作的存取權。如果沒有這些 IAM 許可，您可以在 AWS 主控台中檢視 Detective 入門頁面。因此，在新增這些許可之前，主控台不會顯示任何作用中圖形，即使服務已啟用。

### 支援的 AWS Command Line Interface 版本

若要使用 AWS CLI 執行 Detective 任務，最低必要版本為 1.16.303。

## 啟用 Detective 的建議

在啟用 Detective 之前，請考慮遵循這些建議

### 建議與 GuardDuty 和 對齊 AWS Security Hub CSPM

如果您已註冊 GuardDuty AWS Security Hub CSPM，我們建議您的帳戶是這些服務的管理員帳戶。如果這三項服務的管理員帳戶都相同，則以下整合點可順暢運作。

- 在 GuardDuty 或 Security Hub CSPM 中，檢視 GuardDuty 調查結果的詳細資訊時，您可以從調查結果詳細資訊轉向 Detective 調查結果設定檔。
- 在 Detective 中，調查 GuardDuty 調查結果時，您可以選擇封存該調查結果的選項。

如果您的 GuardDuty 和 Security Hub CSPM 有不同的管理員帳戶，我們建議您根據您更頻繁使用的服務來調整管理員帳戶。

- 如果您更頻繁地使用 GuardDuty，請使用 GuardDuty 管理員帳戶啟用 Detective。

如果您使用 AWS Organizations 管理帳戶，請將 GuardDuty 管理員帳戶指定為組織的 Detective 管理員帳戶。

- 如果您更頻繁地使用 Security Hub CSPM，請使用 Security Hub CSPM 管理員帳戶啟用 Detective。

如果您使用 Organizations 管理帳戶，請將 Security Hub CSPM 管理員帳戶指定為組織的 Detective 管理員帳戶。

如果您無法在所有服務中使用相同的管理員帳戶，則在啟用 Detective 之後，您可以選擇建立跨帳戶角色。此角色會授權管理員帳戶存取其他帳戶。

如需有關 IAM 如何支援此類角色的資訊，請參閱 [《IAM 使用者指南》中的提供存取權給您擁有的另一個 AWS 帳戶中的 IAM 使用者](#)。

### 建議更新 GuardDuty CloudWatch 的通知頻率

在 GuardDuty 中，偵測器會以 Amazon CloudWatch 通知頻率進行設定，以便報告後續發生的調查結果。這包括發送通知給 Detective。

根據預設，頻率為六小時。這意味著即使調查結果重複出現多次，直到六個小時後，新事件才會反映在 Detective 中。

為了減少 Detective 接收此類更新所需的時間，我們建議 GuardDuty 管理員帳戶將其偵測器上的設定變更為 15 分鐘。請注意，變更組態並不會影響使用 GuardDuty 的成本。

如需設定通知頻率的相關資訊，請參閱《Amazon GuardDuty 使用者指南》中的[使用 Amazon CloudWatch Events 監控 GuardDuty 調查結果](#)。

## 啟用 Detective

您可以從 Detective 主控台、Detective API 或 AWS Command Line Interface 啟用 Detective。

每個區域中只能啟用一次 Detective。如果您已經是區域中行為圖表的管理員帳戶，則無法再次在該區域中啟用 Detective。

### Console

若要啟用 Detective (主控台)

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 選擇開始使用。
3. 在啟用 Amazon Detective 頁面上，對齊管理員帳戶 (建議使用) 說明在 Detective 和 Amazon GuardDuty 和 AWS Security Hub CSPM 之間對齊管理員帳戶的建議。請參閱 [the section called “建議與 GuardDuty 和 對齊 AWS Security Hub CSPM”](#)。
4. 連接 IAM 政策按鈕會將您直接導向 IAM 主控台，並開啟建議的政策。您可以選擇將建議的政策連接至您用於 Detective 的主體。如果您沒有在 IAM 主控台中操作的許可，您可以在必要許可內複製 Amazon Resource Name (ARN)，將其提供給 IAM 管理員。他們可以代表您附加政策。

確認所需的 IAM 政策已就位。

5. 透過新增標籤區段，您可將標籤新增至行為圖表。

若要新增標籤，請執行以下操作：

- a. 選擇 Add new tag (新增標籤)。
- b. 針對金鑰，輸入標籤的名稱。
- c. 針對值，輸入標籤值。

若要移除標籤，選擇該標籤的移除選項。

6. 選擇啟用 Amazon Detective。
7. 啟用 Detective 後，您可以邀請成員帳戶加入您的行為圖表。

若要導覽至帳戶管理頁面，選擇立即新增成員。如需邀請成員帳戶的相關資訊，請參閱 [the section called “管理受邀成員帳戶”](#)。

## Detective API, AWS CLI

您可以透過 Detective API 或 AWS Command Line Interface 啟用 Amazon Detective。

### 啟用 Detective (Detective API AWS CLI)

- Detective API：使用 [CreateGraph](#) 操作。
- AWS CLI：在命令列中執行 [create-graph](#) 命令。

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

以下指令會啟用 Detective，並將 Department 標籤值設定為 Security。

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

## Python script on GitHub

您可以在 [GitHub.Detective](#) 在 GitHub 中提供開放原始碼指令碼，執行下列動作：

- 為指定的區域清單中的管理員帳戶啟用 Detective
- 將提供的成員帳戶清單新增至每個產生的行為圖表
- 向成員帳戶發送邀請電子郵件
- 自動接受成員帳戶的邀請

如需如何設定和使用 GitHub 指令碼的相關資訊，請參閱 [the section called “Amazon Detective Python 指令碼”](#)。

## 檢查 Detective 正在從 AWS 您的帳戶擷取資料

啟用 Detective 之後，它會開始從 AWS 您的帳戶擷取資料並擷取到您的行為圖表。

對於初始擷取，資料通常會在 2 小時內出現在行為圖表中。

檢查 Detective 是否擷取資料的一種方法是在 Detective 搜尋頁面上尋找範例值。

若要檢查搜尋頁面上的範例值

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在導覽窗格中，選擇搜尋。
3. 從選取類型功能表中，選擇項目類型。

資料中的範例包含行為圖表資料中已選取類型的識別符範例集。

如果您可以看到範例值，則您知道系統正在提取資料並擷取到您的行為圖表中。

# Detective 行為圖表中的資料

在 Amazon Detective 中，您使用 Detective 行為圖表中的資料進行調查。在本節中，您可以了解 Detective 行為圖表中使用的核心資料來源，以及 Detective 如何使用來源資料來填入該資料來源。

行為圖表是從一個或多個 Amazon Web Services (AWS) 帳戶擷取的 Detective 來源資料所產生的一組連結資料。

行為圖表使用來源資料來執行下列動作。

- 生成系統、使用者以及它們之間隨著時間交互的整體圖片
- 對特定活動進行更詳細的分析，以幫助您回答在進行調查時出現的問題
- 關聯可能與相同事件或安全問題相關的調查結果、實體和證據集合。

請注意，行為圖表資料的所有擷取、模型化和分析都會在每個個別行為圖表的內容中進行。

每個行為圖表都包含來自一個或多個帳戶的資料。當帳戶啟用 Detective 時，它會成為行為圖表的管理員帳戶，並為行為圖表選擇成員帳戶。行為圖表最多可以有 1,200 個成員帳戶。如需管理員帳戶如何管理行為圖表中成員帳戶的資訊，請參閱在 [Detective 中管理帳戶](#)。

## 目錄

- [Detective 如何填入行為圖表](#)
- [新 Detective 行為圖表的訓練期間](#)
- [行為圖表資料結構概觀](#)
- [Detective 行為圖表中使用的來源資料](#)

## Detective 如何填入行為圖表

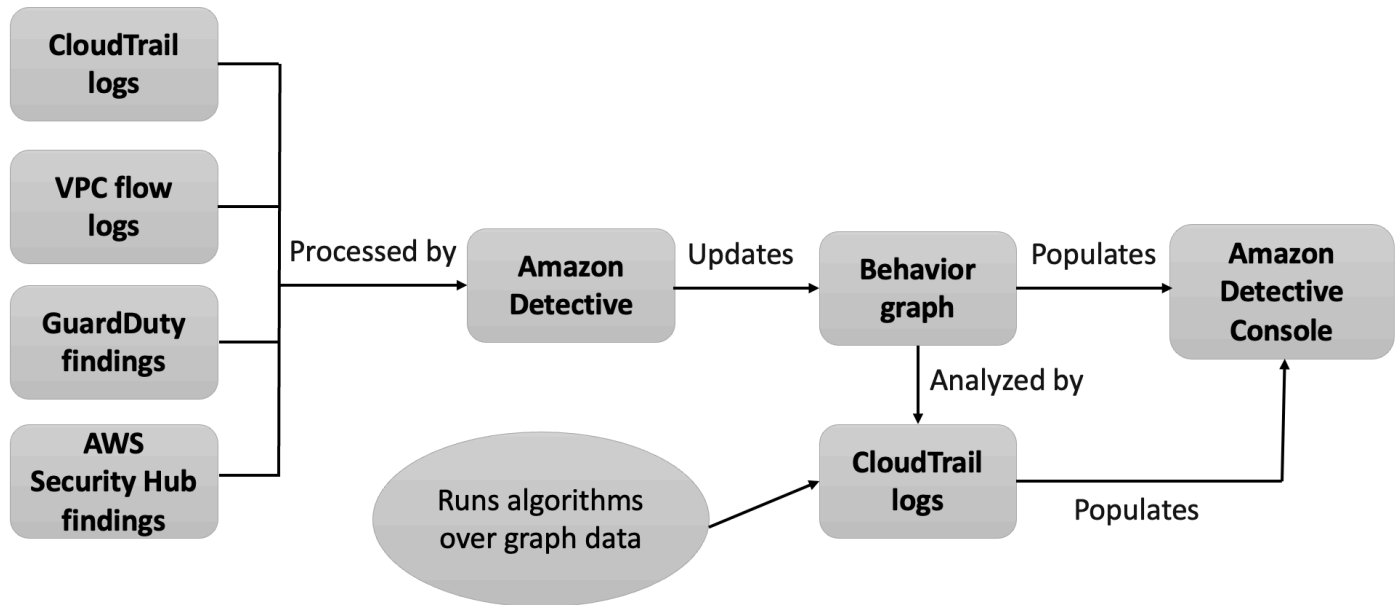
為了提供原始資料以供調查使用，Detective 將來自您 AWS 環境及其他環境的資料匯集在一起，包括以下內容：

- 日誌資料，包括 Amazon Virtual Private Cloud (Amazon VPC) 和 AWS CloudTrail
- 來自 Amazon GuardDuty 的調查結果
- 來自的問題清單 AWS Security Hub CSPM

若要進一步了解行為圖表中使用的來源資料，請參閱[行為圖表中使用的來源資料](#)。

## Detective 如何處理來源資料

當新資料傳入時，Detective 會組合使用擷取和分析來填入行為圖表。



## Detective 擷取

擷取以設定的映射規則為基礎。映射規則基本規定為：每當您看到此資料時，請以此特定方式進行使用，以更新行為圖表資料。

例如，傳入的 Detective 來源資料記錄可能包含 IP 地址。如果是，Detective 會使用該記錄中的資訊來建立新 IP 地址實體或更新現有的 IP 地址實體。

## Detective 分析

分析是較為複雜的演算法，可分析資料以深入了解與實體相關聯的活動。

例如，一種 Detective 分析類型會透過執行演算法來分析活動發生的頻率。針對進行 API 呼叫的實體，演算法會尋找實體通常不會使用的 API 呼叫。該算法還會查找 API 呼叫數目的較大峰值。

分析見解透過提供關鍵分析師問題的答案來支援調查，經常用於填入調查結果和實體設定檔面板。

## 新 Detective 行為圖表的訓練期間

調查結果的其中一個調查途徑是將調查結果範圍時間內的活動與偵測到調查結果之前所發生的活動進行比較。以前從未出現的活動可能更容易出現可疑情況。

部分 Amazon Detective 設定檔面板反白顯示了在調查結果之前時間段內未觀察到的活動。數個設定檔面板也會顯示基準值，以顯示範圍時間前 45 天內的平均活動。範圍時間是實體一段時間內的活動摘要。

隨著系統將越來越多的資料擷取到行為圖表中，Detective 會開發更準確的圖片，了解組織中哪些活動為正常以及異常活動。

但是，要建立此圖片，Detective 需要存取至少兩週的資料。Detective 分析的成熟度也隨著行為圖表中的帳戶數目而提升。

啟用 Detective 後的前兩週將作為訓練期間。在此期間，將範圍時間活動與先前活動進行比較的設定檔面板會顯示 Detective 正處於訓練期間的訊息。

在試用期間，Detective 建議您將盡可能多的成員帳戶新增至行為圖表。這為 Detective 提供了更大的資料集區，可讓它為您的組織產生更準確的正常活動圖片。

## 行為圖表資料結構概觀

行為圖表資料結構定義了擷取和分析資料的結構。它還定義了來源資料映射到行為圖表的方式。

### 行為圖表資料結構中元素的類型

行為圖表資料結構由以下資訊元素組成。

#### 實體

實體表示從 Detective 來源資料中擷取的項目。

每個實體都有一個類型，用來識別它所代表的物件類型。實體類型的範例包括 IP 地址、Amazon EC2 執行個體和 AWS 使用者。

針對每個實體，來源資料也會用來填入實體屬性。屬性值可以直接從來源記錄中擷取，也可以跨多個記錄彙總。

某些屬性由單一純量或彙總值組成。例如，針對 EC2 執行個體，Detective 會追蹤執行個體的類型和處理的位元組總數目。

時間序列屬性會追蹤一段時間內的活動。例如，針對 EC2 執行個體，Detective 會隨時間追蹤其使用的唯一連接埠。

#### 關係

關係表示個別實體之間發生的活動。關係也會從 Detective 來源資料中擷取。

與實體類似，關係具有類型，可識別涉及的實體類型和連接方向。關係類型的範例是連線至 EC2 執行個體的 IP 地址。

針對每個個別關係，例如連線至特定執行個體的特定 IP 地址，Detective 會追蹤一段時間內的發生次數。

## 行為圖表資料結構中的實體類型

行為圖表資料結構包含執行以下作業的實體和關係類型：

- 追蹤正在使用的伺服器、IP 地址和使用者代理程式
- 追蹤正在使用 AWS 的使用者、角色和帳戶
- 追蹤 AWS 環境中發生的網路連線和授權

行為圖表資料結構包含以下實體類型。

### AWS 帳戶

AWS Detective 來源資料中存在的 帳戶。

Detective 會針對每個帳戶回答以下數個問題：

- 帳戶使用了哪些 API 呼叫？
- 帳戶使用了哪些使用者代理程式？
- 帳戶使用了哪些自治系統組織 (ASO)？
- 帳戶在哪些地理位置處於作用中狀態？

### AWS 角色

AWS Detective 來源資料中存在的 角色。

Detective 會針對每個角色回答以下數個問題：

- 角色使用了哪些 API 呼叫？
- 角色使用了哪些使用者代理程式？
- 角色使用了哪些 ASO？
- 角色在哪些地理位置處於作用中狀態？
- 哪些資源擔任了該角色？
- 該角色擔任了哪些角色？

- 哪些角色工作階段涉及該角色？

## AWS 使用者

AWS Detective 來源資料中存在的 使用者。

Detective 會針對每個使用者回答以下數個問題：

- 使用者使用了哪些 API 呼叫？
- 使用者使用了哪些使用者代理程式？
- 使用者在哪些地理位置處於作用中狀態？
- 該使用者擔任了哪些角色？
- 哪些角色工作階段涉及該使用者？

## 聯合身分使用者

聯合身分使用者的執行個體。聯合身分使用者範例如下：

- 使用安全性聲明標記語言 (SAML) 登入的身分
- 使用 Web 聯合身分登入的身分

Detective 會針對每位聯合身分使用者回答以下問題：

- 聯合身分使用者使用哪些身分提供者進行驗證？
- 聯合身分使用者的受眾是什麼？受眾可識別要求聯合身分使用者的 Web 身分權杖的應用程式。
- 聯合身分使用者在哪些地理位置處於作用中狀態？
- 聯合身分使用者使用了哪些使用者代理程式？
- 聯合身分使用者使用了哪些 ASO？
- 該聯合身分使用者擔任了哪些角色？
- 哪些角色工作階段涉及該聯合身分使用者？

## EC2 執行個體

Detective 來源資料中存在的 EC2 執行個體。

Detective 會針對每個 EC2 執行個體回答以下數個問題：

- 已透過哪些 IP 地址與執行個體進行通訊？
- 已使用哪些連接埠與執行個體進行通訊？
- 已向執行個體或從執行個體傳送了多少資料量？
- 該執行個體包含在哪個 VPC 中？

- EC2 執行個體使用了哪些 API 呼叫？
- EC2 執行個體使用了哪些使用者代理程式？
- EC2 執行個體使用了哪些 ASO？
- EC2 執行個體在哪些地理位置處於作用中狀態？
- EC2 執行個體承擔了哪些角色？

## 角色工作階段

擔任角色資源的執行個體。每個角色工作階段都由角色識別符和工作階段名稱識別。

Detective 會針對每個角色回答以下數個問題：

- 此角色工作階段涉及哪些資源？換言之，擔任哪些角色，以及擔任角色的資源是什麼？

請注意，針對跨帳戶角色擔任，Detective 無法識別擔任該角色的資源。

- 角色工作階段使用了哪些 API 呼叫？
- 角色工作階段使用了哪些使用者代理程式？
- 角色工作階段使用了哪些 ASO？
- 角色工作階段在哪些地理位置處於作用中狀態？
- 哪個使用者或角色啟動了該角色工作階段？
- 從該角色工作階段啟動了哪些角色工作階段？

## 問題清單

將輸入至 Detective 來源資料中的調查結果 (由 Amazon GuardDuty 發現)。

針對每個調查結果，Detective 都會追蹤調查結果類型、來源和調查結果活動的時間範圍。

它也會儲存調查結果特定的資訊，例如偵測活動中涉及的角色或 IP 地址。

## IP 位址

Detective 來源資料中存在的 IP 地址。

Detective 會針對每個 IP 地址回答以下數個問題：

- 地址使用了哪些 API 呼叫？
- 地址使用了哪些連接埠？
- 哪些使用者和使用者代理程式使用了 IP 地址？
- IP 地址在哪些地理位置處於作用中狀態？
- 哪些 EC2 執行個體已指派該 IP 地址並與之通訊？

## S3 bucket (S3 儲存貯體)

Detective 來源資料中的 S3 儲存貯體。

Detective 會針對每個 S3 儲存貯體回答以下問題：

- 哪些主體與 S3 儲存貯體進行互動？
- 對 S3 儲存貯體進行了哪些 API 呼叫？
- 主體從哪些地理位置對 S3 儲存貯體進行 API 呼叫？
- 使用了哪些使用者代理程式與 S3 儲存貯體進行互動？
- 使用了哪些 ASO 與 S3 儲存貯體進行互動？

您可以刪除 S3 儲存貯體，然後建立具有相同名稱的新儲存貯體。由於 Detective 使用 S3 儲存貯體名稱來識別 S3 儲存貯體，因此會將它們視為單一 S3 儲存貯體實體。在實體設定檔上，建立時間指首次的建立時間。刪除時間指最近的刪除時間。

若要檢視所有建立和刪除事件，請將範圍時間設定為從建立時間開始，並以刪除時間結束。在整體 API 呼叫量設定檔面板上，顯示範圍時間的活動詳細資訊。篩選要顯示 Create 和 Delete 方法的 API 方法。請參閱 [the section called “整體 API 呼叫量”](#)。

## 使用者代理程式

Detective 來源資料中存在的使用者代理程式。

Detective 會針對每個使用者代理程式回答以下問題：

- 使用者代理程式使用了哪些 API 呼叫？
- 哪些使用者和角色使用了使用者代理程式？
- 哪些 IP 地址使用了使用者代理程式？

## EKS 叢集

Detective 來源資料中存在的 EKS 叢集。

### Note

若要查看此實體類型的完整詳細資訊，必須啟用選用的 EKS 稽核日誌資料來源。如需詳細資訊，請參閱[選用的資料來源](#)

Detective 會針對每個 EKS 叢集回答以下問題：

- 已在此叢集中執行了哪些 Kubernetes API 呼叫？

- 哪些 Kubernetes 使用者和服務帳戶 (主體) 在此叢集中處於作用中狀態？
- 在此叢集中啟動了哪些容器？
- 在此叢集中使用哪些映像來啟動容器？

## Kubernetes Pod

Detective 來源資料中存在的 Kubernetes Pod。

### Note

若要查看此實體類型的完整詳細資訊，必須啟用選用的 EKS 稽核日誌資料來源。如需詳細資訊，請參閱[選用的資料來源](#)

Detective 會針對每個 Pod 回答以下問題：

- 在我的帳戶中，有哪些常見的 Pod 內容器映像？
- 已針對此 Pod 進行了哪些活動？
- 在此 Pod 中執行了哪些容器？
- 該 Pod 中容器的登錄檔在我的帳戶中常見嗎？
- 工作負載的其他 Pod 中是否還有哪些其他正在執行的容器？
- 此裝置中是否存在任何不在工作負載其他 Pod 中的異常容器？

## 容器映像

Detective 來源資料中存在的容器映像。

### Note

若要查看此實體類型的完整詳細資訊，必須啟用選用的 EKS 稽核日誌資料來源。如需詳細資訊，請參閱[選用的資料來源](#)

Detective 會針對每個容器映像回答以下問題：

- 我的環境中還有哪些其他映像與此映像共享相同的儲存庫或登錄檔？
- 我的環境中正在執行多少個映像副本？

## Kubernetes 主體

Detective 來源資料中存在的 Kubernetes 主體。Kubernetes 主體指使用者或服務帳戶。

**Note**

若要查看此實體類型的完整詳細資訊，必須啟用選用的 EKS 稽核日誌資料來源。如需詳細資訊，請參閱[選用的資料來源](#)

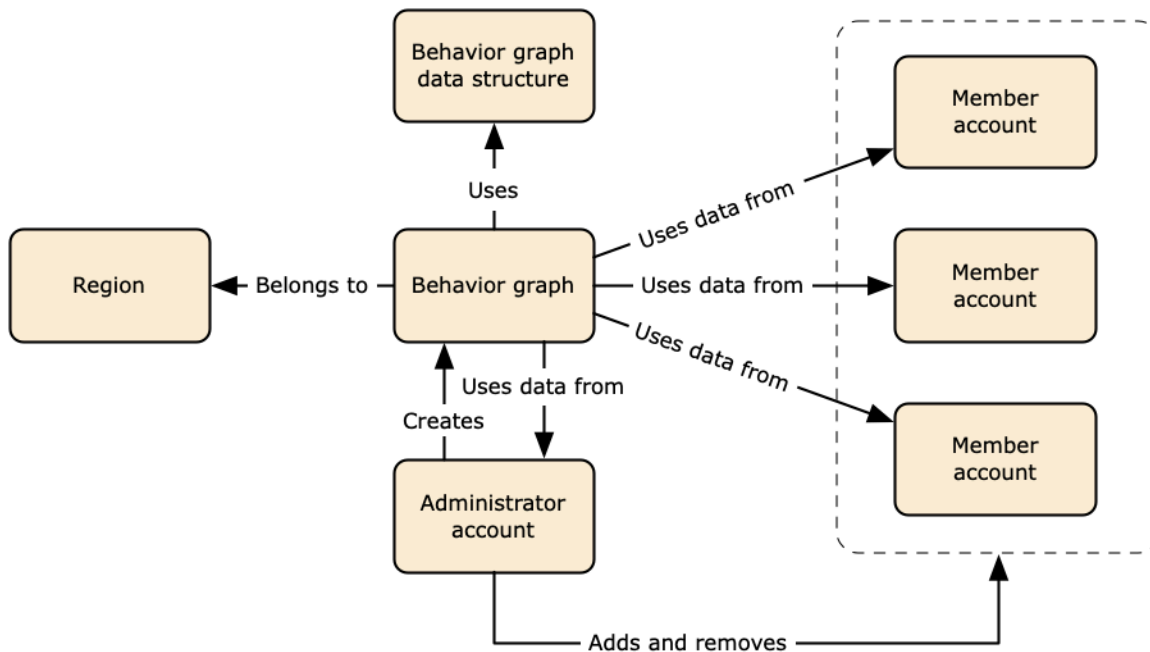
Detective 會針對每個主體回答以下問題：

- 哪些 IAM 主體已經驗證為該主體？
- 哪些調查結果與該主體相關聯？
- 主體使用哪些 IP 地址？

## Detective 行為圖表中使用的來源資料

為了填入行為圖表，Amazon Detective 會使用行為圖表管理員帳戶和成員帳戶中的來源資料。

使用 Detective，您可以訪問長達一年的歷史事件資料。此資料可透過一組視覺化取得，視覺化可顯示已選取時間範圍內活動類型和數目的變化。Detective 將此類變更連結至 GuardDuty 調查結果。



如需行為圖表資料結構的相關資訊，請參閱《Detective 使用者指南》中的[行為圖表資料結構概觀](#)。

## Detective 中核心資料來源的類型

Detective 從這些類型的 AWS 日誌擷取資料：

- AWS CloudTrail 日誌
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
  - 同時擷取 IPv4 和 IPv6 記錄，但不擷取 Elastic Fabric Adapters 產生的 MAC 記錄。
  - 當 log-status 欄位的值處於 OK 狀態時擷取日誌記錄。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[流程日誌記錄](#)。
  - 僅擷取在這些 VPCs 中執行的 Amazon Elastic Compute Cloud 執行個體所產生的流程日誌。不會使用其他資源，例如 NAT 閘道、RDS 執行個體或 Fargate 叢集。
  - 同時擷取已接受和已拒絕的流量。
- 針對已註冊加入 GuardDuty 的帳戶，Detective 也會擷取 GuardDuty 的調查結果。

Detective 會使用獨立且重複的 CloudTrail 和 VPC 流程日誌來使用 CloudTrail 和 VPC 流程日誌事件。此類程序不會影響或使用現有 CloudTrail 和 VPC 流程日誌設定。它們也不會影響此類服務的效能或增加成本。

## Detective 中選用的資料來源的類型

Detective 除了 Detective 核心套件提供的三個資料來源之外，還提供選用的來源套件（核心套件包含 AWS CloudTrail 日誌、VPC 流程日誌和 GuardDuty 調查結果）。您可以隨時為行為圖表啟動或停止選用的資料來源套件。

Detective 為每個區域的所有核心和選用的來源套件提供 30 天免費試用。

### Note

Detective 會將從每個資料來源套件收到的所有資料保留最多 1 年。

目前有以下選用的來源套件可供使用：

- EKS 稽核日誌

透過該選用資料來源套件，Detective 可擷取環境中 EKS 叢集的詳細資訊，並將該資料新增至您的行為圖表。Detective 會將使用者活動與 AWS CloudTrail Management 事件和網路活動與 Amazon VPC Flow Logs 建立關聯，而不需要您手動啟用或停用這些日誌。如需詳細資訊，請參閱 [Amazon EKS 稽核日誌](#)。

- AWS 安全調查結果

此選用的資料來源套件可讓 Detective 從 Security Hub CSPM 擷取資料，並將該資料新增至您的行為圖表。如需詳細資訊，請參閱 [AWS 安全調查結果](#)。

啟動或停止選用的資料來源：

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，於設定下選擇一般。
3. 在選用的來源套件下，選取更新。然後選取要啟用的資料來源，或取消選取已啟用資料來源的方塊，然後選擇更新以變更啟用的資料來源套件。

#### Note

如果您停止然後重新啟動選用的資料來源，您將在某些實體設定檔上顯示的資料中發現間隙。此間隙將在主控台顯示中註明，代表資料來源停止的時間段。當資料來源重新啟動時，Detective 不會追溯擷取資料。

## Amazon EKS 稽核日誌

Amazon EKS 稽核日誌是選用的資料來源套件，可新增至您的 Detective 行為圖表。您可以從主控台的設定頁面或透過 Detective API，查看您帳戶中可用的選用來源套件及其狀態。

系統為此資料來源提供 30 天的免費試用。如需進一步了解，請參閱 [選用的資料來源的免費試用](#)。

透過啟用 Amazon EKS 稽核日誌，Detective 可以使用 Amazon EKS 所建立資源的深入資訊新增至您的行為圖表。此資料來源將提升所提供的有關以下實體類型的資訊：EKS 叢集、Kubernetes Pod、容器映像和 Kubernetes 主體。

此外，如果您已在 Amazon GuardDuty 中啟用 EKS 稽核日誌作為資料來源，您將能夠從 GuardDuty 查看有關 Kubernetes 調查結果的詳細資訊。如需在 GuardDuty 中啟用此資料來源的詳細資訊，請參閱 [Amazon GuardDuty 中的 Kubernetes 保護](#)。

#### Note

此資料來源預設會針對 2022 年 7 月 26 日之後建立的新行為圖表啟用。針對 2022 年 7 月 26 日之前建立的行為圖表，必須手動啟用。

新增或移除 Amazon EKS 稽核日誌作為選用資料來源：

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，於設定下選擇一般。
3. 在來源套件下，選取 EKS 稽核日誌以啟用此資料來源。如果已啟用，請再次選取，即可停止將 EKS 稽核日誌擷取到您的行為圖表中。

## AWS 安全調查結果

AWS 安全性問題清單是選用的資料來源套件，可新增至 Detective 行為圖表。

您可以從主控台的設定頁面或透過 Detective API，查看您帳戶中可用的選用來源套件及其狀態。

系統為此資料來源提供 30 天的免費試用。如需進一步了解，請參閱 [選用的資料來源的免費試用](#)。

啟用 AWS 安全調查結果可讓 Detective 以稱為 AWS Security Format (ASFF) 的標準調查結果格式，使用由 Security Hub 從上游服務彙總的 Security Hub CSPM 調查結果，而不需要耗費時間的資料轉換工作。然後，相互關聯所有產品的問題清單，排定最重要幾個的優先順序。

新增或移除做為選用資料來源 AWS 的安全性問題清單：

### Note

AWS 安全調查結果資料來源預設為針對 2023 年 5 月 16 日之後建立的新行為圖表啟用。針對 2023 年 5 月 16 日之前建立的行為圖表，必須手動啟用。

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，於設定下選擇一般。
3. 在來源套件下，選取 AWS 安全性問題清單以啟用此資料來源。如果已啟用，請再次選取，以停止將 AWS 安全調查結果格式 (ASFF) 的調查結果擷取到您的行為圖表中。

## 目前支援的調查結果

Detective 從 Amazon 或擁有的服務擷取 Security Hub CSPM 中的所有 ASFF 調查結果 AWS。

- 若要查看支援的服務整合清單，請參閱 AWS Security Hub 《使用者指南》中的 [可用 AWS 服務整合](#)。

- 如需支援資源的清單，請參閱《AWS Security Hub 使用者指南》中的[資源](#)。
- AWS 具有合規狀態的服務調查結果未設定為 FAILED，且不會擷取跨區域彙總調查結果。

## Detective 如何擷取和儲存來源資料

啟用 Detective 後，Detective 會開始從行為圖表管理員帳戶擷取來源資料。當成員帳戶新增至行為圖表時，Detective 也會開始使用此類成員帳戶中的資料。

Detective 來源資料包含原始摘要的結構化和處理版本。為了支援 Detective 分析，Detective 會儲存 Detective 來源資料的副本。

Detective 擷取程序會將資料饋送至 Detective 來源資料存放區中的 Amazon Simple Storage Service (Amazon S3) 儲存貯體中。當新來源資料到達時，其他 Detective 元件會接收資料，並開始擷取和分析程序。如需詳細資訊，請參閱《Detective 使用者指南》中的[Detective 如何使用來源資料填入行為圖表](#)。

## Detective 如何強制執行行為圖表的資料量配額

Detective 在每個行為圖表中允許的資料量都有嚴格的配額。資料量指每天流入 Detective 行為圖表的資料量。

當管理員帳戶啟用 Detective，以及成員帳戶接受邀請以提供行為圖表時，Detective 會強制執行此類配額。

- 如果管理員帳戶的資料量每天超過 10 TB，則管理員帳戶無法啟用 Detective。
- 如果從成員帳戶新增的資料量會導致行為圖表每天超過 10 TB，則無法啟用該成員帳戶。

行為圖表的資料量也會隨著時間的推移自然增加。Detective 會每天檢查行為圖表資料量，以確保它不會超過配額。

如果行為圖表資料量接近配額，Detective 會在主控台上顯示警告訊息。為避免超出配額，您可以移除成員帳戶。

如果行為圖表資料量每天超過 10 TB，則您無法將新成員帳戶新增至行為圖表。

如果行為圖表資料量每天超過 15 TB，則 Detective 就會停止將資料擷取至行為圖表中。每天 15 TB 的配額反映正常資料量和資料量峰值。達到此配額時，系統不會在行為圖表中擷取任何新資料，但不會移除現有資料。您仍然可以使用該歷史資料進行調查。主控台會顯示訊息，指出行為圖表的資料擷取已暫停。

如果資料擷取已暫停，您必須使用 支援 重新啟用。如果可能，請在聯絡之前 支援嘗試移除成員帳戶，以取得低於配額的資料量。此舉可以簡化重新啟用行為圖表的資料擷取程序。

# 使用 Detective 摘要儀表板

使用 Amazon Detective 中的摘要儀表板來識別實體，以調查過去 24 小時內的活動來源。Amazon Detective 摘要儀表板可協助您識別與特定異常活動類型相關聯的實體。這是進行調查的數個可能起點之一。

若要顯示摘要儀表板，請在 Detective 導覽窗格中，選擇摘要。當您第一次開啟 Detective 主控台時，預設也會顯示摘要儀表板。

從摘要儀表板中，您可以識別符合下列條件的實體：

- 顯示 Detective 發現的潛在安全事件的調查
- 在新觀察到的地理位置中發生活動所涉及的實體
- 進行最多 API 呼叫次數的實體
- 流量最大的 EC2 執行個體
- 容器數量最多的容器叢集

從每個摘要儀表板面板中，您可以樞紐到所選實體的設定檔。

當您檢閱摘要儀表板時，您可以調整範圍時間，以檢視過去 365 天內任何 24 小時時間範圍的活動。當您變更開始日期和時間時，結束日期和時間會自動更新為您選擇的開始時間之後的 24 小時。

使用 Detective，您可以訪問長達一年的歷史事件資料。此資料可透過一組視覺化取得，視覺化可顯示已選取時間範圍內活動類型和數目的變化。Detective 將此類變更連結至 GuardDuty 調查結果。

如需 Detective 中來源資料的詳細資訊，請參閱[行為圖表中使用的來源資料](#)。

## 调查

調查顯示 Detective 確定的潛在安全事件。在調查面板上，您可以檢視嚴重調查，以及在一段時間內受到安全事件影響的對應 AWS 角色和使用者。調查會將入侵指標分組在一起，以協助判斷 AWS 資源是否涉及可能表示惡意行為及其影響的異常活動。

選取檢視所有調查以檢閱調查結果、分類調查結果群組和資源詳細資訊，以加速您的安全調查。系統會根據選取的範圍時間顯示調查。您可以調整範圍時間，以檢視在過去 365 天 24 小時中的調查。您可以直接錨定至關鍵調查，以查看詳細的調查報告。

如果您識別似乎有可疑活動 AWS 的角色或使用者，您可以直接從調查面板轉向該角色或使用者，以繼續您的調查。轉移至角色或使用者，然後按一下執行調查以產生調查報告。對角色或使用者執行調查後，該角色或使用者會移至已調查標籤。

## 新觀察到的地理位置

新觀察到的地理位置反白顯示了前 24 小時內活動來源的地理位置，但在此之前的基準時間段內未發現該地理位置。

該面板最多包含 100 個地理位置。位置會標示在地圖上，並列在地圖下方的資料表中。

針對每個地理位置，資料表會顯示過去 24 小時內從該地理位置發出的失敗和成功 API 呼叫次數。

您可以展開每個地理位置，以顯示從該地理位置進行 API 呼叫的使用者和角色清單。資料表會針對每個主體列出類型及相關聯的 AWS 帳戶。

如果您識別似乎有可疑的使用者或角色，則可以直接從面板錨定至使用者或角色設定檔，以繼續調查。若要錨定至設定檔，請選擇使用者或角色識別符。

Detective 會使用 MaxMind GeoIP 資料庫來決定請求的位置。MaxMind 在國家/地區層級報告非常高的資料準確性，但準確性會根據國家/地區和 IP 類型等因素而有所不同。如需 MaxMind 的詳細資訊，請參閱 [MaxMind IP 地理位置](#)。如果您認為任何 GeoIP 資料不正確，您可以在 [MaxMind Correct GeoIP2 Data](#) 向 Maxmind 提交更正請求。

## 過去 7 天內作用中的調查結果群組

過去 7 天內作用中的調查結果群組會顯示您環境中發生在設定時間內的 Detective 調查結果、實體和證據的關聯分組。這些分組關聯可能表示惡意行為的異常活動。摘要儀表板會顯示最多五個群組，依群組排序，其中包含上週作用中的最關鍵問題清單。

您可以在政策、帳戶、資源和調查結果內容中選取值，以查看更多詳細資訊。

每天會產生調查結果群組。如果您識別出感興趣的調查結果群組，您可以選取要移至群組設定檔詳細檢視的標題，以繼續調查。

## 具有最大 API 呼叫量的角色和使用者

具有最大 API 呼叫量的角色和使用者可識別過去 24 小時內進行最多 API 呼叫的使用者和角色。

該面板可以包含高達 100 個使用者和角色。您可以查看每個使用者或角色的類型 (使用者或角色) 和相關聯的帳戶。您也可以查看該使用者或角色在過去 24 小時內發出的 API 呼叫次數。

根據預設，系統會顯示服務連結角色。服務連結角色可以產生大量 AWS CloudTrail 活動，這會取代您想要進一步調查的委託人。您可以選擇關閉顯示服務連結角色，從摘要儀表板檢視篩選掉服務連結角色。

您可以匯出逗號分隔值 (.csv) 檔案，其中包含此面板中的資料。

還有一個過去 7 天的 API 呼叫量的時間軸。時間軸可協助您判斷該主體的 API 呼叫量是否存在異常。

如果您在 API 呼叫量方面識別似乎有可疑的使用者或角色，則可以直接從面板錨定至使用者或角色設定檔，以繼續調查。您也可以檢視與使用者或角色相關聯的帳戶設定檔。若要檢視設定檔，請選擇使用者、角色或帳戶識別符。

## 具有最大流量的 EC2 執行個體

具有最大流量的 EC2 執行個體可識別過去 24 小時內總流量最大的 EC2 執行個體。

該面板可以包含高達 100 個 EC2 執行個體。針對每個 EC2 執行個體，您可以查看關聯的帳戶以及前 24 小時內傳入位元組、傳出位元組和總位元組數。

您可以匯出包含此面板中資料的逗號分隔值 (.csv) 設定檔。

您還可以看到顯示過去 7 天內傳入和傳出流量的時間軸。時間軸可協助判斷該 EC2 執行個體的流量是否存在異常。

如果您識別有可疑流量的 EC2 執行個體，則可以直接從面板前往 EC2 執行個體設定檔繼續調查。您也可以檢視擁有 EC2 執行個體的帳戶設定檔。若要檢視設定檔，請選擇 EC2 執行個體或帳戶識別符。

## 具有最多 Kubernetes Pod 的容器叢集

所建立具有最多 Kubernetes Pod 的容器叢集可識別在過去 24 小時內執行最多容器的叢集。

此面板包含最多 100 個叢集組織的叢集，此類叢集與叢集相關聯的調查結果最多。針對每個叢集，您可以看到相關聯的帳戶、該叢集中目前的容器數目以及過去 24 小時內與該叢集相關聯的調查結果數目。您可以匯出包含此面板中資料的逗號分隔值 (.csv) 設定檔。

如果您識別有近期調查結果的叢集，您可以直接從面板錨定至叢集設定檔，以繼續進行調查。您也可以錨定至擁有叢集之帳戶的設定檔。若要錨定至設定檔，請選擇叢集名稱或帳戶識別符。

## 近似值通知

在具有最大 API 呼叫量的角色和使用者和具有最大流量的 EC2 執行個體上，如果值後面加上星號 (\*)，則表示該值為近似值。真值可能等於或大於顯示值。

這是因為 Detective 用來計算每個時間間隔的體積的方法所致。在摘要頁面上，時間間隔為一小時。

Detective 會每小時計算具有最大流量的 1,000 個使用者、角色或 EC2 執行個體的總量。它會排除剩餘使用者、角色或 EC2 執行個體的資料。

如果某一資源有時位於前 1,000 名，則該資源的計算量可能不會包含所有資料。排除非前 1,000 名的時間間隔的資料。

請注意，這僅適用於摘要頁面。使用者、角色或 EC2 執行個體的設定檔提供精確的詳細資訊。

# Detective 如何用於調查

Amazon Detective 會簡化分析、調查並快速識別安全調查結果或可疑活動的根本原因。Detective 提供支援整體調查程序的工具。Detective 中的調查能夠以調查結果、調查結果群組或實體作為起點。

## Detective 中的調查階段

任何 Detective 調查程序都涉及下列階段：

### 分類

當您收到有關可疑惡意或高風險活動執行個體的通知時，調查程序便會啟動。例如，您會被分配到查看透過 Amazon GuardDuty 和 Amazon Inspector 等服務所發現的調查結果或警報。

在分類階段，您可以判斷您是否認為該活動是真陽性 (真正的惡意活動) 還是偽陽性 (非惡意或高風險活動)。Detective 設定檔透過為涉及的實體提供活動的見解來支援分類程序。

針對真陽性執行個體，您將繼續下一個階段。

### 範圍設定

在範圍設定階段，分析師會判斷惡意或高風險活動的程度以及根本原因。

範圍設定可回答以下類型的問題：

- 哪些系統和使用者遭到入侵？
- 攻擊起源於何處？
- 攻擊的持續時間？
- 是否還存在其他待發現的相關活動？例如，如果攻擊者從您的系統中擷取資料，他們會如何取得？

Detective 視覺化可協助您識別所涉或受影響的其他實體。

### 回應

最後一步是對攻擊做出回應，以阻止攻擊，最大程度地減少傷害，並防止類似的攻擊再次發生。

## Detective 調查的起點

每次 Detective 調查都有重要的起點。例如，您可能會獲指派要調查的 Amazon GuardDuty 或 AWS Security Hub CSPM 調查結果。或者，您可能會擔心特定 IP 地址的異常活動。

調查的常用起點包括 GuardDuty 偵測到的調查結果，以及從 Detective 來源資料擷取的實體。

## GuardDuty 偵測到的調查結果

GuardDuty 使用您的日誌資料來發現惡意或高風險活動的可疑執行個體。Detective 會提供資源以幫助您調查此類調查結果。

Detective 會針對各調查結果提供相關的調查結果詳細資訊。Detective 也會顯示連線至調查結果的實體，例如 IP 地址和 AWS 帳戶。

然後，您可以探索涉及的實體的活動，以確定從調查結果中偵測到的活動是否為真正引起關注的原因。

如需詳細資訊，請參閱[the section called “調查結果概觀”](#)。

## AWS Security Hub CSPM 彙總的安全性調查結果

AWS Security Hub CSPM 會在單一位置彙總來自各種問題清單提供者的安全性問題清單，並為您提供安全狀態的完整檢視 AWS。Security Hub CSPM 消除了處理來自多個供應商的大量調查結果的複雜性。它減少了管理和改善所有 AWS 帳戶、資源和工作負載安全性所需的工作量。Detective 會提供資源以幫助您調查此類調查結果。

Detective 會針對各調查結果提供相關的調查結果詳細資訊。Detective 也會顯示連線至調查結果的實體，例如 IP 地址和 AWS 帳戶。

如需詳細資訊，請參閱[the section called “調查結果概觀”](#)。

## 從 Detective 來源資料擷取的實體

Detective 會從擷取的 Detective 來源資料擷取實體，例如 IP 地址和 AWS 使用者。您可以使用其中一個作為調查起點。

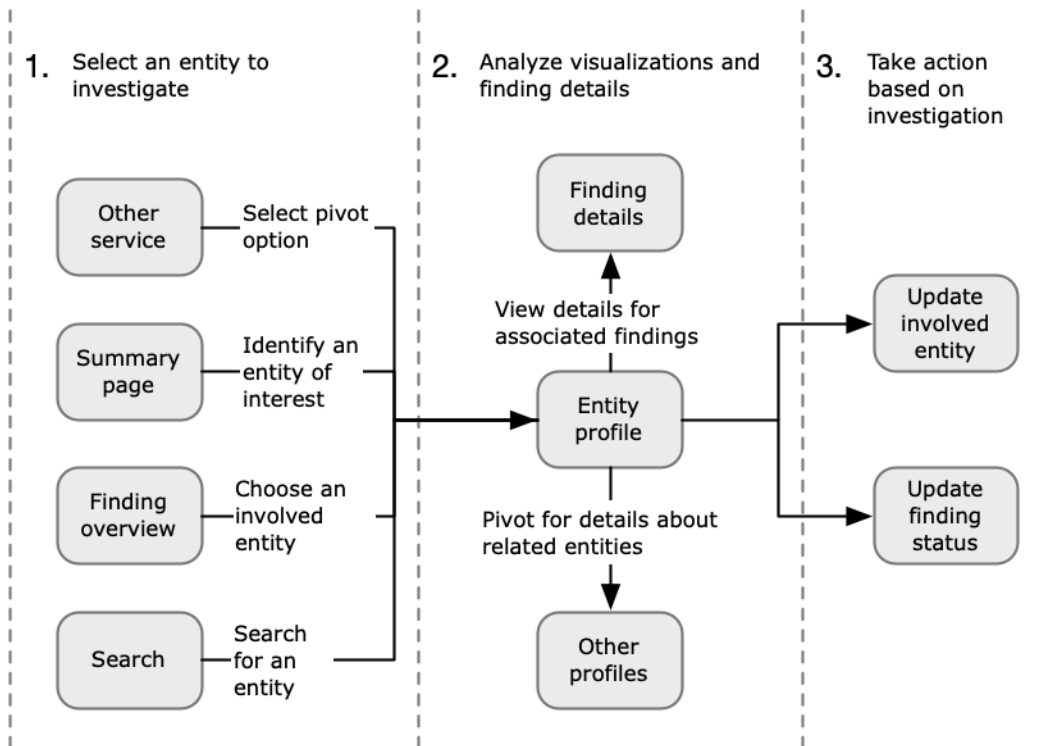
Detective 提供有關實體的一般詳細資訊，例如 IP 地址或使用者名稱。它還提供活動歷史記錄的詳細資訊。例如，Detective 可以報告實體已連線、曾連線或使用的其他 IP 地址。

如需詳細資訊，請參閱[分析實體](#)。

## Detective 調查流程

您可以使用 Amazon Detective 調查實體，例如 EC2 執行個體或 AWS 使用者。您也可以調查安全調查結果。

在高階，下圖顯示 Detective 調查的程序。



### 步驟 1：選取要調查的實體

在查看 GuardDuty 中的調查結果時，分析師可以選擇在 Detective 中調查相關實體。請參閱 [the section called “從其他主控台錨定”](#)。

選取實體後，系統將帶您前往 Detective 中的實體設定檔。

### 步驟 2：分析設定檔的視覺化

每個實體設定檔都包含一組從行為圖表產生的視覺化。行為圖表根據輸入至 Detective 的日誌檔案和其他資料建立。

視覺化會顯示與實體相關的活動。您可以使用此類視覺化來回答問題，以判斷實體活動是否存在異常。請參閱 [分析實體](#)。

為了幫助指導調查，您可以使用為每個視覺化提供的 Detective 指南。該指南概述了顯示的資訊，建議您要提出的問題，並根據答案提出後續步驟。請參閱 [the section called “使用設定檔面板指引”](#)。

每個設定檔都包含相關聯調查結果的清單。您可以檢視調查結果的詳細資訊，以及檢視調查結果概觀。請參閱 [the section called “檢視實體的調查結果”](#)。

從實體設定檔中，您可以錨定至其他實體和調查結果設定檔，以進一步調查相關資產的活動。

## 步驟 3：採取動作

根據調查的結果，採取適當動作。

若調查結果為假陽性，則可將該調查結果封存。在 Detective 中，您可以存檔 GuardDuty 的調查結果。如需詳細資訊，請參閱[封存 Amazon GuardDuty 調查結果](#)。

否則，您應採取適當動作來解決漏洞並減輕損害。例如，您可能需要更新資源的配置。

## Detective 調查

您可以使用 Amazon Detective Investigation，使用入侵指標調查 IAM 使用者和 IAM 角色，這可協助您判斷資源是否涉及安全事件。入侵指標 (IOC) 指在網路、系統或環境中或在網路、系統或環境上觀察到的成品，可以 (具有高可信度) 識別惡意活動或安全事件。透過 Detective Investigations，您可以最大化效率、專注於安全威脅，並強化事件回應功能。

Detective Investigation 使用機器學習模型和威脅情報自動分析 AWS 環境中的資源，以識別潛在的安全事件。透過該調查，您可主動有效且高效地使用以 Detective 行為圖表為基礎的自動化功能來改善安全操作。使用 Detective Investigation，您可以調查攻擊策略、不可能的旅程、標記的 IP 地址和調查結果群組。它會執行初步的安全調查步驟，並產生一份報告，反白顯示 Detective 所識別的風險，協助您瞭解安全事件並回應潛在事件。

### 主題

- [執行 Detective 調查](#)
- [檢閱 Detective Investigations 報告](#)
- [了解 Detective Investigations 報告](#)
- [Detective Investigations 報告摘要](#)
- [下載 Detective Investigations 報告](#)
- [封存 Detective Investigations 報告](#)

## 執行 Detective 調查

使用執行調查來分析 IAM 使用者和 IAM 角色等資源，並產生調查報告。產生的報告詳細說明指出潛在入侵的異常行為。

### Console

請依照下列步驟，使用 Amazon Detective 主控台從調查頁面執行 Detective 調查。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。
3. 在調查頁面中，選擇右上角的執行調查。
4. 在選取資源區段中，您有三種方式可執行調查。您可以選擇對 Detective 建議的資源執行調查。您可以針對特定資源執行調查。您也可以從 Detective 搜尋頁面調查資源。

1. Choose a recommended resource – Detective 會根據其在問題清單和問題清單群組中的活動來建議資源。若要對 Detective 建議的資源執行調查，請在建議資源資料表中選取要調查的資源。

建議的資源表提供了下列詳細資訊：

- 資源 ARN – AWS 資源的 Amazon Resource Name (ARN)。
  - 調查原因：顯示調查資源的主要原因。Detective 建議調查資源的原因如下：
    - 如果資源在過去 24 小時內涉及「高嚴重性」調查結果。
    - 如果資源在過去 7 天內涉及所觀察的調查結果群組。Detective 調查結果群組可讓您檢查與潛在安全事件相關的多項活動。如需詳細資訊，請參閱 [the section called “尋找群組”](#)。
    - 如果資源在過去 7 天內涉及調查結果。
  - 最新調查結果：最新調查結果為最高優先順序，會列在清單頂端。
  - 資源類型：識別資源的類型。例如，AWS 使用者或 AWS 角色。
2. Specify an AWS role or user with an ARN – 您可以選取 AWS 角色或 AWS 使用者，並針對特定資源執行調查。

請依照下列步驟調查特定資源類型。

- a. 從選取資源類型下拉式清單中，選擇 AWS 角色或 AWS 使用者。
  - b. 輸入 IAM 資源的資源 ARN。如需資源 ARNs 的詳細資訊，請參閱《IAM 使用者指南》中的 [Amazon Resource Name \(ARNs\)](#)。
3. Find a resource to investigate from the Search page – 您可以從 Detective 搜尋頁面搜尋所有 IAM 資源。

請依照下列步驟，從搜尋頁面調查資源。

- a. 在導覽窗格中，選擇搜尋。
- b. 在搜尋頁面中，搜尋 IAM 資源。

- c. 導覽至資源的設定檔頁面，然後從該處執行調查。
5. 在調查範圍時間區段中，選擇調查的範圍時間，以評估所選資源的活動。您可以選取開始日期和開始時間，以及結束日期和結束時間 (UTC 格式)。已選取範圍時間範圍最少可介於 3 小時至最多 30 天之間。
6. 選擇執行調查。

## API

若要以程式設計方式執行調查，請使用 Detective API 的 [StartInvestigation](#) 操作。若要使用 AWS Command Line Interface (AWS CLI) 執行調查，請執行 [start-investigation](#) 命令。

在您的請求中，使用這些參數在 Detective 中執行調查：

- **GraphArn**：指定行為圖形的 Amazon Resource Name (ARN)。
- **EntityArn**：指定 IAM 使用者和 IAM 角色的唯一 Amazon Resource Name (ARN)。
- **ScopeStartTime**：(選用) 指定應開始調查的資料和時間。此值為 UTC ISO8601 格式的字串。例如， 2021-08-18T16:35:56.284Z。
- **ScopeEndTime**：(選用) 指定應結束調查的資料和時間。此值為 UTC ISO8601 格式的字串。例如， 2021-08-18T16:35:56.284Z。

此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
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
```

您也可以從 Detective 的下列頁面執行調查：

- Detective 中的 IAM 使用者或 IAM 角色設定檔頁面。
- 調查結果群組的圖形視覺化窗格。
- 所涉及資源的動作欄。
- 調查結果頁面上的 IAM 使用者或 IAM 角色。

Detective 執行資源的調查之後，就會產生調查報告。若要存取報告，請從導覽窗格前往調查。

## 檢閱 Detective Investigations 報告

透過調查報告，您可針對先前在 Detective 中執行的調查，檢閱產生的報告。

若要檢閱調查報告

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。

注意調查報告中的以下屬性。

- ID：產生的調查報告識別符。您可以選擇此 ID 來讀取調查報告的摘要，其中包含調查的詳細資訊。
- 狀態：每項調查都會根據調查的完成狀態與狀態相關聯。狀態值可以為進行中、成功或失敗。
- 嚴重性：每項調查都會指派嚴重性。Detective 會自動指派調查結果的嚴重性。

嚴重性代表在指定範圍時間內對單一資源的調查所分析的處理方式。調查報告的嚴重性並不暗示或以其他方式表示受影響資源對您的組織可能具有的嚴重性或重要性。

調查嚴重性數值為嚴重、高、中、低或資訊 (嚴重性從高到低排序)。

指派為嚴重或高嚴重性值的調查應優先進行進一步檢查，因為此類調查更有可能代表 Detective 所發現的高影響安全問題。

- 實體：實體欄位包含調查中偵測到的特定實體的詳細資訊。有些實體是 AWS 帳戶，例如使用者和角色。
- 狀態：建立日期欄位包含有關首次建立調查報告日期和時間的詳細資訊。

## 了解 Detective Investigations 報告

Detective Investigations 報告會列出指出入侵的不常見行為或惡意活動的摘要。它還會列出 Detective 建議減輕安全風險的建議。

若要檢視特定調查 ID 的調查報告。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。

2. 在導覽窗格中，選擇調查。
3. 在報告資料表中，選取調查 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	Indicators of compromise	Recommendation
05/25/2023 13:00 UTC - 05/31/2023 19:00 UTC	<a href="#">5 Tactics</a> <a href="#">0 Flagged IP</a> <a href="#">170 Impossible travel</a> <a href="#">1 Finding group</a>	Based on our investigation, we recommend you take action to mitigate what we've found on AWS role Admin. Please review <a href="#">Security Best Practices in IAM</a> to secure your AWS resource.
role		

Detective 會針對已選取範圍時間和使用者產生報告。此報告包含入侵指標區段，其中包含有關以下一或多個入侵指標的詳細資訊。當您檢閱每個入侵指標時，可以選擇要深入檢視的項目，並檢閱其詳細資訊。

- 政策。技術和程序：識別潛在安全事件中使用的政策、技術和程序 (TTP)。MITRE ATT&CK 框架用於理解 TTP。政策以[適用於企業的 ATT&CK 矩陣](#)為基礎。
- 威脅情報已標記的 IP 地址：可疑 IP 地址會根據 Detective 威脅情報標記和識別為嚴重或嚴重威脅。
- 不現實的歷程：檢測並識別帳戶中異常和不現實的使用者活動。例如，該指標列出了短時間跨度內使用者從源到目的地位置之間的劇烈變化。
- 相關調查結果群組：顯示與潛在安全事件相關的多個活動。Detective 使用圖表分析技術，可推斷調查結果與實體之間的關係，並將它們合併分組為調查結果群組。
- 相關調查結果：與潛在安全事件相關聯的相關活動。列出連線至資源或調查結果群組的所有不同類別證據。
- 新地理位置：在資源或帳戶層級識別使用的新地理位置。例如，此指標會根據先前的使用者活動列出觀察到的地理位置，該地理位置為罕見或未使用的位置。
- 新增使用者代理程式：在資源或帳戶層級識別使用的新使用者代理程式。
- 新增 ASO：在資源或帳戶層級識別使用的新自治系統組織 (ASO)。例如，該指標會列出指派為 ASO 的新組織。

## Detective Investigations 報告摘要

調查摘要突出反白顯示已選取範圍時間內需要注意的異常指標。使用摘要，您可以更快速地識別潛在安全問題的根本原因，識別模式，並了解受安全事件影響的資源。

您可以在詳細調查報告摘要中檢視以下詳細資訊。

## 調查概觀

在概觀面板中，您可以查看具有高嚴重性活動的 IP 視覺化，這可以為攻擊者的途徑提供更多內容。

Detective 反白顯示調查中的異常活動，例如 IAM 使用者從來源到遠方目的地不可能的行程。

Detective 將調查映射到潛在安全事件中使用的政策、技術和程序 (TTP)。MITRE ATT&CK 框架用於理解 TTP。政策以[適用於企業的 ATT&CK 矩陣](#)為基礎。

## 調查指標

您可以使用指標窗格中的資訊，判斷 AWS 資源是否涉及可能指出惡意行為及其影響的異常活動。入侵指標 (IOC) 指在網路、系統或環境中或在網路、系統或環境上觀察到的成品，可以 (具有高可信度) 識別惡意活動或安全事件。

## 下載 Detective Investigations 報告

您可以下載 JSON 格式的 Detective Investigations 報告，進一步分析報告，或將其存放在您偏好的儲存解決方案，例如 Amazon S3 儲存貯體。

若要從報告資料表中下載調查報告。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。
3. 從報告資料表中選取調查，然後選擇下載。

若要從摘要頁面下載調查報告。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。
3. 從報告資料表中選取調查。
4. 在調查摘要頁面中，選擇下載。

## 封存 Detective Investigations 報告

當您在 Amazon Detective 中完成調查後，您可以存檔調查報告。已封存的調查表示您已完成檢閱調查。

只有當您是 Detective 管理員時，才能封存或取消封存調查。Detective 會為您的已封存調查提供 90 天的儲存期間。

若要封存報告資料表中的調查報告。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。
3. 從報告資料表中選取調查，然後選擇封存。

若要從摘要頁面封存調查報告。

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查。
3. 從報告資料表中選取調查。
4. 在調查摘要頁面中，選擇封存。

# 分析 Amazon Detective 中的問題清單

調查結果是偵測到的潛在惡意活動或其他風險的執行個體。Amazon GuardDuty 和安全性AWS調查結果會載入 Amazon Detective，以便您可以使用 Detective 調查與涉及實體相關聯的活動。GuardDuty 調查結果是 Detective 核心套件的一部分，預設下會予以擷取。Security Hub CSPM 彙總的所有其他 AWS 安全性調查結果都會擷取為選用的資料來源。如需詳細資訊，請參閱[行為圖表中使用的來源資料](#)。

Detective 調查結果概觀提供有關調查結果的詳細資訊。它也會顯示涉及的實體的概觀，以及相關聯實體設定檔的連結。

如果調查結果與較大活動相關，Detective 會通知您前往調查結果群組。我們建議您使用調查結果群組繼續調查，因為透過調查結果群組，您能夠檢查與潛在安全事件相關的多個活動。請參閱 [the section called “尋找群組”](#)。

Amazon Detective 提供調查結果群組的交互式視覺化。該視覺化效果旨在協助您通過更少的努力，以更快、更徹底地方式調查問題。調查結果群組視覺化面板會顯示調查結果群組中的涉及的調查結果和實體。您可以使用此互動式視覺化來分析、了解和分類調查結果群組的影響。此面板可協助視覺化涉及的實體和涉及的調查結果資料表中顯示的資訊。從視覺化顯示中，您可以選取調查結果或實體以供進一步分析。請參閱[尋找群組視覺化](#)。

## 目錄

- [分析 Detective 中的調查結果概觀](#)
- [分析調查結果群組](#)
- [由生成式 AI 提供支援的調查結果群組摘要](#)
- [封存 Amazon GuardDuty 調查結果](#)

## 分析 Detective 中的調查結果概觀

Detective 調查結果概觀提供有關調查結果的詳細資訊。它也會顯示涉及的實體的概觀，以及相關聯實體設定檔的連結。

### 用於調查結果概觀的範圍時間

調查結果概觀的範圍時間設為調查結果時間範圍。調查結果時間範圍會反映所觀測調查結果活動的首次和末次時間。

## 調查結果詳細資訊

右側的面板包含該調查結果的詳細資訊。此為調查結果提供者提供的詳細資訊。

從調查結果詳細資訊中，您也可以封存調查結果。如需詳細資訊，請參閱[封存 Amazon GuardDuty 調查結果](#)。

## 相關實體

調查結果概觀包含與調查結果相關的實體清單。針對每個實體，清單會提供實體的概觀資訊。此資訊會反映對應實體設定檔上實體資訊設定檔面板上的資訊。

您可以根據實體類型來篩選清單。您也可以根據實體識別符中的文字來篩選清單。

若要錨定至實體的設定檔，請選擇查看設定檔。錨定至實體設定檔時會發生以下情況：

- 範圍時間設定為調查結果時間範圍。
- 在實體的關聯調查結果面板上，系統會選取調查結果。調查結果詳細資訊仍會顯示在實體設定檔的右側。

## 故障診斷「找不到頁面」

當您瀏覽至 Detective 中的實體或調查結果時，可能會看到找不到頁面錯誤訊息。

若要解決此問題，請執行下列動作之一：

- 確認實體或調查結果屬於您的其中一個成員帳戶。如需如何檢閱成員帳戶的資訊，請參閱[檢視帳戶清單](#)。
- 請確定您的管理員帳戶與 GuardDuty 和/或 Security Hub CSPM 保持一致，以從這些服務轉向 Detective。如需建議，請參閱[與 GuardDuty 和 Security Hub CSPM 的建議對齊](#)。
- 確認調查結果是在成員帳戶接受您的邀請後發生。
- 確認 Detective 行為圖形是從選用的資料來源套件擷取資料。如需 Detective 行為圖表中使用的來源資料的詳細資訊，請參閱[行為圖表中使用的來源資料](#)。
- 若要允許 Detective 從 Security Hub CSPM 擷取資料並將該資料新增至您的行為圖表，您必須啟用 Detective 做為資料來源套件AWS的安全性調查結果。如需詳細資訊，請參閱[AWS安全性調查結果](#)。

- 如果您要瀏覽至 Detective 中的實體設定檔或調查結果概觀，請確定 URL 格式正確。如需設定檔 URL 格式的詳細資訊，請參閱[使用 URL 瀏覽至實體設定檔或調查結果概觀](#)。

## 分析調查結果群組

Amazon Detective 調查結果群組可讓您檢查與潛在安全事件相關的多項活動。Amazon Detective 中的調查結果群組會在 Detective 偵測到多個調查結果之間的模式或關係，暗示它們與相同的潛在安全事件相關時建立。此分組有助於更有效率地管理和調查相關調查結果。

您可以使用調查結果群組來分析高嚴重性 GuardDuty 調查結果的根本原因。如果威脅行為者嘗試入侵您的 AWS 環境，他們通常會執行一系列動作，導致多個安全調查結果和異常行為。在不同時間和實體中，此類動作均有所涉及。當對調查結果進行獨立調查時，可能會導致它們的重要性發生誤解，並且難以確定根本原因。Amazon Detective 透過應用圖表分析技術來推斷調查結果與實體之間的關係，並將它們進行分組，藉此解決此問題。我們建議將調查結果群組作為調查涉及的實體和調查結果的起點。

Detective 會分析調查結果中的資料，並根據它們共用的資源將它們與其他可能相關的調查結果進行分組。例如，由相同 IAM 角色工作階段所採取的動作或源自相同 IP 地址的動作相關的調查結果，很可能屬於相同的基礎活動。即使 Detective 所建立的關聯不相關，以群組形式調查調查結果仍具有價值。

調查結果群組是根據下列條件建立的。

- 時間鄰近性 – 在接近時間範圍內發生的調查結果通常會分組在一起，因為它們可能與相同的事件有關。
- 常見實體 – 涉及相同實體的問題清單會分組在一起，例如 IP 地址、使用者或資源。這有助於了解環境不同部分的事件範圍。
- 模式和行為 – Detective 會分析調查結果中的模式和行為，例如類似類型的攻擊或可疑活動，以判斷關係並據此分組。
- 策略、技術和程序 (TTPs) – 共用類似 TTPs 的調查結果，如 MITRE ATT&CK 等架構中所述，會分組在一起以突顯潛在的協同攻擊。

這些條件有助於簡化調查程序，讓您可以專注於可能代表相同安全事件的相互關聯調查結果。

除調查結果之外，各群組還包括調查結果所涉及的實體。實體可以包含 以外的資源，AWS 例如 IP 地址或使用者代理程式。

**Note**

在與另一項調查結果相關的初始 GuardDuty 調查結果發生之後，會在 48 小時內建立包含所有相關調查結果和所有所涉實體的調查結果群組。

## 了解調查結果群組頁面

問題清單群組頁面會列出 Amazon Detective 從您的行為圖表收集的所有問題清單群組。請記下問題清單群組的下列屬性：

### 群組的嚴重性

每個調查結果群組都會根據相關調查結果 AWS 的安全調查結果格式 (ASFF) 嚴重性來指派嚴重性。ASFF 調查結果嚴重性值為嚴重、高、中、低或資訊 (嚴重性從高到低排序)。群組的嚴重性等於該群組中調查結果中的最高嚴重性調查結果。

由影響大量實體的嚴重或高嚴重性調查結果組成的群組應優先進行調查，因為它們代表高影響力的安全問題的可能性更高。

### 群組標題

在標題欄位中，各群組都有唯一的 ID 和非唯一標題。它們以該群組的 ASFF 類型命名空間以及叢集中該命名空間內調查結果的數目為基礎。例如，如果群組具有以下標題：群組具有：TTP (2)、效果 (1) 和異常行為 (2)，則會包含五個總調查結果，其中包含 TTP 命名空間中的兩個調查結果、一個在效果命名空間中的調查結果，以及兩個異常行為命名空間中的調查結果。如需命名空間的完整清單，請參閱 [ASFF 的類型分類](#)。

### 群組中的政策

群組中的政策欄位會詳細說明活動所屬的政策類別。以下清單中的政策、技術和程序類別與 [MITRE ATT&CK 矩陣](#) 一致。

您可以在鏈上選取策略，以查看策略的描述。鏈結下方為在群組內偵測到的策略清單。此類類別及其通常所代表的活動如下：

- 初始訪問：對手試圖進入他人的網路。
- 執行：對手試圖進入他人的網路。
- 持續：對手試圖保持他們的立足點。
- 權限提升：對手試圖獲得更高級別的許可。
- 防禦規避：對手試圖避免被發現。

- 憑證存取：對手試圖竊取帳戶名稱和密碼。
- 發現：對手試圖了解和學習某一環境。
- 橫向運動：對手試圖透過環境進行移動。
- 收集：對手試圖收集目標所感興趣的資料。
- 命令與控制：對手試圖進入他人的網路。
- 滲透：對手試圖奪取資料。
- 影響：對手試圖操縱、中斷或銷毀您的系統和資料。
- 其他：表示調查結果中的活動與矩陣中列出的政策不一致。

## 群組中的實體

實體欄位包含在此群組中所偵測到特定實體的詳細資訊。選取此值可根據以下類別對實體進行細分：身分、網路、儲存和運算。每個類別中的實體範例如下：

- Identity – IAM 主體和AWS 帳戶，例如使用者和角色
- 網路：IP 地址或其他網路和 VPC 實體
- 儲存：Amazon S3 儲存貯體或 DDB
- 計算 Amazon EC2 執行個體或 Kubernetes 容器

## 群組內的帳戶

帳戶欄會告訴您哪些AWS帳戶擁有與群組中調查結果相關的實體。AWS帳戶會依名稱和AWS ID 列出，因此您可以優先調查涉及重要帳戶的活動。

## 群組內的調查結果

調查結果欄位會依嚴重性列出群組內的實體。調查結果包括 Amazon GuardDuty 的調查結果、Amazon Inspector 的調查結果、AWS安全調查結果以及來自 Detective 的證據。您可以選取圖表，依嚴重性查看調查結果的確切計數。

GuardDuty 調查結果是 Detective 核心套件的一部分，預設下會予以擷取。Security Hub CSPM 彙總的所有其他AWS安全性問題清單都會擷取為選用的資料來源。如需詳細資訊，請參閱[行為圖表中使用的來源資料](#)。

## 調查結果群組中的資訊調查結果

Amazon Detective 會根據您在過去 45 天內收集的行為圖表中的資料，識別與調查結果群組相關的其他資訊。Detective 會將此資訊呈現為具有資訊嚴重性的調查結果。證據會提供支援資訊，反白顯示在調查結果群組中檢視時，可能可疑的異常活動或未知行為。這可能包括在調查結果範圍時間內新觀察

到的地理位置或所觀察到的 API 呼叫。證據調查結果只能在 Detective 中檢視，而且不會傳送到AWS Security Hub CSPM。

Detective 會使用 MaxMind GeoIP 資料庫來決定請求的位置。MaxMind 會在國家/地區層級報告非常高的資料準確性，但準確性會根據國家/地區和 IP 類型等因素而有所不同。如需 MaxMind 的詳細資訊，請參閱 [MaxMind IP 地理位置](#)。如果您認為任何 GeoIP 資料不正確，您可以在 [MaxMind Correct GeolP2 Data](#) 向 Maxmind 提交更正請求。

您可以觀察不同主體類型的證據 (例如 IAM 使用者或 IAM 角色)。針對部分證據類型，您可以觀察所有帳戶的證據。這意味著證據會影響您的整個行為圖表。如果所有帳戶均觀察到證據調查結果，您還會看到至少一個相同類型的額外資訊證據調查結果，而該證據調查結果是針對個別 IAM 角色。例如，如果您看到針對所有帳戶觀察到的新地理位置的調查結果，則您還會看到另一針對主體觀察到的新地理位置的調查結果。

### 調查結果群組中的證據類型

- 觀察到新地理位置
- 觀察到新自治系統組織 (ASO)
- 觀察到新使用者代理程式
- 已發出新 API 呼叫
- 觀察到所有帳戶的新地理位置
- 觀察到所有帳戶的新 IAM 主體

## 調查結果群組設定檔

當您選取群組標題時，系統會開啟調查結果群組設定檔，其中包含該群組的其他詳細資訊。在調查結果群組設定檔頁面的詳細資訊面板中，調查結果父項和子項群組可支援顯示高達 1000 個實體和調查結果。

群組設定檔頁面會顯示該群組已設定的範圍時間。這是從群組中包含的最早調查結果或證據到群組中最近更新的調查結果或證據的日期和時間。您也可以看到調查結果群組嚴重性，該嚴重性等於群組中調查結果之間最高嚴重性類別。此設定檔面板中的其他詳細資訊包括：

- 涉及的政策鏈顯示了歸屬於該群組中調查結果的策略。政策以 [適用於企業的 ATT&CK 矩陣](#) 為基礎。政策顯示為一串彩色圓點，代表從最早到最新階段的典型攻擊進度。這意味著鏈上最左邊的圓圈通常代表對手試圖獲得或維護您環境的存取較不嚴重的活動。相反，靠右方的活動嚴重性最高，可能包括資料篡改或破壞。

- 該群組與其他群組的關係。有時，一或多個先前未連接的調查結果群組可能會根據新發現的連結合併到新群組中，例如，涉及現有群組中實體的調查結果。在此情況下，Amazon Detective 會停用父群組並建立子群組。您可以追蹤任何群組歷程至其父群組。群組可以具有以下關係：
  - 子調查結果群組：當調查結果同時涉及兩個其他調查結果群組，且該調查結果又牽涉新調查結果時，系統將建立新調查結果群組。針對任何子群組列出調查結果的父群組。
  - 父調查結果群組：當從調查結果群組中建立了一個子群組時，該群組就成為父群組。如果調查結果群組為父群組，則相關的子群組會與其一起列出。當父群組合併到作用中子群組時，其狀態會變成非作用中。

有兩個資訊標籤可開啟設定檔面板。您可以使用涉及的實體和涉及的調查結果標籤，檢視有關該群組的更多詳細資訊。

使用執行調查來產生調查報告。產生的報告會詳細說明指出入侵的異常行為。

## 群組內的設定檔

### 涉及的實體

著重於調查結果群組中的實體，包括每個實體所連結到的群組內的調查結果。系統還會顯示附加至每個實體的標籤，以便您可以根據標籤快速識別重要實體。選取一個實體，以檢視其實體設定檔。

### 涉及的調查結果

包含有關各調查結果的詳細資訊，包括調查結果的嚴重性、各個涉及的實體，以及該調查結果的初次和最後的出現時間。選取清單中的調查結果類型，以開啟包含該調查結果的其他資訊的調查結果詳細資訊面板。作為涉及的調查結果面板的一部分，您可能會根據您的行為圖表的 Detective 證據，發現資訊性調查結果。

## 調查結果群組視覺化

Amazon Detective 提供調查結果群組的交互式視覺化。該視覺化效果旨在協助您通過更少的努力，以更快、更徹底地方式調查問題。調查結果群組視覺化面板會顯示調查結果群組中的涉及的調查結果和實體。您可以使用此互動式視覺化來分析、了解和分類調查結果群組的影響。此面板可協助視覺化涉及的實體和涉及的調查結果資料表中顯示的資訊。從視覺化顯示中，您可以選取調查結果或實體以供進一步分析。

具有彙總調查結果的 Detective 調查結果群組是連線至相同類型資源的調查結果叢集。透過彙總的調查結果，您可以快速評估調查結果群組的組成，並更快地解釋安全問題。在調查結果群組詳細資訊面板

中，系統會合併相似的調查結果，您可以展開調查結果，以一併檢視相對類似的調查結果。例如，對於具有相同類型資訊性調查結果和中等調查結果的證據節點，系統會將其進行彙總。目前，您可以檢視包含彙總調查結果的調查結果群組的標題、來源、類型和嚴重性。

在此互動面板中，您可以：

- 使用執行調查來產生調查報告。產生的報告會詳述表示有危險狀況的異常行為。如需詳細資訊，請參閱 [Detective Investigations](#)。
- 檢視有關具有彙總調查結果的調查結果群組的詳細資訊，以分析所涉證據、實體和調查結果。
- 檢視實體和調查結果的標籤，以識別具有潛在安全問題的受影響實體。您可以關閉標籤。
- 重新排列實體和調查結果，以更深入地理解它們的互連性。透過在調查結果群組中移動已選取的項目，從群組中隔離實體和調查結果。
- 選取證據、實體及調查結果，以檢視有關它們的更多詳細資訊。若要選取多個項目，請選擇 **command/control** 並選擇項目，或使用指標拖放項目。
- 調整配置，便於所有實體與調查結果符合調查結果群組視窗。檢視調查結果群組中較為普遍的實體類型。

#### Note

調查結果群組視覺化面板支援顯示具有最多 100 個實體和調查結果的調查結果群組。

您可以使用下拉式清單來檢視放射、圓、力導向或網格配置中的問題清單和實體。放射配置可改善視覺化效果，更輕鬆地解讀資料。強制導向配置會定位實體和調查結果，以便連結在項目之間保持一致的長度，並且能夠均勻分佈。此舉有助於減少重疊。您選取的配置會定義調查結果在視覺化面板中的位置。

## 時間軸配置

時間軸配置提供一種動態方式，以視覺化方式呈現問題清單群組如何隨時間演進。這可讓您看到事件的進展，協助您使用 Detective 進一步了解安全事件的順序和潛在因果關係。

使用視覺化面板底部的時間軸滑桿來選取特定時間點。視覺效果將會更新，以顯示此時的調查結果群組狀態。可讓您自動進行時間軸的播放按鈕。按一下播放按鈕以開始動畫。視覺效果會即時更新，顯示調查結果群組如何隨時間變更。使用暫停按鈕隨時停止動畫。

您現在可以使用篩選條件下拉式清單，根據問題清單的嚴重性等級來篩選問題清單。當您套用篩選條件時，視覺化效果會更新為僅顯示符合您所選嚴重性層級的問題清單。篩選條件只會影響時間軸中顯示的

問題清單，而不會影響完整的問題清單群組視覺化。這可讓您快速專注於高優先順序的問題，或調查特定類型的問題清單。

您可以結合時間軸配置使用篩選功能，以查看不同嚴重性等級的問題清單如何隨時間出現和發展。

## 增強型調查工作流程

透過新增時間軸配置和篩選功能，您現在可以進行更全面的調查：

1. 首先，使用其中一個靜態配置（放射、圓形、力導向或網格）檢視整個調查結果群組。
2. 使用時間表來了解情況如何隨著時間發展。
3. 使用播放按鈕自動進行時間軸，觀察關鍵時刻或模式。
4. 在重要時間點暫停以進一步調查。
5. 套用篩選條件以專注於特定嚴重性層級的問題清單。
6. 使用鍵盤快速鍵和選擇工具，深入了解感興趣的實體和調查結果。

此增強型工作流程可讓您更精細且徹底地調查複雜的安全案例。您可以執行更有效率且更有效的安全調查，進而加快事件解決速度並改善整體安全狀態。

## 鍵盤快速鍵

您可以使用下列鍵盤快速鍵與問題清單群組視覺化面板互動：

- 按一下 – 選取單一節點、取消選取所有其他節點、在按一下空格時取消選取所有節點。
- Ctrl + 按一下 – 選取單一節點，不會取消選取其他節點。
- 拖曳 – 平移檢視。
- Ctrl + 拖曳 – Marquee 選取，不會取消選取其他節點。
- Shift + Drag – Marquee 選取、取消選取所有其他節點。
- 方向鍵 – 變更節點之間的焦點。
- Ctrl + 空格 – 選取或取消選取目前聚焦的節點。
- Shift + Arrow 鍵 – 變更節點之間的焦點並選取它們。

動態圖例會根據目前圖表中的實體和調查結果而變更。它可以幫助您識別每個視覺化元素所代表的內容。

## 由生成式 AI 提供支援的調查結果群組摘要

根據預設，Amazon Detective 會自動提供個別調查結果群組的摘要。摘要由于 [Amazon Bedrock](#) 上託管的生成式人工智能 (生成式 AI) 模型提供支援。如果啟用 Detective，則可免費使用問題清單群組摘要。

### Note

自 2026 年 2 月 16 日起，Detective 的調查結果群組摘要功能會自動選取最佳 AWS 區域 (來自您地理位置內的區域端點群組)，以處理您的調查結果群組資料，並使用產生摘要 [the section called “跨區域推論”](#)。

如果您不想使用此功能，您可以從 Detective 的主控制台停用此功能，或在用於存取 Detective 主控台的 IAM 角色上使用拒絕許可。請參閱 [the section called “選擇退出問題清單群組摘要”](#)。

透過使用調查結果群組，您可以檢查與潛在安全事件相關的多個安全調查結果，並識別潛在的威脅行為者。調查結果群組的調查結果群組摘要基於此類功能形成。調查結果群組摘要會使用調查結果群組的資料，快速分析調查結果與受影響資源之間的關係，然後以自然語言彙總潛在威脅。您可以利用此類摘要來識別較大的安全威脅、改善調查效率，並縮短回應時間表。

### Note

由生成式 AI 提供支援的調查結果群組摘要可能不會提供完全準確的資訊。如需詳細資訊，請參閱 [《AWS 負責任 AI 政策》](#)。


## 檢閱調查結果群組摘要

通過調查結果群組的調查結果群組摘要，您會獲得安全事件的清晰詳細說明。說明將以自然語言編寫，包括簡潔的標題，涉及資源的摘要以及有關此類資源的精選資訊。

### 若要檢閱調查結果群組摘要

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中，選擇調查結果群組。
3. 在調查結果群組資料表中，選擇要顯示摘要的調查結果群組。系統將顯示詳細資訊頁面。

在詳細資訊頁面上，您可以使用摘要窗格來檢閱調查結果群組中最多調查結果的產生描述性摘要。您也可以檢閱調查結果群組中最多的安全威脅事件分析，然後您可以進一步調查。要將產生的摘要添加到您的筆記或票證系統中，請選擇窗格中的複製圖示。這會講摘要複製到您的剪貼簿中。您還可以在摘要中分享您對調查結果群組摘要輸出的反饋，以供在未來提供更好的體驗。若要分享您的反應，請根據反應的性質選擇大拇指向上或大拇指向下圖示。

 Note

如果您提供有關調查結果群組摘要的反應，您的反饋不會用於模型調整。您的意見回應僅用於簡化有效制定 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.



## 選擇退出問題清單群組摘要

根據預設，調查結果群組會啟用調查結果群組摘要。不想使用調查結果群組摘要功能的客戶可以在使用者層級選擇退出，或透過用來存取 AWS 管理主控台的 IAM 角色選擇退出。

### 使用者層級選擇退出

每個存取 Detective 的使用者都可以設定其個別偏好設定，以選擇退出調查結果群組摘要功能。選擇退出摘要將阻止透過跨區域推論處理調查結果群組資料。

### 選擇退出問題清單群組摘要

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，選擇偏好設定。
3. 在調查結果群組摘要中，選擇編輯。
4. 關閉已啟用。
5. 選擇儲存。

### IAM 角色型選擇退出

可透過修改用於存取 Detective 的 IAM 角色，選擇不接收調查結果群組摘要功能。為角色的 `detective:InvokeAssistant` 許可新增拒絕陳述式將阻止透過該角色存取 Detective 的所有使用者使用調查結果群組摘要功能，防止透過跨區域推論處理調查結果群組資料。然後，使用者可以個別遵循使用者層級選擇退出步驟，以防止摘要窗格出現。

### 使用 IAM 選擇退出問題清單群組摘要

1. 識別用於存取 Amazon Detective 的 IAM 角色。
2. 將具有 `detective:InvokeAssistant` 動作 Deny 效果的 IAM 政策陳述式新增至角色。

## 啟用調查結果群組摘要

如果您先前選擇不接收調查結果群組的調查結果群組摘要，您可以隨時再次啟用它們。

### 啟用調查結果群組摘要

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，選擇偏好設定。

3. 在調查結果群組摘要中，選擇編輯。
4. 打開已啟用。
5. 選擇儲存。

## 跨區域推論

Detective 會自動選取您地理位置內的最佳 AWS 區域，以處理您的調查結果群組資料並產生摘要。這可將可用的運算資源、模型可用性最大化，並提供最佳客戶體驗。您的調查結果群組資料只會儲存在摘要請求產生的區域中，但調查結果群組資料和摘要結果可能會在該區域之外處理。所有資料都會透過 Amazon 的安全網路進行加密傳輸。

Detective 會將您的推論請求安全地路由到發出請求的地理區域內的可用運算資源，如下表所示。

### 跨區域推論路由

支援的 Detective 地理位置	Detective 區域	推論區域
美國	us-east-1	us-east-1、us-east-2、us-west-1、us-west-2
	us-west-2	us-east-1、us-east-2、us-west-1、us-west-2
歐洲	eu-central-1	eu-central-1、eu-central-2、eu-north-1、eu-south-1、eu-south-2、eu-west-1、eu-west-2、eu-west-3
日本	ap-northeast-1	ap-northeast-1、ap-northeast-3

## 支援的區域

問題清單群組摘要可在下列 AWS 區域取得。

- 美國東部 (維吉尼亞北部)
- 美國西部 (奧勒岡)
- 亞太地區 (東京)

- 歐洲 (法蘭克福)

## 封存 Amazon GuardDuty 調查結果

當您完成對 Amazon GuardDuty 調查結果的調查後，您可以封存 Amazon Detective 的調查結果。此舉可以節省傳回至 GuardDuty 進行更新的麻煩。封存調查結果表示您已完成對該調查結果的調查。

如果您也是與調查結果相關聯帳戶的 GuardDuty 管理員帳戶，則只能從 Detective 內部封存 GuardDuty 調查結果。如果您不是 GuardDuty 管理員帳戶，而且您嘗試封存調查結果，則 GuardDuty 會顯示錯誤。

### 若要封存 GuardDuty 調查結果

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在 Detective 主控台的調查結果詳細資訊面板中，選擇封存調查結果。
3. 出現確認提示時，選擇封存。

您可以在 GuardDuty 主控台中檢視已封存的 GuardDuty 調查結果。封存的調查結果會存放在 GuardDuty 90 天，您可以在該期間內隨時檢視。您可以在 GuardDuty 主控台中檢視隱藏的問題清單，方法是從問題清單資料表中選取封存，或透過 GuardDuty API 使用 [ListFindings](#) API 搭配 `afindingCriteria.criterion of service.archived` 等於 `true`。若要進一步了解，請參閱《Amazon GuardDuty 使用者指南》中的 [隱藏規則](#)。

# 分析 Amazon Detective 中的實體

實體是從來源資料中擷取的單個對象。範例包括特定 IP 地址、Amazon EC2 執行個體或 AWS 帳戶。如需實體類型的清單，請參閱 [the section called “行為圖表資料結構中的實體類型”](#)。

Amazon Detective 實體設定檔是單一頁面，提供實體及其活動的詳細資訊。您可以使用實體設定檔，以取得調查結果之調查的支援詳細資訊，或作為常規追捕可疑活動的一部分。

## 目錄

- [使用實體設定檔](#)
- [檢視並與 Detective 設定檔面板互動](#)
- [直接導覽至實體設定檔或調查結果概觀](#)
- [從設定檔面板錨定至另一主控台](#)
- [在設定檔面板上探索活動詳細資訊](#)
- [管理範圍時間](#)
- [在 Detective 中檢視相關調查結果的詳細資訊](#)
- [在 Detective 中檢視大量實體的詳細資訊](#)

## 使用實體設定檔

當您執行以下其中一項動作時，系統會顯示實體設定檔會：

- 在 Amazon GuardDuty 主控台中，選擇調查與已選取調查結果相關的實體的選項。

請參閱 [the section called “從其他主控台錨定”](#)。

- 前往實體設定檔的 Detective URL。

請參閱 [the section called “透過 URL 導覽”](#)。

- 使用 Detective 主控台內的 Detective 搜尋來查詢實體。
- 從另一個實體設定檔或調查結果概觀中選擇實體設定檔的連結。

## 實體設定檔的範圍時間

當您直接導覽至實體設定檔而不提供範圍時間時，範圍時間會設定為前 24 小時。

當您從其他實體設定檔導覽至實體設定檔時，目前已選取的範圍時間會保持不變。

當您從調查結果概觀導覽至實體設定檔時，範圍時間會設為調查結果時間範圍。

如需自訂範圍時間以限制實體設定檔上顯示的資料的資訊，請參閱[管理範圍時間](#)。

## 實體識別符和類型

設定檔的頂端是實體識別符和實體類型。每個實體類型都有對應圖示，以提供設定檔類型的視覺指示器。

## 涉及的調查結果

每個設定檔都包含實體在範圍時間內的涉及的調查結果清單。

您可以查看每個調查結果的詳細資訊、變更範圍時間以反映調查結果時間範圍，並前往搜索結果概觀以尋找其他所涉資源。

請參閱 [the section called “檢視實體的調查結果”](#)。

## 與此實體相關的調查結果群組

每個設定檔都包含容納的調查結果群組清單。

調查結果群組由調查結果、實體和證據組成，Detective 會收集到一個群組中，以提供有關可能安全問題的更多內容。

如需調查結果群組的詳細資訊，請參閱 [the section called “尋找群組”](#)。

## 包含實體詳細資訊和分析結果的設定檔

每個實體設定檔都包含一個或多個標籤。每個標籤都包含一個或多個設定檔面板。每個設定檔面板都包含通過行為圖表資料產生的文字和視覺化。特定標籤和設定檔面板會根據實體類型進行自定義。

對於大多數實體，第一個標籤頂端的面板會提供有關實體的高階摘要資訊。

其他設定檔面板會反白顯示不同類型的活動。對於與調查結果有關的實體，實體設定檔面板上的資訊可以提供其他支援證據，以協助完成調查。每個設定檔面板都可以存取有關如何使用資訊的指南。如需詳細資訊，請參閱 [the section called “使用設定檔面板指引”](#)。

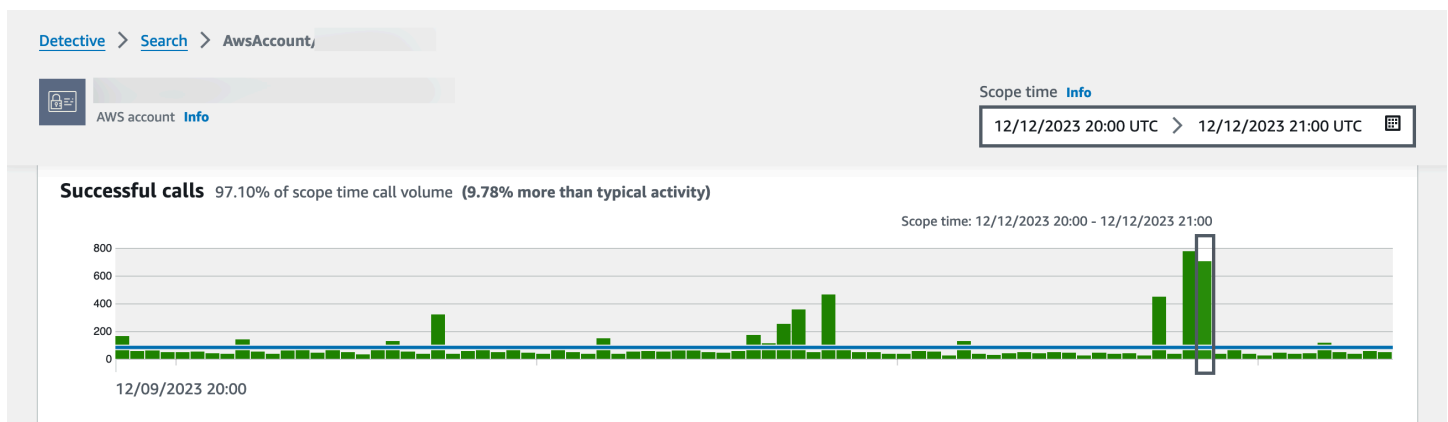
如需設定檔面板、設定檔面板所包含之資料類型以及與其進行互動之可用選項的詳細資訊，請參閱 [the section called “設定檔面板”](#)。

## 在實體設定檔中導覽

實體設定檔包含一個或多個標籤。每個標籤都包含一個或多個設定檔面板。每個設定檔面板都包含通過行為圖表資料產生的文字和視覺化。

當您向下捲動設定檔標籤時，設定檔頂端仍會顯示以下資訊：

- 實體類型
- 實體識別符
- 範圍名稱



## 檢視並與 Detective 設定檔面板互動

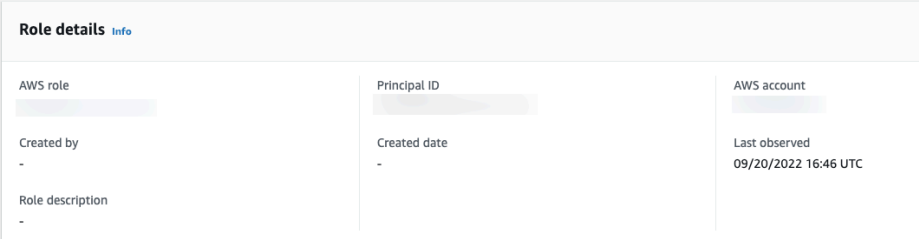
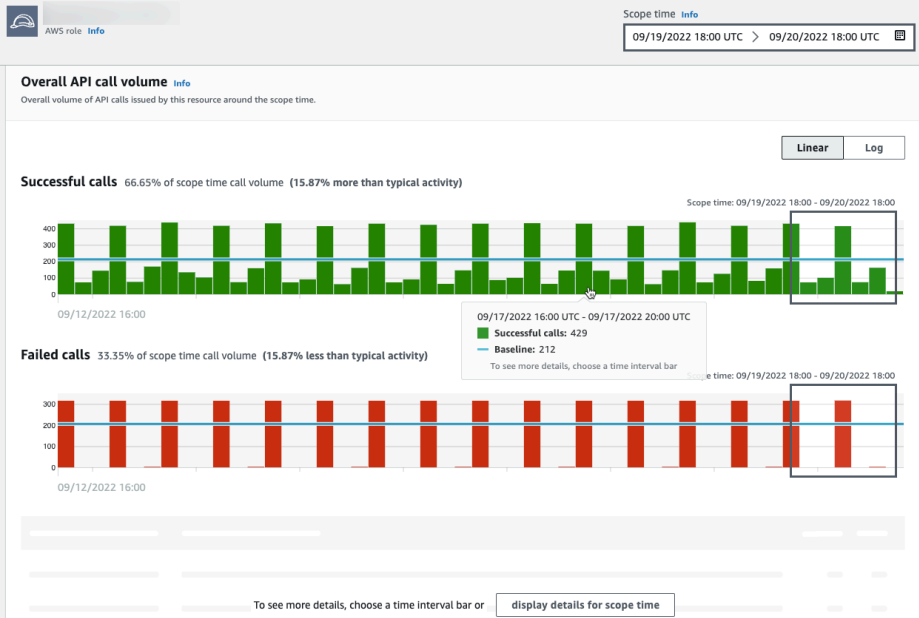
Amazon Detective 主控台上的每個實體設定檔都包含一組設定檔面板。設定檔面板是可提供一般詳細資訊或反白顯示與實體相關聯特定活動的視覺化。設定檔面板使用不同類型的視覺化來呈現不同類型的資訊。他們還可以提供其他詳細資訊或其他設定檔的連結。

每個設定檔面板都旨在幫助分析師找到有關實體及其相關活動的特定問題的答案。此類問題的答案有助於得出有關活動是否代表真正威脅的結論。

設定檔面板使用不同類型的視覺化來呈現不同類型的資訊。

## 設定檔面板上的資訊類型

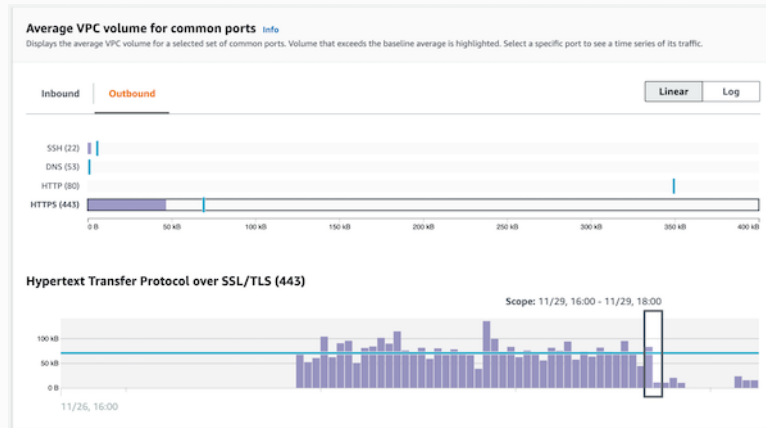
設定檔面板通常提供以下類型的資料。

面板資料類型	描述
有關調查結果或實體的高階資訊	<p>最簡單的面板類型提供有關實體的部分基本資訊。</p> <p>資訊面板中包含的資訊範例包括識別符、名稱、類型和建立日期。</p>  <p>大多數實體設定檔都包含該實體的資訊面板。</p>
活動在一段時間內的一般摘要	<p>顯示實體在一段時間內的活動摘要。</p> <p>此類型面板提供了實體在範圍時間內行為的整體檢視。</p>  <p>以下是在 Detective 設定檔面板上提供的部分摘要資料範例：</p> <ul style="list-style-type: none"> <li>失敗和成功的API呼叫</li> <li>傳入和傳出VPC磁碟區</li> </ul>
依值分組的活動摘要	顯示實體的活動摘要，依特定值分組。

## 面板資料類型

## 描述

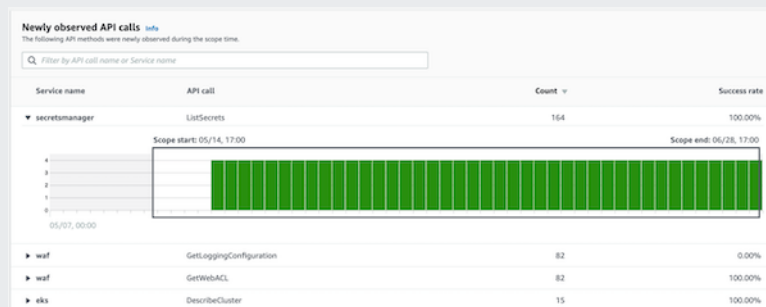
您可以在EC2執行個體的設定檔上看到這種類型的設定檔面板。設定檔面板會顯示與特定服務類型相關聯的常見連接埠，往返EC2執行個體的平均VPC流量日誌資料量。



## 只在範圍時間內開始的活動

在調查期間，查看在特定時間範圍內才開始發生的活動非常有幫助。

例如，是否有以前未看到的API通話、地理位置或使用者代理？

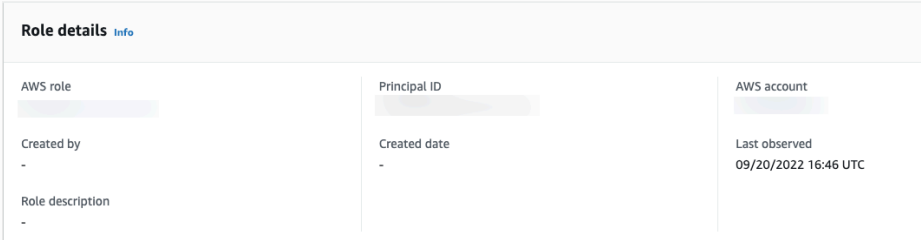


如果行為圖表仍處於訓練模式，則設定檔面板會顯示通知訊息。當行為圖表累積至少兩週的資料時，系統就會移除訊息。如需訓練模型的詳細資訊，請參閱 [the section called “新行為圖表的訓練期間”](#)。

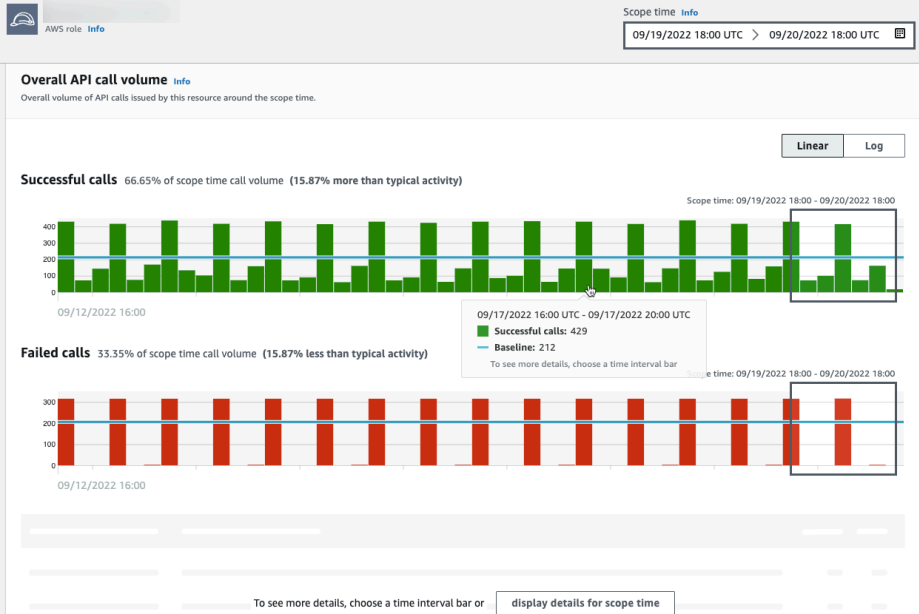
面板資料類型	描述
範圍時間內顯著變更的活動	<p>與新活動面板類似，設定檔面板也可以顯示範圍時間內顯著變更的活動。</p> <p>例如，使用者可能會每週定期發出特定API呼叫數次。如果同一位使用者在單日內突然發出多次相同呼叫，則可能是惡意活動的證據。</p>  <p>如果行為圖表仍處於訓練模式，則設定檔面板會顯示通知訊息。當行為圖表累積至少兩週的資料時，系統就會移除訊息。如需訓練模型的詳細資訊，請參閱 <a href="#">the section called “新行為圖表的訓練期間”</a>。</p>

## 設定檔面板視覺化類型

設定檔面板內容可以採用以下形式之一。

視覺化類型	描述
鍵值對	<p>最簡單的視覺化類型是一組鍵值對。</p> <p>調查結果或實體資訊面板是最常見鍵值對面板範例。</p>  <p>鍵值對也可用於將其他資訊新增至其他類型的面板。</p>

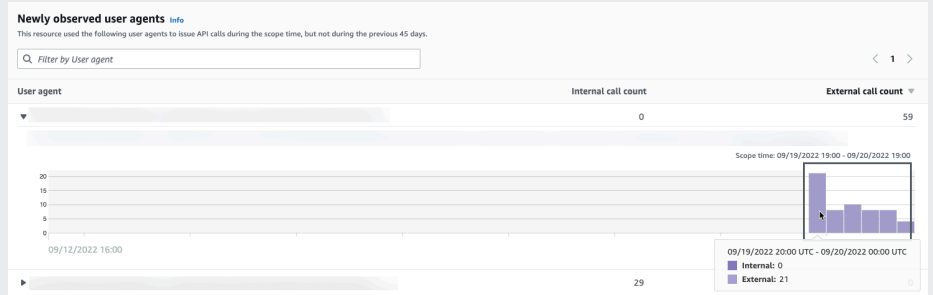
視覺化類型	描述
	<p>從鍵值對面板中，如果值是某一實體的識別符，則可以錨定至其設定檔。</p>
<p>資料表</p>	<p>資料表是項目的簡單多欄位清單。</p>  <p>您可以排序、篩選和逐頁瀏覽資料表。</p> <p>您可以變更要在每個頁面上顯示的項目數目。請參閱 <a href="#">the section called “設定檔面板的偏好設定”</a>。</p> <p>如果資料表中的值為實體的識別符，則您可以錨定至其設定檔。</p>

時間表	時間軸視覺化會顯示定義時間間隔的彙總值。
	 <p>時間軸會反白顯示目前的範圍時間，並包含範圍時間之前和之後的額外周邊時間。周邊時間為範圍時間內的活動提供內容。</p> <p>將滑鼠暫留在某個時間間隔上，即可顯示該時間間隔的資料摘要。</p>

視覺化類型	描述
-------	----

### 可擴展資料表

可擴展資料表結合了資料表和時間軸。



視覺化以資料表開始。

您可以排序、篩選和逐頁瀏覽資料表。

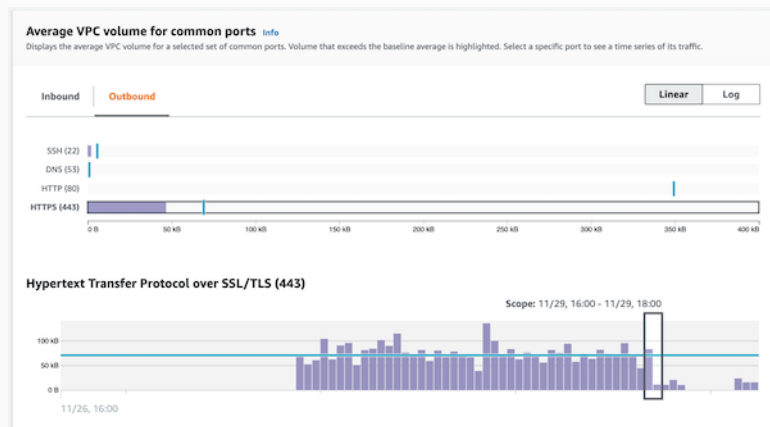
您可以變更要在每個頁面上顯示的項目數目。請參閱 [the section called “設定檔面板的偏好設定”](#)。

然後，您可以展開每一列，以顯示該列特定的時間軸視覺化。

### 長條圖

長條圖會根據群組顯示值。

根據圖表，您可以選擇長條，以顯示相關活動的時間軸。



視覺化類型	描述
<p>地理位置圖表</p>	<p>地理位置圖表會顯示標記為根據地理位置反白顯示資料的地圖。它可以附加在包含有關單個地理位置詳細資訊的資料表之後。</p> <p>請注意，在處理傳入的地理資料時，Detective 會將緯度和經度值四捨五入為一位小數點。</p>

## 設定檔面板內容的備註

檢視設定檔面板的內容時，請注意以下項目：

### 近似計數資料警告

此警告表示因相關資料量而導致無法顯示計數極低的項目。

若要確保計數完全準確，請減少資料量。最簡單的方法是減少範圍時間的長度。請參閱 [the section called “管理範圍時間”](#)。

### 地理位置的四捨五入

Detective 會將所有緯度和經度值四捨五入為一位小數點。

### Detective 如何代表API呼叫的變更

自 2021 年 7 月 14 日起，Detective 會追蹤每次API呼叫的服務。每當 Detective 顯示API方法時，它也會顯示相關聯的服務。在顯示API通話相關資訊的設定檔面板上，通話一律會依服務分組。針對 Detective 在該日期之前擷取的資料，服務名稱會列為未知服務。

此外，從 2021 年 7 月 14 日開始，對於帳戶和角色，整體API通話量設定檔面板的活動詳細資訊將不再顯示發出通話AKID的資源的。針對帳戶，Detective 會顯示發出呼叫之主體 (使用者或角色) 的識別符。針對角色，Detective 會顯示角色工作階段的識別符。針對 Detective 在 2021 年 7 月 14 日之前擷取的資料，識別符會列為未知資源。

對於顯示API通話清單的設定檔面板，相關聯的時間軸會反白顯示發生此轉換的時段。反白顯示將於 2021 年 7 月 14 日開始，並在 Detective 中完全傳播更新時結束。

## 設定檔面板的偏好設定

對於設定檔面板，您可以自訂設定檔面板上每個頁面上顯示的列數，並設定時間戳記格式偏好設定。

### 設定資料表長度

針對包含資料表或可擴展資料表的設定檔面板，您可以設定要在每個頁面上顯示的列數。

設定每個頁面上項目數的偏好設定。

1. 在開啟 Amazon Detective 主控台<https://console.aws.amazon.com/detective/>。
2. 在 Detective 導覽窗格的設定下，選擇偏好設定。
3. 在偏好設定頁面的資料表長度下，按一下編輯。
4. 選擇要在每個頁面上顯示的資料表列數。
5. 選擇 Save (儲存)。

### 設定時間戳記格式

對於設定檔面板，您可以設定時間戳記格式偏好設定，其將套用至 Detective 中每個IAM使用者或IAM角色的所有時間戳記。

#### Note

時間戳記格式偏好設定不會套用至整個 AWS 帳戶。

設定時間戳記的偏好設定。

1. 在開啟 Amazon Detective 主控台<https://console.aws.amazon.com/detective/>。
2. 在 Detective 導覽窗格的設定下，選擇偏好設定。

3. 在偏好設定頁面的時間戳記偏好設定下，檢視並變更所有時間戳記的偏好顯示。
4. 根據預設，時間戳記格式會設定為 UTC。按一下編輯以選擇您的當地時區。

範例：

Example

UTC - 09/20/22 16 : 39 UTC

Local - 09/20/2022 9 : 39 ( UTC-07 : 00 )

5. 選擇 Save (儲存)。

## 直接導覽至實體設定檔或調查結果概觀

若要直接導覽至實體設定檔或 Amazon Detective 中的調查結果概觀，您可以使用以下其中一個選項。

- 從 Amazon GuardDuty 或中 AWS Security Hub CSPM，您可以從 GuardDuty 調查結果轉向對應的 Detective 調查結果設定檔。
- 您可以組合識別調查結果或實體的 Detective URL，並設定要使用的範圍時間。

## 從 Amazon GuardDuty 或 樞紐至實體設定檔或調查結果概觀 AWS Security Hub CSPM

您可以從 Amazon GuardDuty 主控台導覽至與調查結果相關實體的實體設定檔。

從 GuardDuty 和 AWS Security Hub CSPM 主控台，您也可以導覽至調查結果概觀。這也提供了相關實體的實體設定檔連結。

此類連結有助於簡化調查程序。您可以快速使用 Detective 來查看關聯的實體活動並決定後續步驟。然後，您可以將調查結果封存為誤判，或進一步探索以判斷問題範圍。

### 如何錨定至 Amazon Detective 主控台

所有 GuardDuty 調查結果均可使用調查連結。透過 GuardDuty，您可以選擇是否導覽至實體設定檔或調查結果概觀。

從 GuardDuty 主控台錨定至 Detective

1. 前往 <https://console.aws.amazon.com/guardduty/> 開啟 GuardDuty 主控台。

2. 如有必要，請在左側導覽窗格中選擇調查結果。
3. 在 GuardDuty 調查結果頁面上，選擇調查結果。

調查結果詳細資訊窗格會顯示在調查結果清單的右側。

4. 從調查結果詳細資訊窗格中，選擇在 Detective 中調查。

GuardDuty 會顯示 Detective 中可用待調查項目清單。

此清單包含相關實體，例如 IP 地址或 EC2 執行個體以及調查結果。

5. 選擇實體或調查結果。

Detective 主控台會在新標籤中開啟。主控台會向實體或調查結果設定檔開啟。

如果您尚未啟用 Detective，則主控台會開啟提供 Detective 概觀的登陸頁面。您可以在此選擇啟用 Detective。

#### 從 Security Hub CSPM 主控台轉向 Detective

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 如有必要，請在左側導覽窗格中選擇調查結果。
3. 在 Security Hub CSPM 調查結果頁面上，選擇 GuardDuty 調查結果。
4. 在詳細資訊窗格中，選擇在 Detective 中調查，然後選擇調查結果。

當您選擇對調查結果進行調查時，Detective 主控台會在新標籤中開啟。主控台會開啟並顯示調查結果概觀。

Detective 主控台一律會開啟至調查結果來源的區域，即使您從彙總區域進行錨定。如需調查結果彙總的詳細資訊，請參閱《AWS Security Hub 使用者指南》中的[跨區域彙總調查結果](#)。

如果您尚未啟用 Detective，則主控台會開啟 Detective 登陸頁面。您可以在此啟用 Detective。

#### 對錨定進行疑難排解。

若要使用錨定，必須符合以下條件：

- 您的帳戶必須是 Detective 和您要從中錨定的服務的管理員帳戶。
- 您已擔任跨帳戶角色，可授予您管理員帳戶對行為圖表的存取權。

如需有關建議對齊管理員帳戶的詳細資訊，請參閱[與 Amazon GuardDuty 和 的建議對齊 AWS Security Hub CSPM](#)。

如果錨定不起作用，請檢查以下內容。

- 調查結果是否屬於行為圖表中已啟用的成員帳戶？如果關聯帳戶未以成員帳戶的身份邀請加入行為圖表，則行為圖表不會包含該帳戶的資料。

如果受邀成員帳戶不接受邀請，則行為圖表不會包含該帳戶的資料。

- 調查結果是否已封存？Detective 未收到來自 GuardDuty 的封存調查結果。
- 在 Detective 開始將資料擷取至行為圖表之前，該調查結果是否已出現？如果 Detective 所擷取的資料中無調查結果，則行為圖表不會包含該調查結果的資料。
- 調查結果是否來自正確區域？每個行為圖表都針對一個區域。行為圖表不包含來自其他區域的資料。

## 透過 URL 導覽至實體設定檔或調查結果概觀

若要導覽至實體設定檔或在 Amazon Detective 中的調查結果概觀，您可以使用提供直接連結的 URL。URL 可識別調查結果或實體。它也可以指定要在設定檔上使用的範圍時間。Detective 可保存長達一年的歷史事件資料。

### 設定檔 URL 的格式

#### Note

如果您使用舊版 URL 格式，Detective 會自動重新導向至新 URL。舊版 URL 格式為：

```
https://console.aws.amazon.com/detective/home?  
region=Region#type/namespace/instanceID?parameters
```

設定檔 URL 的新版格式如下：

- 針對實體：https://console.aws.amazon.com/detective/home?  
region=*Region*#*entities/namespace/instanceID?parameters*
- 針對調查結果：https://console.aws.amazon.com/detective/home?  
region=*Region*#*findings/instanceID?parameters*

URL 需要以下值。

## ##

您希望使用的區域。

## *type*

您要導覽設定檔的項目類型。

- `entities` : 表示您正在瀏覽至實體設定檔
- `findings` : 表示您正在瀏覽至調查結果概觀

## ####

針對實體，命名空間是實體類型的名稱。

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

## *instanceID*

調查結果或實體的執行個體識別符。

- 針對 GuardDuty 調查結果，則為 GuardDuty 調查結果識別符。
- 若為 AWS 帳戶，則為 帳戶 ID。

- 對於 AWS 角色和使用者，則為角色或使用者的主要 ID。
- 若為聯合身分使用者，則為聯合身分使用者的主體 ID。主體 ID 為 `<identityProvider>:<username>` 或 `<identityProvider>:<audience>:<username>`。
- 針對 IP 地址，則為 IP 地址。
- 針對使用者代理程式，則為使用者代理程式名稱。
- 針對 EC2 執行個體，則為執行個體 ID。
- 針對角色工作階段，則為角色工作階段識別符。工作階段識別符使用格式 `<rolePrincipalID>:<sessionName>`。
- 針對 S3 儲存貯體，則為儲存貯體名稱。
- 針對調查項目群組，則為 UUID。例如：ca6104bc-a315-4b15-bf88-1c1e60998f83
- 針對 EKS 資源，使用以下格式：
  - EKS 叢集：`<clusterName>~<accountId>~EKS`
  - Kubernetes Pod：`<podUid>~<clusterName>~<accountId>~EKS`
  - Kubernetes 主體：`<subjectName>~<clusterName>~<accountId>`
  - 容器映像：`<registry>/<repository>:<tag>@<digest>`

調查結果或實體必須與行為圖表中已啟用的帳戶相關聯。

URL 也可以包含以下選用參數，用於設定範圍時間。如需範圍時間及其在設定檔上使用方式的詳細資訊，請參閱 [the section called “管理範圍時間”](#)。

### scopeStart

在設定檔上使用的範圍時間的開始時間。開始時間必須在過去 365 天內。

該值是紀元時間戳記。

如果您提供了開始時間，但未提供結束時間，則範圍時間會在目前時間結束。

### scopeEnd

在設定檔上使用的範圍時間的結束時間。

該值是紀元時間戳記。

如果您提供了結束時間，但未提供開始時間，則範圍時間會包含結束時間之前的所有時間。

如果您未指定範圍時間，則系統會使用預設的範圍時間。

- 針對調查結果，預設範圍時間會使用觀察到調查結果活動的首次和末次時間。
- 針對實體，預設範圍時間為前 24 小時。

以下是 Detective URL 的範例：

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

該範例 URL 提供以下指示。

- 顯示 IP 地址 192.168.1 的實體設定檔。
- 使用 2019 年 3 月 18 日星期一上午 12:00:00 GMT 開始至 2019 年 3 月 18 日星期一下午 12:00:00 GMT 結束的範圍時間。

## URL 疑難排解

如果 URL 未顯示預期的設定檔，請先檢查 URL 是否使用了正確的格式，以及您是否提供了正確的

- 您是否使用了正確的 URL (findings 或 entities)？
- 您是否指定了正確的命名空間？
- 您是否提供了正確的識別符？

如果值正確，則還可以檢查以下內容。

- 調查結果或實體是否屬於行為圖表中已啟用的成員帳戶？如果關聯帳戶未以成員帳戶的身份邀請加入行為圖表，則行為圖表不會包含該帳戶的資料。

如果受邀成員帳戶不接受邀請，則行為圖表不會包含該帳戶的資料。

- 針對某一調查結果，是否對其封存？Detective 未收到來自 Amazon GuardDuty 的封存調查結果。
- 在 Detective 開始將資料擷取至行為圖表之前，該調查結果或實體是否已出現？如果 Detective 所擷取的資料中無調查結果或實體，則行為圖表不會包含該調查結果的資料。
- 調查結果或實體是否來自正確區域？每個行為圖表都針對一個區域。行為圖表不包含來自其他區域的資料。

## 向 Splunk 新增 Detective 調查結果的 URL

Splunk Trumpet 專案可讓您將資料從 AWS 服務傳送至 Splunk。

您可以設定 Trumpet 專案，以產生 Amazon GuardDuty 調查結果的 Detective URL。然後，您可以使用此類 URL 直接從 Splunk 轉換到相應的 Detective 調查結果設定檔。

Trumpet 專案可以從 GitHub 上透過以下網址找到：<https://github.com/splunk/splunk-aws-project-trumpet>。

在 Trumpet 專案的設定頁面上，從 AWS CloudWatch 事件中，選擇 Detective GuardDuty URL。

## 從設定檔面板錨定至另一主控台

針對 EC2 執行個體、IAM 使用者和 IAM 角色，您可以直接從詳細資訊設定檔面板導覽至對應的主控台。主控台提供的資訊可以為您的安全調查提供額外的輸入。

在 EC2 執行個體詳細資訊設定檔面板上，EC2 執行個體識別符會連結至 Amazon EC2 主控台。

在使用者詳細資訊設定檔面板上，使用者名稱會連結至 IAM 主控台。

在角色詳細資訊設定檔面板上，角色名稱會連結至 IAM 主控台。

## 從設定檔面板錨定至另一實體設定檔

當設定檔面板包含不同實體的識別符時，其通常是該實體設定檔的連結。例外情況指針對 EC2 執行個體上 Amazon EC2 和 IAM 主控台、IAM 使用者和 IAM 角色設定檔的連結。請參閱 [the section called “錨定至其他主控台”](#)。

例如，從 IP 地址清單中，您可能會針對特定 IP 地址顯示設定檔。如此一來，您就可以查看是否有其他資訊可協助您完成調查。

## 在設定檔面板上探索活動詳細資訊

在調查期間，您可能想要進一步調查實體的活動模式。

在以下設定檔面板上，您可以顯示活動詳細資訊的摘要：

- 整體 API 呼叫量，使用者代理程式設定檔上的設定檔面板除外

- 新觀察到的地理位置
- VPC 整體流量
- 針對與單一 IP 地址相關聯的調查結果，往來于調查結果 IP 地址的 VPC 流量
- 容器詳細資訊
- 叢集的 VPC 流量
- Kubernetes 整體 API 活動

活動詳細資訊可回答以下類型的問題：

- 使用了哪些 IP 地址？
- 此類 IP 地址位於何處？
- 每個 IP 地址進行了哪些 API 呼叫，以及他們透過哪些服務進行呼叫？
- 使用哪些主體或存取金鑰識別符 (AKID) 用於呼叫？
- 使用哪些資源用於呼叫？
- 呼叫次數？成功和失敗次數？
- 每個 IP 地址傳入或傳出多少 VPC 流程日誌資料？
- 指定叢集、映像或 Pod 的哪些容器處於作用中狀態？

## 主題

- [整體 API 呼叫量的活動詳細資訊](#)
- [地理位置的活動詳細資訊](#)
- [整體 VPC 流量的活動詳細資訊](#)
- [涉及 EKS 叢集的整體 Kubernetes API 活動](#)

## 整體 API 呼叫量的活動詳細資訊

整體 API 呼叫量的活動詳細資訊，顯示在所選時間範圍內的 API 呼叫資料。

若要顯示單一時間間隔的活動詳細資訊，請在圖表上選擇時間間隔。

若要顯示目前範圍時間的活動詳細資訊，請選擇顯示範圍時間的詳細資訊。

請注意，自 2021 年 7 月 14 日起，Detective 開始儲存並顯示 API 呼叫的服務名稱。該日期會在設定檔面板的時間軸上反白顯示。針對在該日期之前發生的活動，服務名稱為未知服務。

## 活動詳細資訊的內容 (使用者、角色、帳戶、角色工作階段、EC2 執行個體和 S3 儲存貯體)

針對 IAM 使用者、IAM 角色、帳戶、角色工作階段、EC2 執行個體和 S3 儲存貯體，活動詳細資訊包含以下資訊：

- 每個標籤都會提供在所選時間範圍內發出的 API 呼叫組的相關資訊。

針對 S3 儲存貯體，資訊會反映對 S3 儲存貯體進行的 API 呼叫。

API 呼叫會依呼叫它們的服務進行分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

- 針對每個項目，活動詳細資訊都會顯示成功和失敗的呼叫次數。觀察到的 IP 地址標籤也會顯示每個 IP 地址的位置。
- 每個項目均顯示呼叫方的訊息。活動詳細資訊會針對帳戶識別使用者或角色。活動詳細資訊會針對角色識別角色工作階段。針對使用者和角色工作階段，活動詳細資訊會識別存取金鑰識別符 (AKID)。

請注意，從 2021 年 7 月 14 日起，針對帳戶設定檔，活動詳細資訊會顯示使用者或角色，而非 AKID。針對角色設定檔，活動詳細資訊會顯示角色工作階段，而非 AKID。針對在 2021 年 7 月 14 日之前發生的活動，呼叫者會列為未知資源。

活動詳細資訊包含以下標籤：

### 觀察到的 IP 地址

初始顯示用於發出 API 呼叫的 IP 地址清單。

您可以展開每個 IP 地址，以顯示從該 IP 地址發出的 API 呼叫清單。API 呼叫會依呼叫它們的服務進行分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

然後，您可以展開每個 API 呼叫，以顯示來自該 IP 地址的呼叫者清單。根據設定檔而定，呼叫者可能是使用者、角色、角色工作階段或 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
[redacted]	421	311	-
s3	316	311	
config	61	0	
kms	15	0	
DescribeKey	14	0	
[redacted] Role session ([redacted])	14	0	
ListKeys	1	0	
rds	7	0	
ec2	4	0	
autoscaling	3	0	
secretsmanager	2	0	
guardduty	2	0	
es	2	0	

## 依服務分類的 API 方法

最初顯示已發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

您可以展開每個 API 方法，以顯示從中發出呼叫的 IP 地址清單。

然後，您可以展開每個 IP 地址，以顯示從該 IP 地址發出該 API 呼叫的 AKID 清單。

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

API method	Successful calls	Failed calls
s3	316	311
config	61	0
kms	15	0
DescribeKey	14	0
[redacted]	14	0
[redacted] Role session ([redacted])	14	0
ListKeys	1	0
rds	7	0
ec2	4	0
autoscaling	3	0

## 資源或存取金鑰 ID

初始顯示用來發出 API 呼叫的使用者、角色、角色工作階段或 AKID 的清單。

您可以展開每個呼叫者，以顯示呼叫者從 IP 地址發出 API 呼叫的清單。

然後，您可以展開每個 IP 地址，以顯示該呼叫者從該 IP 地址發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

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

Resource	Successful calls	Failed calls
Role session	322	310
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
...	...	...

## 活動詳細資訊的內容 (IP 地址)

針對 IP 地址，活動詳細資訊包含以下資訊：

- 每個標籤都會提供在所選時間範圍內發出的 API 呼叫組的相關資訊。API 呼叫會依發出呼叫的服務分組。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。
- 針對每個項目，活動詳細資訊都會顯示成功和失敗的呼叫次數。

活動詳細資訊包含以下標籤：

### 資源

初始顯示從 IP 地址發出 API 呼叫的資源清單。

針對每個資源，清單包括資源名稱、類型和 AWS 帳戶。

您可以展開每個資源，以顯示資源從 IP 地址發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

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

Resource	Successful calls	Failed calls	Account ID
▼ [redacted] AWS role	3,520	0	[redacted]
▼ 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	
▶ [redacted] AWS role	1,715	0	[redacted]
▶ [redacted] AWS role	504	480	[redacted]

## 依服務分類的 API 方法

最初顯示已發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

您可以展開每個 API 呼叫，以顯示所選期間內從 IP 地址發出的 API 呼叫的資源清單。

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

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
[redacted] AWS role ([redacted])	222	0
[redacted] AWS role ([redacted])	170	0
▶ SendCommand	89	16
▶ logs	165	0
▶ sts	149	0
▶ iam	149	12

## 排序活動詳細資訊

您可以依任何清單欄排序活動詳細資訊。

當您使用第一欄位排序時，系統只會排序頂層清單。較低級別的清單始終按成功 API 呼叫的計數進行排序。

## 篩選活動詳細資訊

您可以使用篩選選項，來專注於活動詳細資訊中所表示的特定子集或活動方面。

在所有標籤上，您可以依第一欄位中的任何值篩選清單。

### 若要新增篩選條件

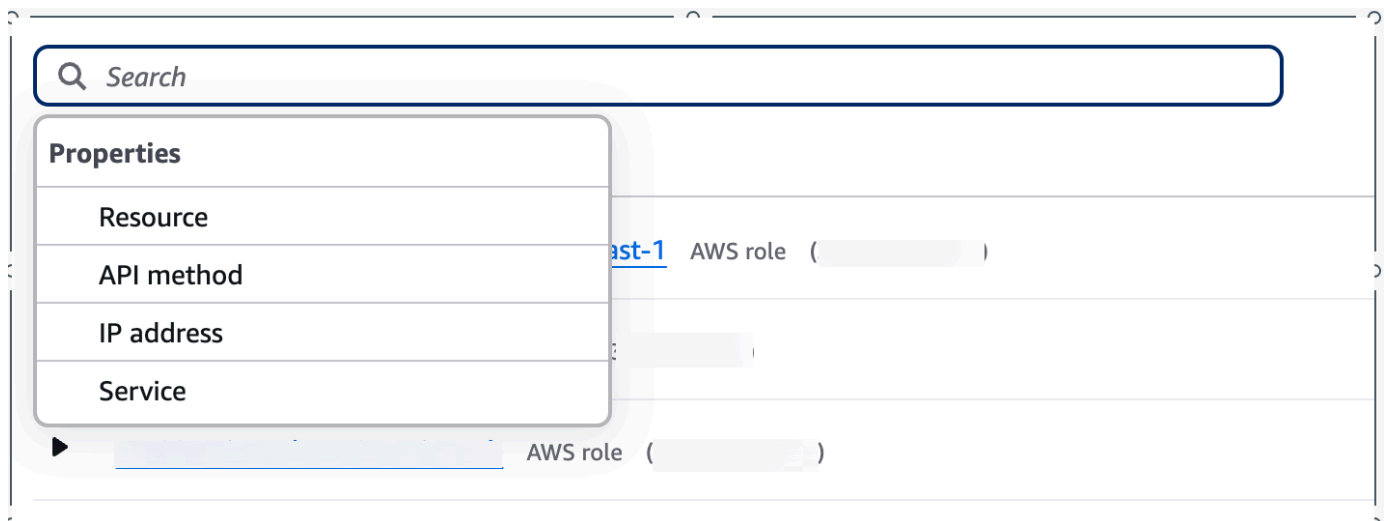
1. 選擇篩選條件方塊。
2. 從屬性中，選擇要用於篩選的內容。
3. 提供用於篩選的值。篩選條件支援部分值。例如，當您依 API 方法進行篩選時，如果篩選依據為 **Instance**，則結果會在其名稱內包含帶有 Instance 的任何 API 操作。所以 ListInstanceAssociations 和 UpdateInstanceInformation 兩者將匹配。

針對服務名稱、API 方法和 IP 地址，您可以指定值或選擇內建篩選條件。

針對通用 API 子字串，請選擇代表操作類型的子字串，例如 List、Create 或 Delete。每個 API 方法名稱都以操作類型開頭。

針對 CIDR 模式，您可以選擇僅包含公用 IP 地址、私有 IP 地址或符合特定 CIDR 模式的 IP 地址。

4. 選擇布林值選項 **#####**：包含 或 **!**：不包含；或 **API ##** 或 **IP ##** = 等於 或 **!**：不等於設定篩選條件。



若要移除篩選條件，請選擇右上角的 x 圖示。

若要清除所有篩選條件，請選擇清除篩選條件。

## 選取活動詳細資訊的時間範圍

當您首次顯示活動詳細資訊時，時間範圍是範圍時間或選取的時間間隔。您可以變更活動詳細資訊的時間範圍。

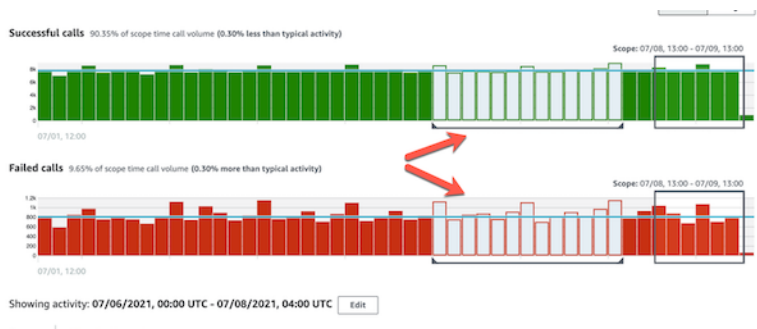
若要變更活動詳細資訊的時間範圍

1. 選擇編輯。
2. 在編輯時間範圍上，選擇要使用的開始和結束時間。

若要將時間範圍設定為設定檔的預設範圍時間，請選擇設定為預設範圍時間。

3. 選擇更新時間範圍。

活動詳細資訊的時間範圍會在設定檔面板圖表上反白顯示。



## 查詢原始日誌

Amazon Detective 與 Amazon Security Lake 集成，這意味著您可以查詢和擷取 Security Lake 存儲的原始日誌資料。如需此整合的詳細資訊，請參閱 [與 Security Lake 的偵測整合](#)。

使用此整合，您可以從 Security Lake 原生支援的以下來源收集和查詢日誌和事件。

- AWS CloudTrail 管理事件 1.0 版及更新版本
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌 1.0 版及更新版本
- Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌 2.0 版

### Note

在 Detective 內查詢原始資料日誌無須額外收費。其他 AWS 服務的使用費，包括 Amazon Athena，仍以公告費率計費。

## 若要查詢原始日誌

1. 選擇顯示範圍時間的詳細資訊。
2. 您可以在此開始查詢原始日誌。
3. 在原始日誌預覽資料表中，您可以檢視透過從 Security Lake 查詢資料擷取的日誌和事件。如需有關原始事件日誌的詳細資訊，您可以檢視 Amazon Athena 中顯示的資料。

您可以在查詢原始日誌資料表中取消查詢請求、在 Amazon Athena 中查看結果以及下載結果為逗號分隔值 (.csv) 設定檔。

如果您在 Detective 中查看日誌，但查詢未傳回任何結果，這可能因以下原因造成。

- 原始日誌可能會先在 Detective 中變成可用，然後才在 Security Lake 日誌表中顯示。請稍後再試。
- Security Lake 可能會缺少日誌。如果您等待了很久的時間，則表示 Security Lake 缺少日誌。請與您的 Security Lake 管理員聯絡以解決問題。

## 地理位置的活動詳細資訊

新觀察到的地理位置活動詳細資訊顯示了在範圍時間內從地理位置發出的 API 呼叫。API 呼叫包括從地理位置發出的所有呼叫。它們不限於使用調查結果或設定檔實體的呼叫。針對 S3 儲存貯體，活動呼叫指對 S3 儲存貯體進行的 API 呼叫。

Detective 會使用 MaxMind GeoIP 資料庫來決定請求的位置。MaxMind 在國家/地區層級報告非常高的資料準確性，但準確性會根據國家/地區和 IP 類型等因素而有所不同。如需 MaxMind 的詳細資訊，請參閱 [MaxMind IP 地理位置](#)。如果您認為任何 GeoIP 資料不正確，您可以在 [MaxMind Correct GeoIP2 Data](#) 向 Maxmind 提交更正請求。

API 呼叫會依發出呼叫的服務分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

若要顯示活動詳細資訊，請執行以下其中一項動作：

- 在地圖上，選擇一個地理位置。
- 在清單中，選擇地理位置的詳細資訊。

活動詳細資訊會取代地理位置清單。若要傳回地理位置清單，請選擇返回至所有結果。

請注意，自 2021 年 7 月 14 日起，Detective 開始儲存並顯示 API 呼叫的服務名稱。針對在該日期之前發生的活動，服務名稱為未知服務。

## 活動內容詳細資訊

每個標籤都會提供範圍時間內從地理位置發出的所有 API 呼叫的相關資訊。

針對每個 IP 地址、資源和 API 方法，清單會顯示成功和失敗的 API 呼叫次數。

活動詳細資訊包含以下標籤：

### 觀察到的 IP 地址

初始顯示用於從所選地理位置發出 API 呼叫的 IP 地址清單。

您可以展開每個 IP 地址，以顯示從該 IP 地址發出 API 呼叫的資源。清單會顯示資源名稱。若要查看主體 ID，請將滑鼠游標移至名稱上。

然後，您可以展開每個資源，以顯示該資源從該 IP 地址發出的特定 API 呼叫。API 呼叫會依發出呼叫的服務分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

IP address	Successful calls	Failed calls
10.0.0.0/24	27,564	2,453
aws-logs-911111111111-us-east-1	27,564	2,453
som	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
10.0.0.1	24,635	1,512
10.0.0.2	24,632	1,511

### Resource

初始顯示從選取的地理位置發出 API 呼叫的資源清單。清單會顯示資源名稱。若要查看主體 ID，請將滑鼠游標停放在名稱上。針對每個資源，資源標籤也會顯示相關 AWS 帳戶。

您可以展開每個使用者或角色，以顯示該資源發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。針對 S3 儲存貯體，服務始終為 Amazon S3。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。

然後，您可以展開每個 API 呼叫，以顯示資源發出 API 呼叫的來源 IP 地址清單。

Resource	Successful calls	Failed calls	Account ID
[Redacted] AWS role	189,097	17	[Redacted]
[Redacted] AWS role	49,267	3,023	[Redacted]
ssm	46,254	0	
UpdateInstanceInformation	25,932	0	
[Redacted]	12,968	0	
[Redacted]	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	

## 排序活動詳細資訊

您可以依任何清單欄排序活動詳細資訊。

當您使用第一欄位排序時，系統只會排序頂層清單。較低級別的清單始終按成功 API 呼叫的計數進行排序。

## 篩選活動詳細資訊

您可以使用篩選選項，來專注於活動詳細資訊中所表示的特定子集或活動方面。

在所有標籤上，您可以依第一欄位中的任何值篩選清單。

若要新增篩選條件

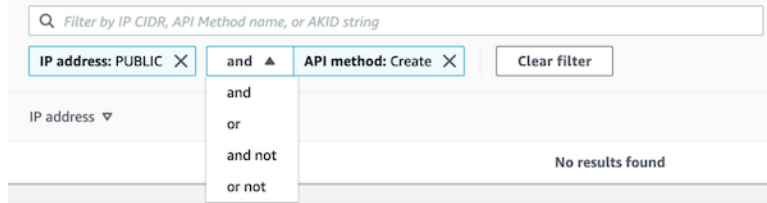
1. 選擇篩選條件方塊。
2. 從屬性中，選擇要用於篩選的內容。
3. 提供用於篩選的值。篩選條件支援部分值。例如，當您依 API 方法進行篩選時，如果篩選依據為 **Instance**，則結果會在其名稱內包含帶有 Instance 的任何 API 操作。所以 ListInstanceAssociations 和 UpdateInstanceInformation 兩者將匹配。

針對服務名稱、API 方法和 IP 地址，您可以指定值或選擇內建篩選條件。

針對通用 API 子字串，請選擇代表操作類型的子字串，例如 List、Create 或 Delete。每個 API 方法名稱都以操作類型開頭。

針對 CIDR 模式，您可以選擇僅包含公用 IP 地址、私有 IP 地址或符合特定 CIDR 模式的 IP 地址。

- 如果您有多個篩選條件，請選擇布林值選項來設定此類篩選條件的連線方式。



- 若要移除篩選條件，請選擇右上角的 x 圖示。
- 若要清除所有篩選條件，請選擇清除篩選條件。

## 整體 VPC 流量的活動詳細資訊

針對 EC2 執行個體，整體 VPC 流量的活動詳細資訊會顯示所選時間範圍內 EC2 執行個體和 IP 地址之間的互動。

針對 Kubernetes Pod，整體 VPC 流量會針對所有目的地 IP 地址，顯示 Kubernetes Pod 指派之 IP 地址的進出整體位元組量。在這一情況下 (`hostNetwork:true`)，Kubernetes Pod 的 IP 地址并非唯一地址。在此情況下，面板會顯示具有傳送至相同組態的其他 Pod 的流量，以及託管 Pod 的節點。

針對 IP 地址，整體 VPC 流量的活動詳細資訊會顯示 IP 地址與 EC2 執行個體在所選時間範圍內的互動。

若要顯示單一時間間隔的活動詳細資訊，請在圖表上選擇時間間隔。

若要顯示目前範圍時間的活動詳細資訊，請選擇顯示範圍時間的詳細資訊。

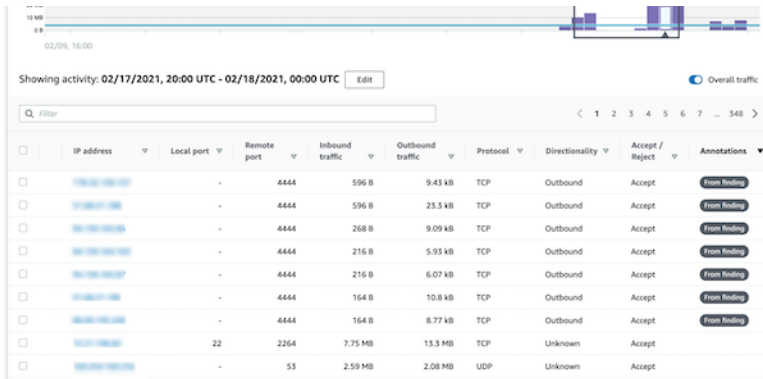
## 活動內容詳細資訊

內容反映在所選時間範圍內的活動。

針對 EC2 執行個體，活動詳細資訊包含 IP 地址、本機連接埠、遠端連接埠、通訊協定和方向的每個唯一組合的項目。

針對 IP 地址，活動詳細資訊包含 EC2 執行個體、本機連接埠、遠端連接埠、通訊協定和方向的每個唯一組合的項目。

每個項目都會顯示傳入流量、傳出流量以及存取要求是否已接受或拒絕。在調查結果設定檔上，注釋欄位會指出 IP 地址何時與目前調查結果相關。



	IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Annotations
<input type="checkbox"/>		-	4444	596 B	9.43 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	596 B	23.3 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	268 B	9.09 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	216 B	5.93 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	216 B	6.07 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	164 B	10.8 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		-	4444	164 B	8.77 kB	TCP	Outbound	Accept	From Endpoint
<input type="checkbox"/>		22	2264	7.75 MB	13.3 MB	TCP	Unknown	Accept	
<input type="checkbox"/>		-	53	2.59 MB	2.08 MB	UDP	Unknown	Accept	

## 排序活動詳細資訊

您可以依據資料表中的任何欄位來排序活動詳細資訊。

根據預設，活動詳細資訊會先依註釋排序，然後依傳入流量排序。

## 篩選活動詳細資訊

若要專注於特定活動，您可以依以下值篩選活動詳細資訊：

- IP 地址或 EC2 執行個體
- 本機或遠端連接埠
- Direction
- 通訊協定
- 請求是否被接受或拒絕

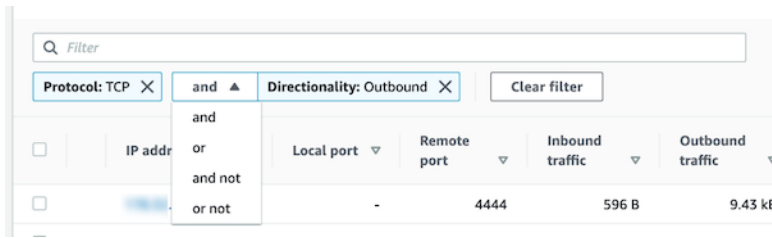
若要新增和移除篩選條件

1. 選擇篩選條件方塊。
2. 從屬性中，選擇要用於篩選的內容。
3. 提供用於篩選的值。篩選條件支援部分值。

若要依 IP 地址進行篩選，您可以指定值或選擇內建篩選條件。

針對 CIDR 模式，您可以選擇僅包含公用 IP 地址、私有 IP 地址或符合特定 CIDR 模式的 IP 地址。

4. 如果您有多個篩選條件，請選擇布林值選項來設定此類篩選條件的連線方式。



- 若要移除篩選條件，請選擇右上角的 x 圖示。
- 若要清除所有篩選條件，請選擇清除篩選條件。

## 選取活動詳細資訊的時間範圍

當您首次顯示活動詳細資訊時，時間範圍是範圍時間或選取的時間間隔。您可以變更活動詳細資訊的時間範圍。

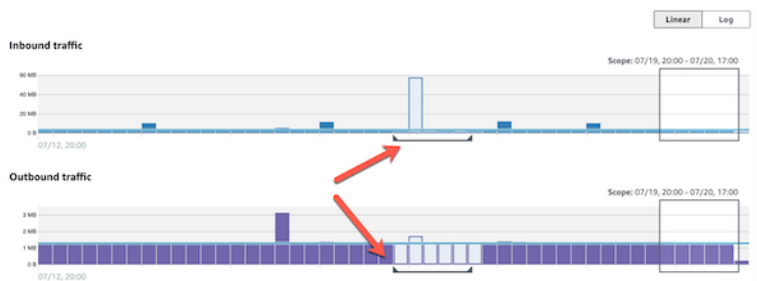
若要變更活動詳細資訊的時間範圍

- 選擇編輯。
- 在編輯時間範圍上，選擇要使用的開始和結束時間。

若要將時間範圍設定為設定檔的預設範圍時間，請選擇設定為預設範圍時間。

- 選擇更新時間範圍。

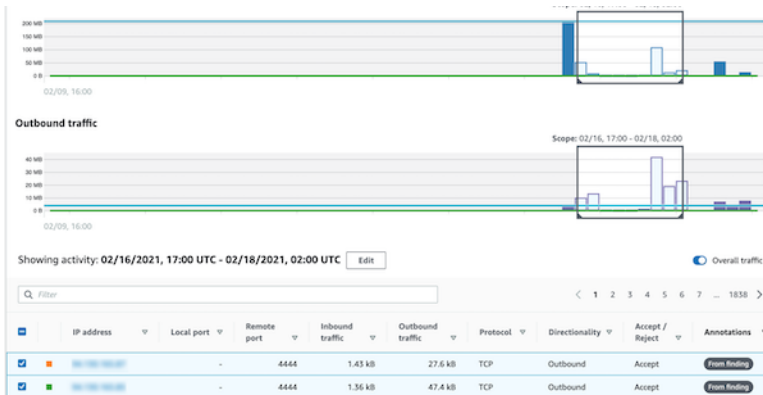
活動詳細資訊的時間範圍會在設定檔面板圖表上反白顯示。



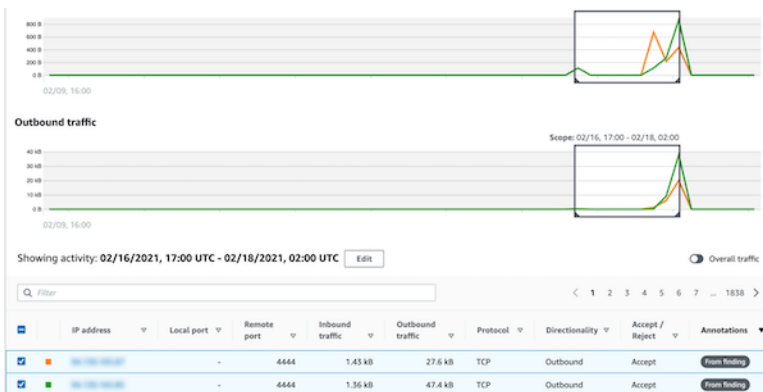
## 顯示所選列的流量

當您識別感興趣的資料列時，可以在主圖表上顯示此類資料列隨時間變化的流量。

針對每個要新增至圖表的資料列，勾選核取方塊。針對每個已選取的資料列，流量會在傳入或傳出圖表上顯示為一條線。



若要專注於所選項目的流量，您可以隱藏整體流量。若要顯示或隱藏整體流量，請切換整體流量。



## 顯示 EKS 叢集的 VPC 流量

Detective 可以為 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌提供可見度，此類日誌代表周遊 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集的流量。針對 Kubernetes 資源，VPC 流程日誌的內容取決於 EKS 叢集中部署的容器網路介面 (CNI)。

使用預設組態的 EKS 叢集會使用 Amazon VPC CNI 外掛程式。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的[管理 VPC CNI](#)。Amazon VPC CNI 外掛程式會使用 Pod 的 IP 地址傳送內部流量，並將來源 IP 地址翻譯為節點的 IP 地址以進行外部通訊。Detective 可以擷取內部流量並將其關聯到正確的 Pod，但無法對外部流量執行相同動作。

如果您希望 Detective 能夠對 Pod 的外部流量具有可見度，請啟用外部來源網路地址轉譯 (SNAT)。啟用 SNAT 具有限制和缺點。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的[適用於 Pod 的 SNAT](#)。

如果您使用不同的 CNI 外掛程式，Detective 針對使用 `hostNetwork:true` 的 Pod 有限可見度。針對此類 Pod，VPC 流程面板會顯示傳入 Pod IP 地址的所有流量。這包括傳入託管節點的流量以及傳入具有 `hostNetwork:true` 組態之節點上任何 Pod 的流量。

Detective 會針對以下 EKS 叢集組態，在 EKS Pod 的 VPC 流程面板中顯示流量：

- 在具有 Amazon VPC CNI 外掛程式的叢集中，任何在叢集的 VPC 內傳送流量的 Pod (具有組態 `hostNetwork:false`)。
- 在具有 Amazon VPC CNI 外掛程式和組態 `AWS_VPC_K8S_CNI_EXTERNALSNAT=true` 的叢集中，任何在叢集 VPC 外部傳送流量的 Pod (具有 `hostNetwork:false`)。
- 任何具有組態 `hostNetwork:true` 的 Pod。來自節點的流量會與來自具有組態 `hostNetwork:true` 之其他 Pod 的流量混合在一起。

Detective 不會在 VPC 流程面板中顯示以下項目的流量：

- 在具有 Amazon VPC CNI 外掛程式和組態 `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` 的叢集中，任何在叢集 VPC 外部傳送流量的 Pod (具有組態 `hostNetwork:false`)。
- 在無需針對 Kubernetes 使用 Amazon VPC CNI 外掛程式的叢集內，任何具有組態 `hostNetwork:false` 的 Pod。
- 傳送流量至相同節點中託管的另一個 Pod 的任何 Pod。

## 顯示共用 Amazon VPC 的 VPC 流程流量

Detective 可以深入查看共用 VPC 的 Amazon Virtual Private Cloud (Amazon VPC) Flow Logs：

- 如果 Detective 成員帳戶擁有共用 Amazon VPC，而且還有其他非 Detective 帳戶使用共用 VPC，則 Detective 會監控來自該 VPC 的所有流量，並且對 VPC 內的所有流量流程提供視覺效果。
- 如果您的共用 Amazon VPC 內有 Amazon EC2 執行個體，而共用 VPC 擁有者不是 Detective 成員，則 Detective 不會監控來自 VPC 的任何流量。如果您想要檢視 VPC 內的流量流程，則必須將 Amazon VPC 擁有者新增為 Detective 圖形的成員。

## 涉及 EKS 叢集的整體 Kubernetes API 活動

涉及 EKS 叢集的整體 Kubernetes API 活動的活動詳細資訊，顯示所選時間範圍內成功和失敗的 Kubernetes API 呼叫次數。

若要顯示單一時間間隔的活動詳細資訊，請在圖表上選擇時間間隔。

若要顯示目前範圍時間的活動詳細資訊，請選擇顯示範圍時間的詳細資訊。

## 活動詳細資訊的內容 (叢集、Pod、使用者、角色和角色工作階段)

針對叢集、Pod、使用者、角色或角色工作階段，活動詳細資訊包含以下資訊：

- 每個標籤都會提供在所選時間範圍內發出的 API 呼叫組的相關資訊。

針對叢集，API 呼叫發生在叢集內部。

針對 Pod，API 呼叫會以 Pod 為目標。

針對使用者、角色和角色工作階段，API 呼叫是由認證為該使用者、角色或角色工作階段的 Kubernetes 使用者發出。

- 針對每個項目，活動詳細資訊會顯示成功、失敗、未經授權和禁止的呼叫次數。
- 資訊包括 IP 地址、Kubernetes 呼叫類型、受呼叫影響的實體，以及進行呼叫的主體 (服務帳戶或使用者)。從活動詳細資訊中，您可以錨定至 IP 地址、主體和受影響實體的設定檔。

活動詳細資訊包含以下標籤：

### Subject

初始顯示用於進行 API 呼叫的服務帳戶和使用者清單。

您可以展開每個服務帳戶和使用者，以顯示帳戶或使用者從 IP 地址中 API 呼叫的清單。

然後，您可以展開每個 IP 地址，以顯示該帳戶或使用者從該 IP 地址進行的 Kubernetes API 呼叫。

展開 Kubernetes API 呼叫，查看 requestURI 以識別已完成的動作。

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

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
▶ 10.0.100.55 IP address	25,245	0	0	0

## IP Address (IP 地址)

初始顯示從 IP 地址中進行 API 呼叫的清單。

您可以展開每個呼叫，以顯示進行呼叫 Kubernetes 主體 (服務帳戶和使用者) 清單。

然後，您可以將每個主體展開到範圍時間內由主體發出的 API 呼叫類型清單。

展開 API 呼叫類型，查看 requestURI 以識別已完成的動作。

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

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 API 呼叫

初始顯示 Kubernetes API 呼叫動詞清單。

您可以展開每個 API 動詞以顯示與該動作相關聯的 requestURI。

然後，您可以展開每個 requestURI，以查看進行 API 呼叫的 Kubernetes 主體 (服務帳戶和使用者)。

展開主體以查看主體用來進行 API 呼叫的 IP。

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

## 排序活動詳細資訊

您可以依任何清單欄排序活動詳細資訊。

當您使用第一欄位排序時，系統只會排序頂層清單。較低級別的清單始終按成功 API 呼叫的計數進行排序。

## 篩選活動詳細資訊

您可以使用篩選選項，來專注於活動詳細資訊中所表示的特定子集或活動方面。

在所有標籤上，您可以依第一欄位中的任何值篩選清單。

## 選取活動詳細資訊的時間範圍

當您首次顯示活動詳細資訊時，時間範圍是範圍時間或選取的時間間隔。您可以變更活動詳細資訊的時間範圍。

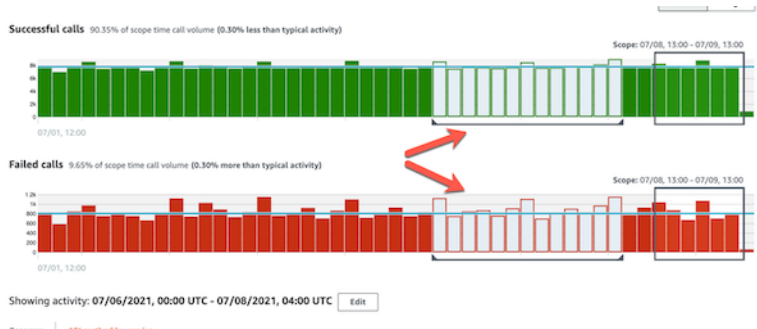
若要變更活動詳細資訊的時間範圍

1. 選擇編輯。
2. 在編輯時間範圍上，選擇要使用的開始和結束時間。

若要將時間範圍設定為設定檔的預設範圍時間，請選擇設定為預設範圍時間。

### 3. 選擇更新時間範圍。

活動詳細資訊的時間範圍會在設定檔面板圖表上反白顯示。



### 在調查期間使用設定檔面板指引

每個設定檔面板都旨在提供您進行調查和分析相關實體活動時出現的特定問題的答案。

為每個設定檔面板提供的指引可協助您找到答案。

設定檔面板指引以面板自身的單一句子開頭。本指引提供了面板上顯示的資料的簡要說明。

若要顯示面板的更多詳細指引，請從面板標題中選擇更多資訊。此擴充指引會在說明窗格中顯示。

該指引可以提供以下類型的資訊：

- 面板內容概觀
- 如何使用面板回答相關問題
- 根據答案建議的後續步驟

## 管理範圍時間

自訂用於限制實體設定檔上顯示資料的範圍時間。

實體設定檔上顯示的圖表、時間軸和其他資料都基於目前的範圍時間。範圍時間指一段時間內實體的活動摘要。這會出現在 Amazon Detective 主控台中每個設定檔的右上角。此類圖表、時間軸和其他視覺化上顯示的資料以範圍時間為基礎。針對某些設定檔面板，系統會在範圍時間之前和之後都會增加額外時間，以提供內容。在 Detective 中，預設會以 UTC 顯示所有時間戳記。您可以透過變更時間戳記偏好設定來選取當地時區。若要更新時間戳記偏好設定，請參閱 [the section called “設定時間戳記格式”](#)。

Detective 分析會在檢查異常活動時使用範圍時間。分析程序會在範圍時間內取得活動，然後將其與範圍時間前 45 天的活動進行比較。它還使用 45 天的時間範圍來產生活動的基準線。

在調查結果概觀中，範圍時間會反映調查結果的首次和末次觀察時間。如需調查結果概觀的詳細資訊，請參閱 [the section called “調查結果概觀”](#)。

當您進行調查時，您可以調整範圍時間。例如，如果原始分析基於一天的活動，您可能需要將其展開為一週或一個月。擴大的時間段可以幫助您更好地了解活動是否屬於正常模式或異常模式。

您也可以設定範圍時間，以符合目前實體的關聯調查結果。

當您變更範圍時間時，Detective 會重複其分析，並根據新範圍時間更新顯示的資料。

範圍時間不能短於一小時，不得超過一年。開始和結束時間必須相隔一小時。

## 設定特定開始和結束日期及時間

您可以從 Detective 主控台設定範圍時間的開始和結束日期。

若要設定新範圍時間的特定開始和結束時間

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在實體設定檔上，選擇範圍時間。
3. 在編輯範圍時間面板的開始下，選擇範圍時間的新開始日期和時間。針對新開始時間，您只選擇小時。
4. 在結束下，選擇範圍時間的新結束日期和時間。針對新結束時間，您只選擇小時。結束時間至少必須比開始時間晚一小時。
5. 完成編輯後，若要儲存變更並更新顯示的資料，請選擇更新範圍時間。

## 編輯範圍時間的時間長度

當您設定範圍時間長度時，Detective 會將範圍時間設定為從目前時間算起的时间長度。

若要編輯範圍時間的時間長度

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在實體設定檔上，選擇範圍時間。
3. 在編輯範圍時間面板的歷史旁邊，選擇範圍時間的時間長度。

指定時間範圍會更新開始和結束設定。

4. 完成編輯後，若要儲存變更並更新顯示的資料，請選擇更新範圍時間。

## 將範圍時間設定為調查結果時間範圍

每個調查結果都有相關的時間範圍，其將反映首次和末次觀察調查結果的時間。當您檢視調查結果概觀時，範圍時間會變更為調查結果時間範圍。

從實體設定檔中，您可以將範圍時間與關聯調查結果的時間範圍對齊。此舉可讓您可以調查在此期間發生的活動。

若要將範圍時間與調查結果時間範圍對齊，請在相關的調查結果面板上，選擇您要使用的調查結果。

Detective 會填入調查結果詳細資訊，並將範圍時間設定為調查結果時間範圍。

## 在摘要頁面上設定範圍時間

檢閱摘要頁面時，您可以調整範圍時間，以檢視過去 365 天內任何 24 小時時間範圍的活動。

若要在摘要頁面上設定範圍時間

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇摘要。
3. 在範圍時間面板的摘要旁邊，您可以變更開始日期和時間。開始時間必須在過去 365 天內。

當您變更開始日期和時間時，結束日期和時間會自動更新為您選擇的開始時間之後的 24 小時。

### Note

使用 Detective，您可以訪問長達一年的歷史事件資料。如需 Detective 中來源資料的詳細資訊，請參閱 [行為圖表中使用的來源資料](#)。

4. 完成編輯後，若要儲存變更並更新顯示的資料，請選擇更新範圍時間。

## 在 Detective 中檢視相關調查結果的詳細資訊

每個實體設定檔都包含一個相關的調查結果面板，其中列出目前範圍時間內涉及的實體的調查結果。表明某個一實體已遭入侵的跡象即為其參與了多項調查結果。調查結果的類型還可以提供有關要關注的活動類型的洞察。

關聯的調查結果面板會立即顯示在實體詳細資訊設定檔面板下方。

對於每項調查結果，資料表包含以下資訊：

- 調查結果標題，也是調查結果概觀的連結。
- 與調查結果相關聯的 AWS 帳戶，這也是帳戶設定檔的連結
- 調查結果類型
- 最早觀察到調查結果的時間
- 最近觀察到調查結果的時間
- 調查結果的嚴重性

若要顯示調查結果的調查結果詳細資訊，請選擇調查結果的按鈕。Detective 將填入頁面右側的調查結果詳細資訊面板。Detective 也會將範圍時間變更為調查結果時間範圍。此舉可讓您可以專注於在此期間發生的活動。

如果您從搜尋結果概觀導覽至實體設定檔，則系統會自動選取該調查結果，並顯示調查結果的詳細資訊。

若要從調查結果詳細資訊導覽回調查結果概觀，請選擇查看所有相關實體。

您也可以封存調查結果。如需詳細資訊，請參閱[封存 Amazon GuardDuty 調查結果](#)。

## 在 Detective 中檢視大量實體的詳細資訊

在[行為圖表](#)中，Amazon Detective 會追蹤實體之間的關係。例如，每個行為圖表都會追蹤 AWS 使用者何時建立 AWS 角色，以及 EC2 執行個體何時連線到 IP 地址。

當實體在一段時間內發生太多關係時，Detective 將無法儲存所有關係。如果在目前的範圍時間內發生此類情況，Detective 會通知您。Detective 還提供了大量實體的出現的清單。

### 什麼是大量實體？

在指定的時間間隔內，實體可能是極大數目連線的起點或目的地。例如，EC2 執行個體可能具有來自數百萬個 IP 地址的連線。

在每個時間間隔內，Detective 將保持其可以承載的連線數目的限制。如果某一實體超過該限制，則 Detective 會捨棄該時間間隔內的連線。

例如，假設每個時間間隔的限制為 100,000,000 個連線。如果 EC2 執行個體在一段時間間隔內連線到超過 100,000,000 個 IP 地址，則 Detective 會捨棄該時間間隔中的連線。

不過，您可能可以根據關係另一端的實體來分析該活動。為了繼續該範例，當 EC2 執行個體可能從數百萬個 IP 地址進行連線時，單一 IP 地址將連線到極少的 EC2 執行個體。每個 IP 地址設定檔都提供 IP 地址所連線的 EC2 執行個體的詳細資訊。

## 檢視設定檔上的大量實體通知

如果範圍時間包含大量實體的時間間隔，則 Detective 會在調查結果或實體設定檔的頂端顯示通知。針對調查結果設定檔，通知則針對涉及的實體。

該通知包括具有大量時間間隔的關係清單。每個清單項目都包含關係的說明和大量時間間隔的開始。

大量時間間隔可能是可疑活動的指標。若要了解同時發生了哪些其他活動，您可以將調查集中在大量時間間隔上。大量實體通知包括用於將範圍時間設置為該時間間隔的選項。

將範圍時間設定為大量時間間隔

1. 在大量實體通知中，選擇時間間隔。
2. 在快顯功能表上，選擇套用範圍時間。

## 檢視當前範圍時間的大量實體清單

大量實體頁面包含目前範圍時間內的大量時間間隔和實體清單。

若要顯示大量實體頁面

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇大量實體。

每個清單項目包含以下資訊：

- 大量時間間隔的開始
- 實體類型的識別符
- 關係的說明，例如「從 IP 地址連線的 EC2 執行個體」

您可以透過任何欄篩選和排序清單。您也可以導覽至涉及的實體的實體設定檔。

若要導覽至某一實體設定檔

1. 在大量實體清單中，選擇要從何列進行導覽。

## 2. 選擇檢視具有大量範圍時間的設定檔。

當您使用此選項導覽至實體設定檔時，範圍時間設定如下：

- 範圍時間在大量時間間隔之前的 30 天開始。
- 範圍時間在大量時間間隔結束時結束。

## 在 Detective 中搜尋調查結果或實體

使用 Amazon Detective 搜尋功能，您可以搜尋調查結果或實體。從搜尋結果中，您可以導覽至實體設定檔或調查結果概觀。如果搜尋傳回的結果超過 10,000 個，則系統只會顯示前 10,000 個結果。變更排序順序會變更傳回的結果。

您可以將搜尋結果匯出為逗號分隔值 (.csv) 設定檔。此檔案包含搜尋頁面中傳回的資料。資料會以逗號分隔值 (CSV) 格式匯出。匯出資料的檔案名稱遵循模式 `detective-page-panel-yyyy-mm-dd.csv` 格式。您可以使用其他支援 CSV 匯入 AWS 的服務、第三方應用程式或試算表程式來控制資料，藉此豐富您的安全調查。

### Note

如果匯出目前正在進行中，請等待匯出完成，然後再嘗試匯出其他資料。

## 完成搜尋

若要完成搜尋，請選擇要搜尋的實體類型。然後提供確切的識別符或包含萬用字元 \* 或 ? 的識別符。若要搜尋一系列 IP 地址，您也可以使用 CIDR 或 點符號。請參閱以下搜尋字串範例。

針對 IP 地址：

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

針對所有其他類型的實體：

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

- \*min

針對每個實體類型，支援以下識別符：

- 對於調查結果、調查結果識別符或調查結果 Amazon Resource Name ( ARN )。
- 對於 AWS 帳戶，則為 帳戶 ID。
- 對於 AWS 角色和 AWS 使用者，可能是主體 ID、名稱或 ARN。
- 對於容器叢集，叢集名稱或 ARN。
- 針對容器映像，則為儲存庫或容器映像的完整摘要。
- 對於容器 Pod 或任務，Pod 名稱或 Pod UID的。
- 對於EC2執行個體、執行個體識別符或 ARN。
- 針對調查結果群組，則為調查結果群組識別符。
- 對於 IP 地址，中的地址CIDR或點符號。
- 針對 Kubernetes 主體 (服務帳戶或使用者)，則為名稱。
- 針對角色工作階段，您可以使用以下任一值來搜尋：
  - 角色工作階段識別符。

角色工作階段識別符使用 `<rolePrincipalID>:<sessionName>` 格式。

請見此處範例：AROA12345678910111213:MySession。

- 角色工作階段 ARN
- 工作階段名稱
- 所擔任角色的主體 ID
- 擔任的角色名稱
- 對於 S3 儲存貯體，儲存貯體名稱或儲存貯體 ARN。
- 若為聯合身分使用者，則為主體 ID 或使用者名稱。主體 ID 為 `<identityProvider>:<username>` 或 `<identityProvider>:<audience>:<username>`。
- 針對使用者代理程式，則為使用者代理程式名稱。

若要搜尋調查結果或實體

1. 登入 AWS 管理主控台。然後在 開啟 Detective 主控台<https://console.aws.amazon.com/detective/>。

2. 在導覽窗格中，選擇搜尋。
3. 從選擇類型功能表中，選擇您要尋找的項目類型。

請注意，當您選擇使用者時，您可以搜尋 AWS 使用者或聯合身分使用者。

資料中的範例包含行為圖表資料中已選取類型的識別符範例集。若要顯示其中某一範例的設定檔，請選擇其識別符。

4. 輸入要搜尋的確切識別符或包含萬用字元的識別符。  
搜尋不區分大小寫。
5. 選擇搜尋或按 Enter 鍵。

## 對搜尋結果進行排序

當您完成搜尋後，Detective 會顯示最多 10,000 個符合結果的清單。針對使用唯一識別符的搜尋，只有一個相符結果。

從結果中，若要導覽至實體設定檔或調查結果概觀，請選擇識別符。

對於調查結果、角色、使用者和 EC2 執行個體，搜尋結果包含相關聯的帳戶。若要導覽至帳戶的設定檔，請選擇帳戶識別符。

## 搜尋疑難排解

如果 Detective 無法找到調查結果或實體，請先檢查您輸入的識別符是否正確。如果識別符正確，您還可以檢查以下內容。

- 調查結果或實體是否屬於行為圖表中已啟用的成員帳戶？如果關聯帳戶未以成員帳戶的身份邀請加入行為圖表，則行為圖表不會包含該帳戶的資料。

如果受邀成員帳戶不接受邀請，則行為圖表不會包含該帳戶的資料。

- 針對某一調查結果，是否對其封存？Detective 不會從 Amazon 接收封存的調查結果 GuardDuty。
- 在 Detective 開始將資料擷取至行為圖表之前，該調查結果或實體是否已出現？如果 Detective 所擷取的資料中無調查結果或實體，則行為圖表不會包含該調查結果的資料。
- 調查結果或實體是否來自正確區域？每個行為圖表都是特有的 AWS 區域。行為圖表不包含來自其他區域的資料。

# 在 Detective 中管理帳戶

當帳戶啟用 Detective 時，它會成為行為圖表的管理員帳戶，並為行為圖表選擇成員帳戶。管理員帳戶可以邀請帳戶加入行為圖表。當帳戶接受邀請時，Detective 會啟用該帳戶作為成員帳戶。透過邀請加入的成員帳戶可將自己從行為圖表中移除。

當帳戶作為成員帳戶啟用時，Detective 會開始提取成員帳戶的資料並擷取到該行為圖表中。

每個行為圖表都包含來自一個或多個帳戶的資料。行為圖表最多可以有 1,200 個成員帳戶。

如果您與整合 AWS Organizations，則組織管理帳戶會為組織指定 Detective 管理員帳戶。然後，該 Detective 管理員帳戶會成為組織行為圖表的管理員帳戶。Detective 管理員帳戶可以在組織行為圖表中將任何組織帳戶作為成員帳戶啟用。組織帳戶無法將自己從組織行為圖表中移除。

Detective 會就其對各行為圖表提供的資料向每個帳戶收取費用。如需追蹤行為圖表中每個帳戶的資料量的資訊，請參閱[預測和監控 Amazon Detective 成本](#)。

## 目錄

- [Detective 中的帳戶限制和建議](#)
- [使用 Organizations 管理行為圖表帳戶](#)
- [指定組織的 Detective 管理員](#)
- [帳戶的可用動作](#)
- [檢視帳戶清單](#)
- [以 Detective 成員帳戶管理組織帳戶](#)
- [在 Detective 中管理受邀成員帳戶](#)
- [針對成員帳戶：管理行為圖表邀請和成員資格](#)
- [帳戶動作對行為圖表的影響](#)
- [使用 Detective Python 指令碼來管理帳戶](#)

## Detective 中的帳戶限制和建議

在 Amazon Detective 中管理帳戶時，請注意以下限制與建議。

### 成員帳戶的數目上限

Detective 允許在每個行為圖表中最多容納 1,200 個成員帳戶。

如果您使用 AWS Organizations 來管理帳戶，根據預設，Detective 會在帳戶管理頁面上顯示最多 5000 個成員帳戶。如果您想要檢視所有帳戶，請選取載入所有帳戶。傳回所有結果可能需要幾分鐘的時間。

## 帳戶和區域

如果您使用 AWS Organizations 來管理帳戶，組織管理帳戶會為組織指定 Detective 管理員帳戶。該 Detective 管理員帳戶會成為組織行為圖表的管理員帳戶。

所有區域的 Detective 管理員帳戶必須相同。組織管理帳戶會分別在每個區域中指定 Detective 管理員帳戶。Detective 管理員帳戶也會分別管理每個區域中的組織行為圖表和成員帳戶。

針對透過邀請建立的成員帳戶，系統只會在邀請寄出的區域建立管理員與成員關聯。管理員帳戶必須在每個區域中啟用 Detective，並且在每個區域中都有獨立的行為圖表。然後，管理員帳戶會邀請每個帳戶在該區域關聯為成員帳戶。

一個帳戶可以是相同區域中多個行為圖表的成員帳戶。一個帳戶在每個區域只能成為一個行為圖表的管理員帳戶。帳戶可以是不同區域的管理員帳戶。

## 管理員帳戶與 Security Hub CSPM 和 GuardDuty 的一致性

為了確保與 AWS Security Hub CSPM 和 Amazon GuardDuty 的整合能夠順利運作，我們建議所有這些服務中的管理員帳戶都是相同的帳戶。

請參閱 [the section called “建議與 GuardDuty 和 對齊 AWS Security Hub CSPM”](#)。

## 授予管理員帳戶所需的許可

為了確保管理員帳戶具有管理其行為圖表所需的許可，將 [AmazonDetectiveFullAccess](#) 受管政策附加到 IAM 主體。

## 反映組織在 Detective 中的更新

對組織的變更不會立即反映在 Detective 中。

針對大多數變更 (例如新增和已移除的組織帳戶)，Detective 最多可能需要一小時才會收到通知。

變更組織中指定的 Detective 管理員帳戶所需的傳播時間較短。

## 使用 Organizations 管理行為圖表帳戶

您可能具有現有行為圖表，其中包含接受手動邀請的成員帳戶。如果您已註冊 AWS Organizations，請使用下列步驟使用 Organizations 來啟用和管理成員帳戶，而不是使用手動邀請程序：

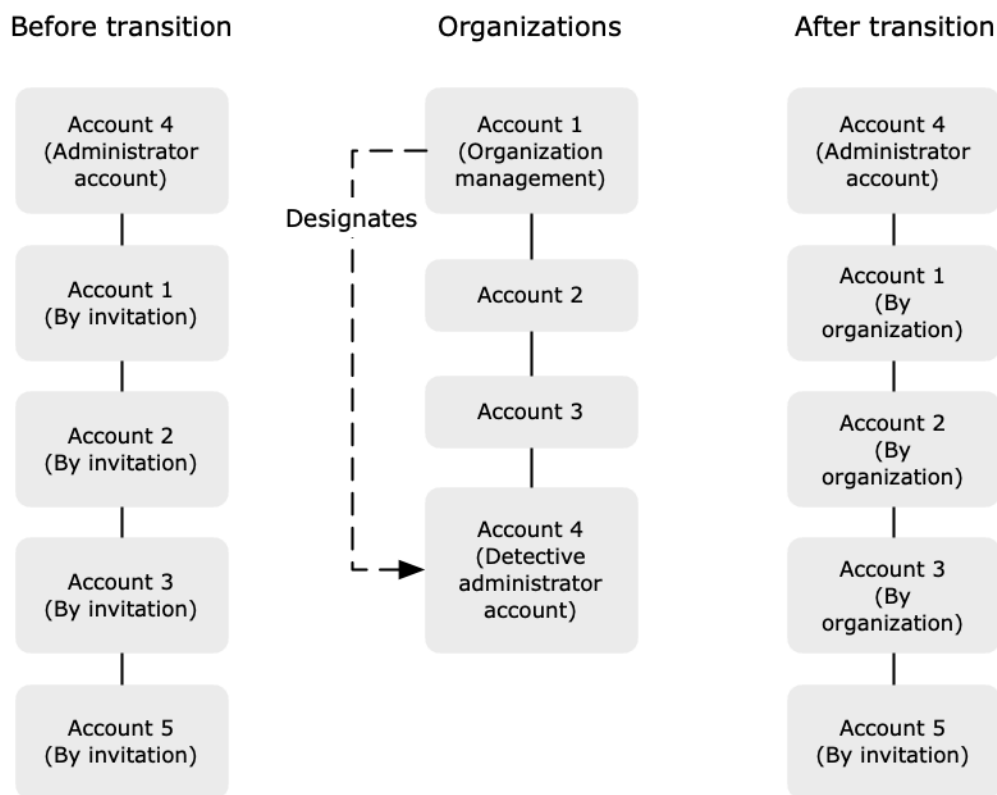
1. [為您的組織指定 Detective 管理員帳戶](#)。此舉會建立組織行為圖表。

如果 Detective 管理員帳戶已有行為圖表，則該行為圖表會成為組織行為圖表。

2. [在組織行為圖表中自動將新組織帳戶作為成員帳戶啟用](#)。

如果組織行為圖表具有組織帳戶的現有成員帳戶，則會自動啟用此類帳戶。

下圖顯示轉換前的行為圖表結構、組織中的組態以及轉換後的行為圖表帳戶結構的概觀。



### 為組織指定 Detective 管理員帳戶

組織管理帳戶會指定組織的 Detective 管理員帳戶。請參閱 [the section called “指定 Detective 管理員帳戶”](#)。

為簡化轉換，Detective 建議您選擇目前的管理員帳戶作為組織的 Detective 管理員帳戶。

如果組織中針對 Detective 有委派的管理員帳戶，則您必須使用該帳戶或組織管理帳戶作為 Detective 管理員帳戶。

否則，當您首次指定非組織管理帳戶的 Detective 管理員帳戶時，Detective 會呼叫組織，使該帳戶成為 Detective 的委派管理員帳戶。

## 啟用組織帳戶作為成員帳戶

Detective 的委派管理員帳戶是 Detective 行為圖表的管理員帳戶。Detective 管理員帳戶選擇要在組織行為圖表中作為成員帳戶啟用的組織帳戶。請參閱 [the section called “管理組織成員帳戶”](#)。

在帳戶頁面上，Detective 管理員帳戶可查看組織中的所有帳戶。

如果 Detective 管理員帳戶已經成為行為圖表的管理員帳戶，則該行為圖表會成為組織行為圖表。在該行為圖表中已經成為成員帳戶的組織帳戶，會自動作為成員帳戶啟用。其他組織帳戶的狀態為非成員。

組織帳戶具有依組織類型，即使它們先前為受邀成員帳戶。

不屬於組織的成員帳戶具有依邀請類型。

帳戶管理頁面也提供自動啟用新組織帳戶選項，以便在新增帳戶至組織時自動啟用新帳戶。請參閱 [the section called “啟用新的組織帳戶”](#)。該選項最初處於關閉狀態。

當 Detective 管理員帳戶首次顯示帳戶管理頁面時，系統會顯示包含啟用所有組織帳戶按鈕的訊息。當您選擇啟用所有組織帳戶時，Detective 會執行以下動作：

- 將所有目前組織帳戶作為成員帳戶啟用。
- 打開自動啟用新組織帳戶的選項。

成員帳戶清單上也有啟用所有組織帳戶選項。

## 指定組織的 Detective 管理員

在組織行為圖表中，Detective 管理員帳戶會管理所有組織帳戶的行為圖表成員資格。

Detective 管理員帳戶的管理方式 – 組織管理帳戶會為每個組織指定 Detective 管理員帳戶 AWS 區域。

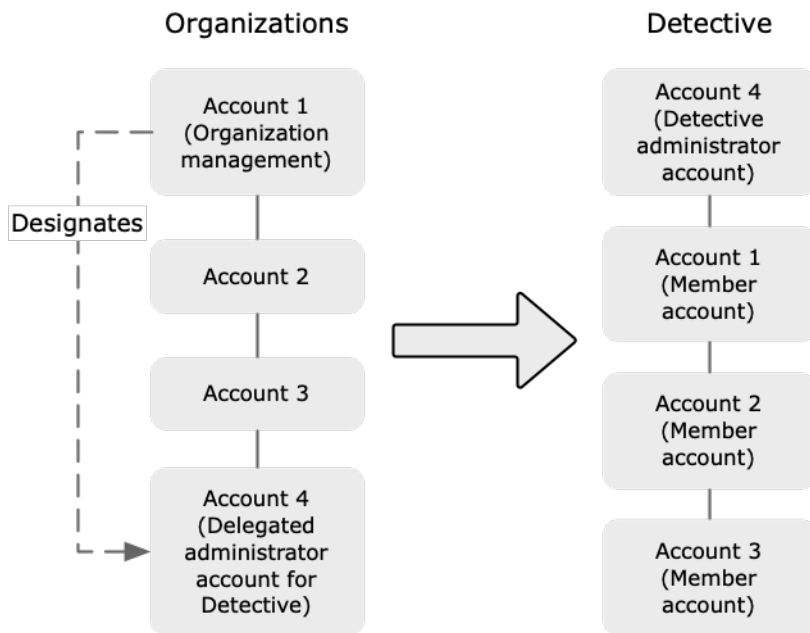
將 Detective 管理員帳戶設定為委派管理員帳戶 – Detective 管理員帳戶也會成為其中 Detective 的委派管理員帳戶 AWS Organizations。如果組織管理帳戶將自己指定為 Detective 管理員帳戶，則存在例外情況。組織管理帳戶無法成為組織中委派的管理員。

在組織中設定委派的管理員帳戶之後，組織管理帳戶只能選擇委派的管理員帳戶或他們自己的帳戶作為 Detective 管理員帳戶。我們建議您在所有區域中選擇委派的管理員帳戶。

建立和管理組織行為圖表 – 當組織管理帳戶選擇 Detective 管理員帳戶時，Detective 會為該帳戶建立新的行為圖表。該行為圖表是組織行為圖表。

如果 Detective 管理員帳戶是現有行為圖表的管理員帳戶，則該行為圖表會成為組織行為圖表。

Detective 管理員帳戶會在組織行為圖表中選擇要啟用的組織帳戶做為成員帳戶。



Detective 管理員帳戶也可以傳送邀請至不屬於組織的帳戶。如需詳細資訊，請參閱[the section called “管理組織成員帳戶”](#)及[the section called “管理受邀成員帳戶”](#)。

設定 Detective 管理員帳戶所需的許可 – 為確保組織管理帳戶能夠設定 Detective 管理員帳戶，您可以將 [AmazonDetectiveOrganizationsAccess 受管政策](#) 連接到您的 AWS Identity and Access Management (IAM) 實體。

## 指定 Detective 管理員

組織管理帳戶可以使用 Detective 主控台來指定 Detective 管理員帳戶。

您無需啟用 Detective 即可管理 Detective 管理員帳戶。您可以從啟用 Detective 頁面管理 Detective 管理員帳戶。

### Enable Detective page (Console)

若要從啟用 Detective 頁面指定 Detective 管理員，請遵循下列步驟。

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 選擇開始使用。
3. 在管理員帳戶所需的許可面板中，為您選擇的帳戶授予必要的許可，以便他們能夠以 Detective 管理員的身分操作，並具有對 Detective 中所有動作的完整存取許可。若要以管理員身分操作，建議將 AmazonDetectiveFullAccess 政策附加至主體。
4. 選擇從 IAM 附加政策，直接在 IAM 主控台中檢視建議的政策。
5. 根據您是否在 IAM 主控台中擁有許可，執行以下步驟：
  - 如果您有在 IAM 主控台中操作的許可，請將建議的政策附加到您用於 Detective 的主體。
  - 如果您沒有在 IAM 主控台中操作的許可，請複製政策的 Amazon Resource Name (ARN)，並將其提供給 IAM 管理員。然後，他們可以代表您附加政策。
6. 在委派管理員下，選擇 Detective 管理員帳戶。

可用的選項取決於您是否擁有組織中 Detective 的委派管理員帳戶。

- 如果您沒有組織中 Detective 的委派管理員帳戶，請輸入帳戶的帳戶識別符，將其指定為 Detective 管理員帳戶。

在手動邀請程序中，您可能已有現有管理員帳戶和行為圖表。如果的確如此，我們建議您將該帳戶指定為 Detective 管理員帳戶。

如果您在 Organizations for Amazon GuardDuty AWS Security Hub CSPM 或 Amazon Macie 中有委派管理員帳戶，則 Detective 會提示您選取其中一個帳戶。您也可以輸入不同的帳戶。

- 如果您確實擁有組織中 Detective 的委派管理員帳戶，系統會提示您選擇該帳戶或您的帳戶。我們建議您在所有區域中選擇委派的管理員帳戶。

## 7. 選擇委派。

如果您已啟用 Detective，或者是現有行為圖表中的成員帳戶，則您可以從一般頁面指定 Detective 管理員帳戶。

### General page (Console)

若要從一般頁面指定 Detective 管理員，請遵循下列步驟。

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，於設定下選擇通用。

3. 在受管政策面板中，您可進一步了解 Detective 支援的所有受管政策。您可以根據您希望使用者在 Detective 中執行的動作，向帳戶授予必要的許可。若要以管理員身分操作，建議將 AmazonDetectiveFullAccess 政策附加至主體。
4. 根據您是否在 IAM 主控台中擁有許可，執行以下步驟：
  - 如果您有在 IAM 主控台中操作的許可，請將建議的政策附加到您用於 Detective 的主體。
  - 如果您沒有在 IAM 主控台中操作的許可，請複製政策的 Amazon Resource Name (ARN)，並將其提供給 IAM 管理員。然後，他們可以代表您附加政策。

可用的選項取決於您是否擁有組織中 Detective 的委派管理員帳戶。

- 如果您沒有組織中 Detective 的委派管理員帳戶，請輸入帳戶的帳戶識別符，將其指定為 Detective 管理員帳戶。

在手動邀請程序中，您可能已有現有管理員帳戶和行為圖表。如果的確如此，則我們建議您將該帳戶指定為 Detective 管理員帳戶。

如果您在 Organizations for Amazon GuardDuty AWS Security Hub CSPM 或 Amazon Macie 中有委派管理員帳戶，則 Detective 會提示您選取其中一個帳戶。您也可以輸入不同的帳戶。

- 如果您確實擁有組織中 Detective 的委派管理員帳戶，系統會提示您選擇該帳戶或您的帳戶。我們建議您在所有區域中選擇委派的管理員帳戶。

## 5. 選擇委派。

### Detective API, AWS CLI

若要指定 Detective 管理員帳戶，您可以使用 API 呼叫或 AWS Command Line Interface。您必須使用組織的管理帳戶憑證。

如果您已經擁有組織中 Detective 的委派管理員帳戶，則您必須選擇該帳戶或您的帳戶，我們建議您選擇委派的管理員帳戶。

#### 指定 Detective 管理員帳戶 (Detective API AWS CLI)

- Detective API：使用 [EnableOrganizationAdminAccount](#) 操作。您必須提供 Detective 管理員 AWS 帳戶的帳戶識別符。若要取得帳戶識別符，使用 [ListOrganizationAdminAccounts](#) 操作。
- AWS CLI：在命令列中執行 [enable-organization-admin-account](#) 命令。

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

## 範例

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

## 移除 Detective 管理員帳戶

組織管理帳戶可以移除區域中目前的 Detective 管理員帳戶。當您移除 Detective 管理員帳戶時，Detective 只會將其從目前的區域中移除。它不會變更組織中的委派管理員帳戶。

當組織管理帳戶移除區域中的 Detective 管理員帳戶時，Detective 會刪除組織行為圖表。已移除的 Detective 管理員帳戶將停用 Detective。

若要移除 Detective 目前委派的管理員帳戶，您可以使用組織 API。當您移除組織中 Detective 的委派管理員帳戶時，Detective 會刪除所有組織行為圖表，其中委派的管理員帳戶是 Detective 管理員帳戶。將組織管理帳戶作為 Detective 管理員帳戶的組織行為圖表不會受到影響。

### Console

您可以從 Detective 主控台移除 Detective 管理員帳戶。

當您移除 Detective 管理員帳戶時，系統會停用該帳戶的 Detective，並且會刪除組織行為圖表。Detective 管理員帳戶僅會在目前區域中移除。

#### Important

移除 Detective 管理員帳戶不會影響組織中委派的管理員帳戶。

若要移除 Detective 管理員帳戶 (啟用 Detective 頁面)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 選擇開始使用。
3. 在委派的管理員下，選擇停用 Amazon Detective。
4. 在確認對話方塊上，輸入 **disable**，然後選擇停用 Amazon Detective。

## 若要移除 Detective 管理員帳戶 (一般頁面)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，於設定下選擇通用。
3. 在委派的管理員下，選擇停用 Amazon Detective。
4. 在確認對話方塊上，輸入 **disable**，然後選擇停用 Amazon Detective。

## Detective API, AWS CLI

若要移除 Detective 管理員帳戶，您可以使用 API 呼叫或 AWS CLI。您必須使用組織的管理帳戶憑證。

當您移除 Detective 管理員帳戶時，系統會停用該帳戶的 Detective，並且會刪除組織行為圖表。

### Important

移除 Detective 管理員帳戶不會影響組織中委派的管理員帳戶。

## 若要移除 Detective 管理員帳戶 (Detective API) AWS CLI

- Detective API：使用 [DisableOrganizationAdminAccount](#) 操作。

當您使用 Detective API 移除 Detective 管理員帳戶時，只會在發出 API 呼叫或指令的區域中移除該帳戶。

- AWS CLI：在命令列中執行 [disable-organization-admin-account](#) 命令。

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

## 移除委派管理員帳戶

移除 Detective 管理員帳戶並不會自動移除組織中委派的管理員帳戶。若要移除 Detective 的委派管理員帳戶，您可以使用組織 API。

當您移除委派的管理員帳戶時，這會刪除委派管理員帳戶為 Detective 管理員帳戶的所有組織行為圖表。此舉還會停用此類區域中帳戶的 Detective。

## 若要移除委派管理員帳戶 (Organizations API) AWS CLI

- 組織 API：使用 [DeregisterDelegatedAdministrator](#) 操作。您必須提供 Detective 管理員帳戶的帳戶識別符，以及 Detective 的服務主體，即 `detective.amazonaws.com`。
- AWS CLI：在命令列中執行 [deregister-delegated-administrator](#) 命令。

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

### 範例

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

## 帳戶的可用動作

管理員和成員帳戶可以存取以下 Detective 動作。在資料表中，值具有以下含義：

- 任何：帳戶可對同一 Detective 管理員帳戶下的所有帳戶執行動作。
- 自我：帳戶只能在自己的帳戶上執行動作。
- 破折號 (-)：帳戶無法執行動作。

在組織行為圖表中，Detective 管理員帳戶會判斷要將哪些組織帳戶作為成員帳戶啟用。他們可以設定 Detective，使其自動將新組織帳戶作為成員帳戶啟用，或手動啟用組織帳戶。

管理員帳戶可以在行為圖表中邀請帳戶成為成員帳戶。當成員帳戶接受邀請並啟用時，Amazon Detective 就會開始擷取成員帳戶的資料，並將其擷取到該行為圖表中。

對於非組織行為圖表的行為圖表，所有成員帳戶均為受邀帳戶。

以下資料表反映管理員帳戶與成員帳戶的預設許可。您可以使用自訂IAM原則來限制進一步存取 Detective 功能和功能。

動作	管理員帳戶 (組織)	管理員帳戶 (邀請)	成員 (組織)	成員 (邀請)
檢視帳戶	任何	任何	自我 (檢視管理員帳戶)	自我 (檢視管理員帳戶)
移除成員帳戶	任何 移除受邀帳戶 組織帳戶已解除關聯	任何	–	自我
新增或移除選用的資料來源套件	任何 (設定適用於所有成員帳戶)	任何 (設定適用於所有成員帳戶)	–	–
停用 Detective	自我	自我	–	–
檢視行為圖表資料	任何	任何	–	–
啟用或停用選用的資料來源套件	全部	全部	–	–

## 檢視帳戶清單

管理員帳戶可以使用 Detective 主控台或 API 來檢視帳戶清單。清單包括：

- 管理員帳戶受邀加入行為圖表的帳戶。此類帳戶具有依邀請類型。
- 針對組織行為圖表，則為組織中所有帳戶。此類帳戶的類型為依組織。

結果不包括拒絕邀請的受邀成員帳戶，或從行為圖表中移除的管理員帳戶。清單只包含以下狀態的帳戶。

### 正在進行中的驗證

針對受邀帳戶，Detective 會在傳送邀請之前驗證帳戶電子郵件地址。

針對組織帳戶，Detective 會驗證帳戶是否屬於組織。Detective 也會驗證啟用此帳戶的 Detective 管理員帳戶。

### 驗證失敗

驗證失敗。邀請未傳送，或組織帳戶未啟用為成員。

### 已邀請

針對受邀帳戶。邀請已傳送，但成員帳戶尚未回應。

### 非成員

針對組織行為圖表中的組織帳戶。組織帳戶目前非成員帳戶。它不會將資料提供至組織行為圖表。

### 已啟用

針對受邀帳戶，成員帳戶接受邀請，並將資料提供至行為圖表。

針對組織行為圖表中的組織帳戶，Detective 管理員帳戶會將帳戶啟用為成員帳戶。帳戶將資料提供至組織行為圖表。

### 未啟用

針對受邀帳戶，成員帳戶已接受邀請，但無法啟用。

針對組織行為圖表中的組織帳戶，Detective 管理員帳戶會嘗試啟用帳戶，但該帳戶無法得到啟用。

對於受邀帳戶，Detective 會檢查成員帳戶的數量。行為圖表中成員帳戶的數目上限為 1,200。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。

Detective 會檢查您的資料磁碟區是否在 Detective 配額內。流入行為圖表的資料量必須小於 Detective 允許的最大值。如果目前擷取的磁碟區超過行為圖表資料磁碟區每天 10 TB 的限制，則 Detective 將不會允許您新增其他成員帳戶。

## 列出帳戶 (主控台)

您可以使用 AWS 管理主控台 查看和篩選帳戶清單。

### 若要顯示帳戶清單 (主控台)

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。

成員帳戶清單包含以下帳戶：

- 您的帳戶
- 您邀請向行為圖表提供資料的帳戶
- 在組織行為圖表中，則為所有組織帳戶

針對每個帳戶，清單都會顯示以下資訊：

- AWS 帳戶識別符。
- 針對組織帳戶，則為帳戶名稱。
- 帳戶類型 (按邀請或按組織)。
- 針對受邀帳戶，則為帳戶根使用者電子郵件地址。
- 帳戶狀態。
- 帳戶的每日資料量。Detective 無法擷取未啟用為成員帳戶的帳戶資料量。
- 上次更新帳戶狀態的日期。

您可以使用資料表頂端的標籤，根據成員帳戶狀態篩選清單。每個標籤都會顯示相符成員帳戶的數目。

- 選擇全部以檢視所有成員帳戶。
- 選擇已啟用以檢視狀態為已啟用的帳戶。
- 選擇未啟用以檢視狀態為已啟用以外的帳戶。

您還可以將其他篩選條件添加到成員帳戶清單中。

若要將篩選條件新增至行為圖表中的帳戶清單 (主控台)

1. 選擇篩選條件方塊。
2. 選擇您要用於篩選清單的欄位：
3. 針對指定欄位，選擇要用於篩選的值。
4. 若要移除篩選條件，選擇右上角的 x 圖示。
5. 如需更新清單以包含最新狀態資訊，則請選擇右上角的重新整理圖示。

## 列出您的成員帳戶 (Detective API AWS CLI)

您可以使用 API 呼叫或 AWS Command Line Interface 檢視行為圖表中的成員帳戶清單。

若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

### 擷取成員帳戶的清單 (Detective API AWS CLI)

- Detective API：使用 [ListMembers](#) 操作。若要識別預期行為圖表，指定行為圖表 ARN。

請注意，針對組織行為圖表，[ListMembers](#) 不會傳回您未啟用為成員帳戶或與行為圖表解除關聯的組織帳戶。

- AWS CLI：在命令列中執行 [list-members](#) 命令。

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

範例：

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

### 若要擷取行為圖表中特定成員帳戶的詳細資訊 (Detective API AWS CLI)

- Detective API：使用 [GetMembers](#) 操作。指定行為圖表標 ARN 和成員帳戶的帳戶識別符清單。
- AWS CLI：在命令列中執行 [get-members](#) 命令。

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

範例：

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

## 以 Detective 成員帳戶管理組織帳戶

在組織行為圖表中，Detective 管理員帳戶會判斷要將哪些組織帳戶作為成員帳戶啟用。根據預設，新組織帳戶不會啟用為成員帳戶。他們的狀態為非成員。Detective 管理員可以將 Detective 設定自動將新組織帳戶作為成員帳戶在組織管理圖表中啟用。

Detective 管理員可以設定 Detective，以自動將新組織帳戶啟用為成員帳戶。當您選擇自動啟用組織帳戶時，Detective 會在將新帳戶新增到組織時開始將新帳戶作為成員帳戶啟用。Detective 不會啟用尚未啟用的現有組織帳戶。

如果您不想自動啟用新的組織帳戶，Detective 可以手動將組織帳戶啟用為成員帳戶。他們也可以手動啟用取消關聯的組織帳戶。如果組織行為圖表已啟用最多 1,200 個帳戶，Detective 管理員就無法將組織帳戶啟用為成員帳戶。在此情況下，組織帳戶狀態仍然為非成員。

Detective 管理員也可以取消組織帳戶與組織行為圖表的關聯。若要停止從組織行為圖表中的組織帳戶擷取資料，您可以取消與帳戶的關聯。該帳戶的現有資料會保留在行為圖表中。

### 目錄

- [將新組織帳戶啟用為 Detective 成員帳戶](#)
- [將組織帳戶啟用為 Detective 成員帳戶](#)
- [將組織帳戶取消關聯為 Detective 成員帳戶](#)

## 將新組織帳戶啟用為 Detective 成員帳戶

Detective 管理員可以將 Detective 設定自動將新組織帳戶作為成員帳戶在組織管理圖表中啟用。

將新帳戶新增至組織時，此類帳戶會新增至帳戶管理頁面上的清單中。針對組織帳戶，類型為依組織。

根據預設，新組織帳戶不會啟用為成員帳戶。他們的狀態為非成員。

當您選擇自動啟用組織帳戶時，Detective 會在將新帳戶新增到組織時開始將新帳戶作為成員帳戶啟用。Detective 不會啟用尚未啟用的現有組織帳戶。

Detective 只有在行為圖表的成員帳戶數目上限為 1,200 時，才能將組織帳戶啟用為成員帳戶。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。

### Console

在帳戶管理頁面上，自動啟用新組織帳戶設定可決定是否在帳戶新增至組織時自動啟用帳戶。

要自動將新組織帳戶作為成員帳戶啟用

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 切換自動啟用新組織帳戶至開啟位置。

## DetectiveAPI/AWS CLI

若要判斷是否要將新組織帳戶自動啟用為 Detective 成員帳戶，管理員帳戶可以使用 Detective API 或 AWS Command Line Interface。

若要檢視和管理組態，您必須提供行為圖表 ARN。若要取得 ARN，使用 [ListGraphs](#) 操作。

若要檢視自動啟用組織帳戶的目前組態

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

在回應中，如果自動啟用新組織帳戶，則 `AutoEnable` 為 `true`。

- AWS CLI：在命令列中執行 [describe-organization-configuration](#) 命令。

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

### 範例

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

若要自動啟用新組織帳戶

- Detective API：使用 [UpdateOrganizationConfiguration](#) 操作。若要自動啟用新組織帳戶，則將 `AutoEnable` 設定為 `true`。
- AWS CLI：在命令列中執行 [update-organization-configuration](#) 命令。

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

### 範例

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

## 將組織帳戶啟用為 Detective 成員帳戶

如果您未自動啟用新組織帳戶，則可以手動啟用此類帳戶。您亦需手動啟用已解除關聯的帳戶。

### 決定是否可以啟用帳戶

如果組織行為圖表已啟用高達 1,200 個帳戶，則無法將組織帳戶作為成員帳戶啟用。在此情況下，組織帳戶狀態仍然為非成員。帳戶不會將資料提供至行為圖表。

一旦成員帳戶得以啟用，Detective 會自動將成員帳戶狀態變更為已啟用。例如，如果管理員帳戶移除其他成員帳戶以為帳戶騰出空間，成員帳戶狀態會變更為已啟用。

### Console

在帳戶管理頁面中，您可以將組織帳戶作為成員帳戶啟用。

若要將組織帳戶作為成員帳戶啟用

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 若要檢視目前未啟用的帳戶清單，選擇未啟用。
4. 您可以選取特定的組織帳戶，或啟用所有組織帳戶。

若要啟用已選取的組織帳戶：

- a. 選取您要啟用的每個組織帳戶。
- b. 選擇啟用帳戶。

若要啟用所有組織帳戶，選擇啟用所有組織帳戶。

### Detective API/AWS CLI

您可以使用 Detective API 或 AWS Command Line Interface，在組織行為圖表中將組織帳戶啟用為成員帳戶。若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

若要將組織帳戶作為成員帳戶啟用

- Detective API：使用 [CreateMembers](#) 操作。您必須提供圖表 ARN。

針對每個帳戶，指定帳戶識別符。組織行為圖表中的組織帳戶不會收到邀請。您不需要提供電子郵件地址或其他邀請資訊。

- AWS CLI：在命令列中執行 [create-members](#) 命令。

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-arn <behavior graph ARN>
```

範例

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

## 將組織帳戶取消關聯為 Detective 成員帳戶

若要停止從組織行為圖表中的組織帳戶擷取資料，您可以取消與帳戶的關聯。該帳戶的現有資料會保留在行為圖表中。

當您取消組織成員帳戶的關聯時，該帳戶的狀態會變更為非成員。Detective 不會再將該帳戶的資料擷取到您的行為圖表。此帳戶的現有資料會保留在行為圖表中，而帳戶會保留在清單中。

### Console

在帳戶管理頁面中，您可以取消組織帳戶作為成員帳戶的關聯。

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 若要顯示已啟用帳戶的清單，選擇啟用。
4. 選取要取消關聯帳戶的核取方塊。
5. 選擇動作。然後選擇停用帳戶。

已解除關聯帳戶的帳戶狀態會變更為非成員。

## Detective API/AWS CLI

若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

取消組織帳戶與組織行為圖表的關聯

- Detective API：使用 [DeleteMembers](#) 操作。指定圖表 ARN 和要取消關聯成員帳戶的帳戶識別符清單。
- AWS CLI：在命令列中執行 [delete-members](#) 命令。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

範例

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

## 在 Detective 中管理受邀成員帳戶

Detective 管理員帳戶可以在其行為圖表中邀請帳戶成為成員帳戶。行為圖表最多可容納 1,200 個成員帳戶。當成員帳戶接受邀請並啟用時，Amazon Detective 就會開始擷取成員帳戶的資料，並將其擷取到該行為圖表中。

若要邀請個別帳戶，您可以手動指定要邀請的成員帳戶，將其資料貢獻至行為圖表。如果您想要新增成員帳戶清單，您可以選擇提供 .csv 檔案，其中包含要邀請加入行為圖表的成員帳戶清單。

對於組織行為圖表以外的行為圖表，所有成員帳戶都是受邀帳戶。Detective 管理員帳戶也可以邀請非組織帳戶的帳戶加入組織行為圖表。

在高層級中，邀請帳戶提供行為圖表的程序如下。

1. 對於每個要新增的成員帳戶，管理員帳戶會提供 AWS 帳戶識別符和根使用者電子郵件地址。
2. Detective 會驗證電子郵件地址是否為帳戶的根使用者電子郵件地址。如果帳戶資訊有效，Detective 會將邀請傳送至成員帳戶。

Detective 不會執行此驗證或傳送電子郵件邀請給這些區域中的成員帳戶：

- AWS GovCloud (美國東部) 區域

- AWS GovCloud (美國西部) 區域

對於其他區域，您可以使用 Detective API 的 `DisableEmailNotification` [CreateMembers](#) 操作。如果 `DisableEmailNotification` 設為 `true`，則 Detective 不會傳送邀請給成員帳戶。對於集中管理的帳戶，這是一個有用的設定。

### 3. 成員帳戶將接受或拒絕邀請。

即使管理員帳戶未發送邀請電子郵件，成員帳戶仍然必須回應邀請。

### 4. 成員帳戶接受邀請後，Detective 會開始將成員帳戶的資料擷取至行為圖表。

### 5. 一旦成員帳戶符合啟用資格，Detective 會自動將成員帳戶狀態變更為已啟用。

例如，如果管理員帳戶移除其他成員帳戶以為帳戶騰出空間，成員帳戶狀態會變更為已啟用。

如果超過一個帳戶未啟用，則 Detective 會以帳戶受邀順序啟用帳戶。檢查是否啟用任何未啟用帳戶的程序將每小時執行一次。

管理員帳戶也可以手動啟用帳戶，而不必等待自動程序。例如，管理員帳戶可能想要選取要啟用的帳戶。如需如何啟用成員帳戶的資訊，請參閱 [the section called “啟用未啟用的成員帳戶”](#)。

請注意，Detective 在 2021 年 5 月 12 日開始自動啟用未啟用的帳戶。系統不會自動啟用之前未啟用的帳戶。管理員帳戶必須手動啟用此類帳戶。

管理員帳戶可以從行為圖表中移除受邀成員帳戶。Detective 不會從行為圖表中移除任何現有資料，而此類資料會跨成員帳戶彙總資料。

## 目錄

- [邀請個別帳戶加入行為圖表](#)
- [邀請成員帳戶清單至行為圖表](#)
- [啟用未啟用的成員帳戶](#)
- [從行為圖表移除成員帳戶](#)

## 邀請個別帳戶加入行為圖表

您可以手動指定要邀請的成員帳戶，以便將其資料提供至行為圖表。

## Console

使用 Detective 主控台手動選取要邀請的成員帳戶。

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 選擇動作。然後選擇邀請帳戶。
4. 在新增帳戶下，選擇新增個別帳戶。
5. 若要將成員帳戶新增至邀請清單，請執行以下步驟。
  - a. 選擇新增帳戶。
  - b. 針對AWS 帳戶 ID，輸入 AWS 帳戶 ID。
  - c. 針對電子郵件，輸入帳戶的根使用者電子郵件地址。
6. 若要從清單中移除帳戶，為該帳戶選擇移除帳戶。
7. 在個人化邀請電子郵件下，在邀請電子郵件中新增自訂內容。

例如，您可以使用該區域提供聯絡資訊。或者將其用於提醒成員帳戶，他們需要將必要的 IAM 政策附加到其使用者或角色，然後才能接受邀請。

8. 成員帳戶 IAM 政策包含成員帳戶所需的 IAM 政策文本。電子郵件邀請函包含此政策文字。若要複製政策文本，選擇複製。
9. 選擇 Invite (邀請)。

## Detective API/AWS CLI

您可以使用 Detective API 或 AWS Command Line Interface 來邀請成員帳戶將其資料貢獻至行為圖表。若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

### 邀請成員帳戶加入行為圖表 (Detective API) AWS CLI

- Detective API：使用 [CreateMembers](#) 操作。您必須提供圖表 ARN。針對每個帳戶，指定帳戶識別符和根使用者電子郵件地址。

若取消向成員帳戶發送邀請電子郵件，請設置 `DisableEmailNotification` 為 `true`。`DisableEmailNotification` 預設為 `false`。

如果您確實發送邀請電子郵件，則可以選擇提供自訂文本以新增至邀請電子郵件中。

- AWS CLI：在命令列中執行 `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>"
```

### 範例

```
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 --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."
```

要指示不發送邀請電子郵件到成員帳戶，則加入 `--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
```

### 範例

```
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
```

## 邀請成員帳戶清單至行為圖表

在 Detective 主控台中，您可以提供包含待邀請加入至行為圖表的成員帳戶清單的 `.csv` 檔案。

系統會將檔案第一行做為標頭列。每個帳戶都會列在單獨的行上。每個成員帳戶項目都包含 AWS 帳戶 ID 和帳戶的根使用者電子郵件地址。

範例：

```
Account ID,Email address
111122223333,srodriguez@example.com
```

```
444455556666,rroe@example.com
```

Detective 在處理檔案時，會忽略已受邀帳戶，除非該帳戶狀態為驗證失敗。該狀態表示為帳戶提供的電子郵件地址與帳戶的根使用者電子郵件地址不符。在這種情況下，Detective 會刪除原始邀請，然後再次嘗試驗證電子郵件地址並傳送邀請。

此選項還會提供範本，供您用於建立帳戶清單。

從 .csv 清單邀請成員帳戶 (主控台)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 選擇動作。然後選擇邀請帳戶。
4. 在新增帳戶下，選擇從 .csv 新增。
5. 若要下載要使用的範本檔案，請選擇下載 .csv 範本。
6. 若要選取包含帳戶清單的檔案，請選擇選擇 .csv 檔案。
7. 在檢閱成員帳戶下，確認 Detective 在檔案中找到的成員帳戶清單。
8. 在個人化邀請電子郵件下，在邀請電子郵件中新增自訂內容。

例如，您可以提供聯絡資訊，或提醒成員帳戶有關必要的 IAM 政策。

9. 成員帳戶 IAM 政策包含成員帳戶所需的 IAM 政策文本。電子郵件邀請函包含此政策文字。若要複製政策文本，選擇複製。
10. 選擇 Invite (邀請)。

## 新增跨區域的成員帳戶清單

Detective 在 GitHub 中提供開放原始碼 Python 指令碼，可讓您執行下列動作：

- 將指定的成員帳戶清單新增至跨區域特定清單的管理員帳戶行為圖表。
- 如果管理員帳戶在區域中沒有行為圖表，則指令碼也會啟用 Detective，並在該區域中建立行為圖表。
- 傳送邀請電子郵件到成員帳戶。
- 自動接受成員帳戶的邀請。

如需如何設定和使用 GitHub 指令碼的相關資訊，請參閱 [the section called “Amazon Detective Python 指令碼”](#)。

## 啟用未啟用的成員帳戶

成員帳戶接受邀請後，Amazon Detective 會檢查成員帳戶的數量。行為圖表中成員帳戶的數目上限為 1,200。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。如果 Detective 無法啟用成員帳戶，則會將成員帳戶狀態設定為未啟用。

未啟用的成員帳戶不會將資料提供至行為圖表。

Detective 會自動啟用帳戶，因為行為圖表可以容納帳戶。

您也可以嘗試手動啟用未啟用成員帳戶的成員帳戶。例如，您可以移除現有的成員帳戶以減少資料量。您可以嘗試啟用未啟用成員帳戶，不必等待啟用帳戶的自動程序。

### Console

成員帳戶清單包括用於啟用未啟用的選取成員帳戶的選項。

若要啟用未啟用的成員帳戶

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 在我的成員帳戶下，選取要啟用的每個成員帳戶的核取方塊。

您只能啟用狀態為未啟用的成員帳戶。

4. 選擇啟用帳戶。

Detective 會決定是否可以啟用成員帳戶。如果可以啟用成員帳戶，狀態會變更為已啟用。

### Detective API/CLI

您可以使用 API 呼叫或 AWS Command Line Interface 來啟用未啟用的單一成員帳戶。若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

若要啟用未啟用的成員帳戶

- Detective API：使用 [StartMonitoringMember](#) API 操作。您必須提供行為圖表 ARN。若要識別成員帳戶，請使用 AWS 帳戶識別符。
- AWS CLI：執行 [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
```

## 從行為圖表移除成員帳戶

管理員帳戶可以隨時從行為圖表中移除受邀的成員帳戶。

Detective 會自動移除終止於 的成員帳戶 AWS，但 AWS GovCloud（美國東部）和 AWS GovCloud（美國西部）區域除外。

從行為圖表中移除受邀成員帳戶時，會發生以下情況。

- 成員帳戶已從我的成員帳戶中移除。
- Amazon Detective 停止從已移除的帳戶擷取資料。

Detective 不會從行為圖表中移除任何現有資料，而此類資料會跨成員帳戶彙總資料。

### Console

您可以使用 AWS 管理主控台 從行為圖表中移除受邀的成員帳戶。

若要移除成員帳戶 (主控台)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 在帳戶清單中，選取要移除成員帳戶的核取方塊。

您無法從清單中移除自己的帳戶。

4. 選擇動作。然後選擇停用帳戶。

### Detective API/CLI

您可以使用 Detective API 或 AWS Command Line Interface 從行為圖表中移除受邀的成員帳戶。若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

## 從行為圖表中移除受邀的成員帳戶 (Detective API) AWS CLI

- Detective API：使用 [DeleteMembers](#) 操作。指定圖表 ARN 和要移除成員帳戶的帳戶識別符清單。
- AWS CLI：在命令列中執行 [delete-members](#) 命令。

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

範例：

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

## Python script

Detective 在 GitHub 中提供了開放原始指令碼。您可以是該指令碼，將指定的成員帳戶清單從跨區域特定清單的管理員帳戶行為圖表中移除。

如需如何設定和使用 GitHub 指令碼的相關資訊，請參閱 [the section called “Amazon Detective Python 指令碼”](#)。

## 針對成員帳戶：管理行為圖表邀請和成員資格

Amazon Detective 會針對每個成員帳戶所提供的每個行為圖表，收取擷取的資料費用。

透過帳戶管理頁面，成員帳戶可以查看其所屬行為圖表的管理員帳戶。

受邀加入行為圖表的成員帳戶可以檢視並回應其邀請。他們也可以將自己的帳戶從行為圖表中移除。

針對組織行為圖表，組織帳戶不會控制其帳戶是否為成員帳戶。Detective 管理員帳戶會選擇要作為成員帳戶啟用或停用的組織帳戶。

## 目錄

- [成員帳戶所需的 IAM 政策](#)
- [檢視行為圖表的邀請清單](#)
- [回應行為圖表邀請](#)

- [從行為圖表中移除帳戶](#)

## 成員帳戶所需的 IAM 政策

成員帳戶必須先將必要 IAM 政策附加到其主體上，才能檢視和管理邀請。主體可以是現有使用者或角色，您也可以建立新使用者或角色以供 Detective 使用。

理想情況下，管理員帳戶會讓其 IAM 管理員附加必要政策。

成員帳戶 IAM 政策授予成員帳戶在 Amazon Detective 中的存取動作。提供行為圖表的電子郵件邀請包含該 IAM 政策的文本。

若要使用此政策，請以圖表 ARN 取代 *<behavior graph ARN>*。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "arn:aws:detective:us-east-1:123456789012:graph/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
      ],
      "Resource": "*"
    }
  ]
}
```

請注意，組織行為圖表中的組織帳戶不會收到邀請，也無法取消其帳戶與組織行為圖表的關聯。如果它們不屬於其他行為圖表，則只需要 ListInvitations 許可即可。透過 ListInvitations，使用者可以查看行為圖表的管理員帳戶。管理邀請和取消成員資格的許可僅適用於透過邀請的成員資格。

## 檢視行為圖表的邀請清單

從 Amazon Detective 主控台、Detective API 或 AWS Command Line Interface 成員帳戶可以看到其行為圖表邀請。

### 檢視行為圖表邀請 (主控台)

您可以從 檢視行為圖表邀請 AWS 管理主控台。

#### 若要檢視行為圖表邀請 (主控台)

1. 登入 AWS 管理主控台。然後前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。

在帳戶管理頁面上，我的管理員帳戶包含您在當前區域中開啟和已接受的行為圖表邀請。針對組織帳戶，我的管理員帳戶也包含組織行為圖表。

如果您的帳戶目前處於免費試用期，頁面也會顯示免費試用的剩餘天數。

清單中不包含您拒絕的邀請、您放棄的成員資格或是管理員帳戶移除的成員資格。

每個邀請都會顯示管理員帳戶、接受邀請的日期以及邀請的目前狀態。

- 針對您尚未回應的邀請，狀態為已邀請。
- 針對您接受的邀請，狀態為已啟用或未啟用。

如果狀態為已啟用，則您的帳戶會將資料提供至行為圖表。

如果狀態為未啟用，則您的帳戶不會將資料提供至行為圖表。

在 Detective 檢查您是否已啟用 GuardDuty，以及您的帳戶是否因此導致行為圖表的資料量超出 Detective 的配額上限時，您的帳戶狀態會初始設為未啟用。

如果您的帳戶不會造成行為圖表超出配額，則 Detective 會將您的帳戶狀態更新為已啟用。否則，狀態會保持為未啟用。

當行為圖表能夠容納您帳戶的資料量時，Detective 會自動將其更新為已啟用。例如，管理員帳戶可能會移除其他成員帳戶，以便啟用您的帳戶。管理員帳戶也可以手動啟用您的帳戶。

## 檢視行為圖表邀請 (Detective API) AWS CLI

您可以從 Detective API 或 AWS Command Line Interface 列出行為圖表邀請。

### 擷取行為圖表的開啟和接受邀請清單 (Detective API) AWS CLI

- Detective API：使用 [ListInvitations](#) 操作。
- AWS CLI：在命令列中執行 [list-invitations](#) 命令。

```
aws detective list-invitations
```

## 回應行為圖表邀請

在您接受邀請後，Detective 會檢查成員帳戶的數量。行為圖表中成員帳戶的數目上限為 1,200。如果行為圖表已包含 1,200 個成員帳戶，則無法啟用新帳戶。

接受邀請後，Detective 會在您的帳戶中啟用。Detective 會檢查您的資料磁碟區是否在 Detective 配額內。流入行為圖表的資料量必須小於 Detective 允許的最大值。如果目前擷取的磁碟區超過每天 10 TB 的限制，您無法新增更多帳戶，且 Detective 會停用進一步的資料擷取。Detective 主控台會顯示通知，指出資料磁碟區太大且狀態保持未啟用。

如果您拒絕邀請，則該邀請會從邀請清單中移除，且 Detective 不會在行為圖表中使用您的帳戶資料。

### 回應行為圖表邀請 (主控台)

您可以使用 AWS 管理主控台 來回應電子郵件邀請，其中包含 Detective 主控台的連結。您只能回應狀態為已邀請的邀請。

#### 若要回應行為圖表邀請 (主控台)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 在我的管理員帳戶下，若要接受邀請並開始向行為圖表貢獻資料，選擇接受邀請。

若要拒絕邀請並將其從清單中移除，選擇拒絕。

## 回應行為圖表邀請 (Detective API) AWS CLI

您可以從 Detective API 或 AWS Command Line Interface 回應行為圖表邀請。

### 接受行為圖表邀請 (Detective API) AWS CLI

- Detective API：使用 [AcceptInvitation](#) 操作。您必須指定圖表 ARN。
- AWS CLI：在命令列中執行 [accept-invitation](#) 命令。

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

範例：

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

### 拒絕行為圖表邀請 (Detective API) AWS CLI

- Detective API：使用 [RejectInvitation](#) 操作。您必須指定圖表 ARN。
- AWS CLI：在命令列中執行 [reject-invitation](#) 命令。

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

範例：

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

## 從行為圖表中移除帳戶

接受邀請後，您可以隨時從行為圖表中移除帳戶。當您從行為圖表中移除帳戶時，Amazon Detective 會停止將您帳戶中的資料擷取至行為圖表中。現有資料會保留在行為圖表中。

只有受邀帳戶可以從行為圖表中移除其帳戶。組織帳戶無法從組織行為圖表中移除其帳戶。

### 從行為圖表中移除您的帳戶 (主控台)

您可以使用 [從行為圖表 AWS 管理主控台](#) 中移除您的帳戶。

## 若要從行為圖表 (主控台) 移除帳戶

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，選擇帳戶管理。
3. 在我的管理員帳戶下，針對您要放棄的行為圖表，選擇放棄。

## 從行為圖表中移除您的帳戶 (Detective API) AWS CLI

您可以使用 Detective API 或 從行為圖表 AWS Command Line Interface 中移除您的帳戶。

### 從行為圖表中移除您的帳戶 (Detective API) AWS CLI

- Detective API：使用 [DisassociateMembership](#) 操作。您必須指定圖表 ARN。
- AWS CLI：在命令列中執行 [disassociate-membership](#) 命令。

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

範例：

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

## 帳戶動作對行為圖表的影響

此類動作對 Amazon Detective 資料和存取有以下影響。

### Detective 遭到停用

當管理員帳戶停用 Detective 時，會發生以下情況：

- 行為圖表遭到移除。
- Detective 會停止從管理員帳戶及該行為圖表的成員帳戶擷取資料。

### 成員帳戶遭到從行為圖表中移除

從行為圖表中移除成員帳戶時，Detective 會停止從該帳戶擷取資料。

行為圖表中的現有資料不會受到影響。

對於受邀帳戶，該帳戶會從我的成員帳戶清單中移除。

對於組織行為圖表中的組織帳戶，帳戶狀態會變更為非成員。

## 成員帳戶離開組織

當成員帳戶離開組織時，會發生以下情況：

- 該帳戶會從組織行為圖表的我的成員帳戶清單中移除。
- Detective 停止從該帳戶中擷取資料。

行為圖表中的現有資料不會受到影響。

## AWS 帳戶已暫停

當管理員帳戶暫停時 AWS，帳戶會失去在 Detective 中檢視行為圖表的許可。Detective 停止將資料擷取至行為圖表中。

當成員帳戶暫停時 AWS，Detective 會停止擷取該帳戶的資料。

90 天後，帳戶將被終止或重新激活。當管理員帳戶重新啟用時，系統會還原其 Detective 許可。Detective 會恢復從帳戶擷取資料。重新啟用成員帳戶後，Detective 會繼續從該帳戶擷取資料。

## AWS 帳戶已關閉

當 AWS 帳戶關閉時，Detective 會回應關閉，如下所示。

- 針對管理員帳戶，Detective 會刪除行為圖表。
- 針對成員帳戶，Detective 會從行為圖表中移除該帳戶。

AWS 從管理員帳戶關閉的生效日期起，會保留帳戶的政策資料 90 天。在 90 天期間結束時，會 AWS 永久刪除帳戶的所有政策資料。

- 若要保留問題清單超過 90 天，您可以封存政策。您也可以將自訂動作與 EventBridge 規則搭配使用，將問題清單存放在 S3 儲存貯體中。
- 只要 AWS 保留政策資料，當您重新開啟已關閉的帳戶時，會將該帳戶 AWS 重新指派為服務管理員，並復原該帳戶的服務政策資料。

- 如需詳細資訊，請參閱[關閉帳戶](#)。

### Important

對於 AWS GovCloud (US) 區域中的客戶：

- 在關閉帳戶前，請先備份帳戶資源，然後刪除。在您關閉帳戶後，您將沒有存取這些的權限。

## 使用 Detective Python 指令碼來管理帳戶

Amazon Detective 在 GitHub 儲存庫 ([amazon-detective-multiaccount-scripts](#)) 中提供了一組開放原始 Python 指令碼。此類指令碼需要 Python 3。

您可透過下屬操作執行以下任務：

- 為跨區域的管理員帳戶啟用 Detective。

啟用 Detective 後，您可以將標籤指派給行為圖表。

- 將成員帳戶新增至管理員帳戶的跨區域行為圖表。
- 可以選擇向成員帳戶發送邀請電子郵件。您還可以將請求設定為不發送邀請電子郵件。
- 將成員帳戶從管理員帳戶的跨區域行為圖表中移除。
- 為跨區域的管理員帳戶停用 Detective。當管理員帳戶停用 Detective 時，系統會停用每個區域中的管理員帳戶行為圖表。

## enableDetective.py 指令碼概觀

enableDetective.py 指令碼會執行以下操作：

1. 如果管理員帳戶尚未在該區域中啟用 Detective，則為每個指定區域中的管理員帳戶啟用 Detective。

當您使用指令碼啟用 Detective 後，您可以將標籤指派給行為圖表。

2. 可以選擇將管理員帳戶發送的要求傳送至各行為圖表的指定成員帳戶。

邀請電子郵件訊息會使用預設訊息內容，且無法自訂。

您還可以將請求設定為不發送邀請電子郵件。

### 3. 自動接受成員帳戶的邀請。

由於指令碼會自動接受邀請，因此成員帳戶可以忽略此類訊息。

我們建議您直接與成員帳戶聯絡，通知他們邀請已自動接受。

## disableDetective.py 指令碼概觀

disableDetective.py 指令碼會從指定區域的管理員帳戶行為圖表中刪除指定的成員帳戶。

它還提供了一個選項，以在跨指定區域中停用管理員帳戶的 Detective。

### 指令碼的必要許可

指令碼需要管理員帳戶中的預先存在 AWS 角色，以及您新增或移除的所有成員帳戶中的預先存在角色。

#### Note

所有帳戶中的角色名稱必須相同。

IAM 政策 [建議的最佳實務](#) 是使用最小範圍的角色。若要執行指令碼的 [建立圖表](#)、[建立成員](#) 以及 [將成員新增至圖表](#) 的工作流程，必要的許可如下：

- detective:CreateGraph
- detective:CreateMembers
- detective>DeleteGraph
- detective>DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

### 角色信任關係

角色信任關係必須允許您的執行個體或本機憑證擔任該角色。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_doe"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果您沒有包含必要許可的共同角色，則必須在每個成員帳戶中建立至少具有此類許可的角色。您還需在管理員帳戶中建立角色。

在您建立角色後，請確認執行以下操作：

- 在每個帳戶中使用相同的角色名稱。
- 在上方新增必要的許可 (建議) 或選取 [AmazonDetectiveFullAccess](#) 受管政策。
- 如上所述，新增角色信任關係區塊。

若要自動化此程序，您可以使用 `EnableDetective.yaml` CloudFormation 範本。由於範本只會建立全域資源，因此可以在任何區域中執行。

## 為 Python 指令碼設置執行環境

您可以從 EC2 執行個體或本機電腦執行指令碼。

### 啟動和設定 EC2 執行個體

執行指令碼的一個選項是透過 EC2 執行個體進行執行。

若要啟動和設定 EC2 執行個體

1. 在管理員帳戶中啟動 EC2 執行個體。如需如何啟動 EC2 執行個體的詳細資訊，請參閱 [《Amazon EC2 使用者指南》](#) 中的 [Amazon EC2 Linux 執行個體入門](#)。Amazon EC2

2. 將 IAM 角色附加至執行個體，該角色具有允許執行個體在管理員帳戶中呼叫 AssumeRole 的許可。

如果您使用 EnableDetective.yaml CloudFormation 範本，則會 EnableDetective 建立具有名為 設定檔的執行個體角色。

否則，如需建立執行個體角色的相關資訊，請參閱部落格文章 [使用 EC2 主控台輕鬆取代或連接 IAM 角色至現有 EC2 執行個體](#)。

3. 安裝所需的軟體：

- 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. 將儲存庫複製到 EC2 執行個體。

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

## 設定本機電腦以執行指令碼

您也可以從本機電腦中執行指令碼。

### 設定本機電腦以執行指令碼

1. 請確定您已針對具有呼叫 AssumeRole 許可的管理員帳戶設定本機電腦憑證。
2. 安裝所需的軟體：
  - Python 3
  - Boto (最低版本 1.15)
  - GitHub 指令碼

平台	設定說明
Windows	<ol style="list-style-type: none"><li>1. 安裝 Python 3 (<a href="https://www.python.org/downloads/windows/">https://www.python.org/downloads/windows/</a>)。</li><li>2. 開啟命令提示。</li></ol>

平台	設定說明
	<ol style="list-style-type: none"> <li>若要安裝 Boto，請執行：<code>pip install boto3</code></li> <li>從 GitHub (<a href="https://github.com/aws-samples/amazon-detective-multiaccount-scripts">https://github.com/aws-samples/amazon-detective-multiaccount-scripts</a>) 下載指令碼來源程式碼。</li> </ol>
Mac	<ol style="list-style-type: none"> <li>安裝 Python 3 (<a href="https://www.python.org/downloads/mac-osx/">https://www.python.org/downloads/mac-osx/</a>)。</li> <li>開啟命令提示。</li> <li>若要安裝 Boto，請執行：<code>pip install boto3</code></li> <li>從 GitHub (<a href="https://github.com/aws-samples/amazon-detective-multiaccount-scripts">https://github.com/aws-samples/amazon-detective-multiaccount-scripts</a>) 下載指令碼來源程式碼。</li> </ol>
Linux	<ol style="list-style-type: none"> <li>若要安裝 Python 3，請執行以下其中一項： <ul style="list-style-type: none"> <li><code>sudo apt-get -y install python3-pip python3 git</code></li> <li><code>sudo yum install git python</code></li> </ul> </li> <li>若要安裝 Boto，請執行：<code>sudo pip install boto3</code></li> <li>從 <a href="https://github.com/aws-samples/amazon-detective-multiaccount-scripts">https://github.com/aws-samples/amazon-detective-multiaccount-scripts</a> 複製指令碼來源程式碼。</li> </ol>

## 建立要新增或移除的成員帳戶 .csv 清單

若要識別要新增至行為圖表或從行為圖表中移除的成員帳戶，您需要提供包含帳戶清單的 .csv 檔案。

在單獨的行上列出各個帳戶。每個成員帳戶項目都包含 AWS 帳戶 ID 和帳戶的根使用者電子郵件地址。

請參閱下列範例：

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

## 執行 enableDetective.py

您可以從 EC2 `enableDetective.py` 執行個體或本機電腦執行指令碼。

請執行 `enableDetective.py`。

1. 將 `.csv` 檔案複製到 EC2 執行個體或本機電腦上的 `amazon-detective-multiaccount-scripts` 目錄。
2. 切換至 `amazon-detective-multiaccount-scripts` 目錄。
3. 執行 `enableDetective.py` 指令碼。

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
--input_file inputFileName --tags tagValueList --enabled_regions regionList --
disable_email
```

執行指令碼時，請取代以下值：

*administratorAccountID*

管理員 AWS 帳戶的帳戶 ID。

*roleName*

要在管理員帳戶和每個成員帳戶中擔任 AWS 的角色名稱。

*inputFileName*

包含要新增至管理員帳戶行為圖表的成員帳戶清單的 `.csv` 檔案名稱。

*tagValueList*

(選用) 要指派給新行為圖表的標籤值清單 (以逗號分隔)。

針對每個標籤值，格式為 `key=value`。例如：

```
--tags Department=Finance,Geo=Americas
```

*regionList*

(選用) 以逗號分隔的區域清單，可在其中將成員帳戶新增至管理員帳戶的行為圖表。例如：

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

管理員帳戶可能尚未在區域中啟用 Detective。在這種情況下，指令碼會啟用 Detective，並為管理員帳戶建立新行為圖表。

如果您未提供區域清單，則指令碼會在 Detective 支援的所有區域中運作。

`--disable_email`

(選用) 如果包含，則 Detective 不會向成員帳戶發送邀請電子郵件。

## 執行 `disableDetective.py`

您可以從 EC2 `disableDetective.py` 執行個體或本機電腦執行指令碼。

請執行 `disableDetective.py`。

1. 將 `.csv` 檔案複製至 `amazon-detective-multiaccount-scripts` 目錄。
2. 若要在指定的區域清單中使用 `.csv` 檔案以從管理員帳戶的行為圖表中刪除列出的成員帳戶，請執行 `disableDetective.py` 指令碼，如下所示：

```
disableDetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList
```

3. 若要在所有區域中停用管理員帳戶的 Detective，請執行標有 `--delete-master` 標記的 `disableDetective.py` 指令碼。

```
disableDetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList --delete_master
```

執行指令碼時，請取代以下值：

*administratorAccountID*

管理員 AWS 帳戶的帳戶 ID。

*roleName*

要在管理員帳戶和每個成員帳戶中擔任 AWS 的角色名稱。

*inputFileName*

包含要從管理員帳戶行為圖表移除的成員帳戶清單的 `.csv` 檔案名稱。

即使您停用 Detective，也必須提供 `.csv` 檔案。

*regionList*

(選用) 要執行以下其中一項動操作的區域清單 (以逗號分隔)：

- 從管理員帳戶的行為圖表中移除成員帳戶。
- 如果包含 `--delete-master` 標記，請停用 Detective。

例如：

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

如果您未提供區域清單，則指令碼會在 Detective 支援的所有區域中運作。

# Amazon Detective 與 Amazon Security Lake 整合

Amazon Security Lake 是完全受管的安全資料湖服務。您可以使用 Security Lake，將來自 AWS 環境、SaaS 提供者、內部部署來源、雲端來源和第三方來源的安全資料，自動集中到存放在您 AWS 帳戶中的專用資料湖。Security Lake 可協助您分析安全資料，讓您更全面地了解整個組織的安全狀態。透過 Security Lake，您還可以改善工作負載、應用程式和資料的保護。

Amazon Detective 與 Amazon Security Lake 集成，這意味著您可以查詢和擷取 Security Lake 存儲的原始日誌資料。

使用此整合，您可以從 Security Lake 原生支援的以下來源收集日誌和事件。Detective 最多支援來源版本 2 (OCSF 1.1.0)。

- AWS CloudTrail 管理事件 1.0 版及更新版本
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌 1.0 版及更新版本
- Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌 2.0 版。— 若要使用 Amazon EKS 稽核日誌做為來源，您必須將 `ram:ListResources` 新增至 IAM 許可。如需詳細資訊，請參閱 [將必要的 IAM 許可新增至您的帳戶](#)。

如需 Security Lake 如何自動將來自原生支援服務的日誌和事件轉換為 AWS OCSF 結構描述的詳細資訊，請參閱 [Amazon Security Lake 使用者指南](#)。

將 Detective 與 Security Lake 整合之後，Detective 會開始從 Security Lake 提取與 AWS CloudTrail 管理事件和 Amazon VPC 流程日誌相關的原始日誌。如需詳細資訊，請參閱 [查詢原始日誌](#)。

## 啟用 Detective 與 Security Lake 的整合

若要將 Detective 與 Security Lake 整合，您必須完成下列步驟。

### 1. [開始之前](#)

使用組織管理帳戶，為您的組織指定委派的 Security Lake 管理員。確定 Security Lake 已啟用，並確認 Security Lake 正在從 AWS CloudTrail 管理事件和 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌收集日誌和事件。

為了符合安全參考架構，Detective 建議使用 Log Archive 帳戶，並延遲使用 Security Lake 部署的安全工具帳戶。

### 2. [建立 Security Lake 訂閱者](#)

若要使用來自 Amazon Security Lake 的日誌和事件，您必須是 Security Lake 的訂閱用戶。請依照以下步驟將查詢存取權授予 Detective 帳戶管理員。

### 3. 將必要 AWS Identity and Access Management (IAM) 許可新增至您的 IAM 身分。

- 新增這些許可，以建立與 Security Lake 的 Detective 整合：
  - 將這些 AWS Identity and Access Management (IAM) 許可連接至您的 IAM 身分。如需詳細資訊，請參閱將[必要的 IAM 許可新增至您的帳戶](#)一節。
  - 將此 IAM 政策新增至您計劃用來傳遞 CloudFormation 服務角色的 IAM 主體。如需詳細資訊，請參閱[新增許可到您的 IAM 主體](#)一節。
- 如果您已將 Detective 與 Security Lake 整合，請使用整合將這些 (IAM) 許可連接到您的 IAM 身分。如需詳細資訊，請參閱將[必要的 IAM 許可新增至您的帳戶](#)一節。

### 4. [接受資源共享 ARN 邀請並啟用整合](#)

使用 AWS CloudFormation 範本來設定為 Security Lake 訂閱者建立和管理查詢存取所需的參數。如需建立堆疊的詳細步驟，請參閱[使用 AWS CloudFormation 範本建立堆疊](#)。完成建立堆疊之後，請啟用整合。

如需如何使用 Detective 主控台將 Amazon Detective 與 Amazon Security Lake 整合的示範，請觀看下列影片：[Amazon Detective 與 Amazon Security Lake 整合 - 如何設定-->](#)

## 開始將 Detective 與 Security Lake 整合之前

本主題說明初步步驟，例如為您的組織委派 Security Lake 管理員、為您的 Detective 管理員帳戶啟用 Security Lake，以及驗證 Security Lake 正在收集日誌和事件。

Security Lake 與整合 AWS Organizations，以管理組織中多個帳戶的日誌收集。若要將 Security Lake 用於組織，您的 AWS Organizations 管理帳戶必須先為您的組織指定委派的 Security Lake 管理員。接下來，委派的 Security Lake 管理員必須啟用 Security Lake，並為組織中的成員帳戶啟用日誌和事件收集。

將 Security Lake 與 Detective 整合之前，請確定已為 Detective 管理員帳戶啟用 Security Lake。您必須先使用 Security Lake 主控台啟用 Security Lake，以設定您的資料湖設定和日誌收集。如需如何啟用 Security Lake 的詳細步驟，請參閱《Amazon Security Lake 使用者指南》中的[入門指南](#)。

此外，確認 Security Lake 正在從 AWS CloudTrail 管理事件和 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌收集日誌和事件。如需 Security Lake 中日誌收集的詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的[從 AWS 服務收集資料](#)。

## 步驟 1：在 Detective 中建立 Security Lake 訂閱者

本主題說明如何使用 Detective 主控台來建立 Security Lake 訂閱者。

若要使用來自 Amazon Security Lake 的日誌和事件，您必須是 Security Lake 的訂閱用戶。訂閱用戶可以查詢和存取 Security Lake 收集的資料。具有查詢存取權的訂閱者可以使用 Amazon Athena 等服務，直接在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中查詢 AWS Lake Formation 資料表。若要成為訂閱用戶，Security Lake 管理員必須為您提供可讓您查詢資料湖的訂閱用戶存取權。如需管理員如何執行此操作的詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的[建立具有查詢存取權的訂閱用戶](#)。

請依照下列步驟建立 Security Lake 訂閱者，以授予 Detective 管理員帳戶的查詢存取權。

在 Security Lake 中建立 Detective 訂閱用戶

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中選擇整合。
3. 在 Security Lake 訂閱用戶窗格中，記錄帳戶 ID 和外部 ID 值。

要求 Security Lake 管理員使用 ID 以實現以下操作：

- 若要在 Security Lake 中為您建立 Detective 訂閱用戶。

- 若要為訂閱用戶設定為具有存取權。
- 為確保使用 Lake Formation 許可建立 Security Lake 查詢訂閱用戶，請在 Security Lake 主控台中選取 Lake Formation 作為資料存取方法。

當 Security Lake 管理員為您建立訂閱用戶時，Security Lake 會為您產生 Amazon 資源共享 ARN。請管理員將此 ARN 傳送給您。

4. 在 Security Lake 訂閱用戶窗格中輸入由 Security Lake 管理員提供的資源共享 ARN。
5. 從 Security Lake 管理員收到資源共享 ARN 之後，請在 Security Lake 訂閱用戶窗格中的資源共享 ARN 方塊中輸入 ARN。

## 步驟 2：在 Detective 中將必要的 IAM 許可新增至您的帳戶

本主題說明您必須新增至 IAM 身分的 AWS Identity and Access Management (IAM) 許可政策詳細資訊。

若要啟用 Detective 與 Security Lake 的整合，您必須將下列 AWS Identity and Access Management (IAM) 許可政策連接至您的 IAM 身分。

將以下內嵌政策附加到角色。如果您想要使用自己的 Amazon S3 儲存貯體存放 Athena 查詢結果，請以 Amazon S3 儲存貯體名稱取代 `athena-results-bucket`。如果您希望 Detective 自動產生 Amazon S3 儲存貯體來存放 Athena 查詢結果，請從 IAM 政策中移除整個 `S3objectPermissions`。

如果您沒有將此政策連接至 IAM 身分所需的許可，請聯絡您的 AWS 管理員。如果您有必要的許可，但發生問題，請參閱《IAM 使用者指南》中的[對存取遭拒錯誤訊息進行故障診斷](#)。

### JSON

```
{
  "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:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue*:123456789012:database/amazon_security_lake*",
        "arn:aws:glue*:123456789012:table/amazon_security_lake*/amazon_security_lake*",
        "arn:aws:glue*:123456789012: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:*:123456789012:parameter/Detective/SLI"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudformation:GetTemplateSummary",
    "iam:ListRoles"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "securitylake.amazonaws.com"
      ]
    }
  }
}
]
```

### 步驟 3：接受資源共享 ARN 邀請

本主題說明使用 AWS CloudFormation 範本接受資源共用 ARN 邀請的步驟，這是啟用 Detective 與 Security Lake 整合之前的必要步驟。

若要從 Security Lake 存取原始資料日誌，您必須接受來自 Security Lake 管理員所建立的 Security Lake 帳戶的資源共享邀請。您還需要設定跨帳戶資料表共享的 AWS Lake Formation 許可。此外，您必須建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體，以接收原始查詢日誌。

在此下一個步驟中，您將使用 AWS CloudFormation 範本建立堆疊：接受資源共享 ARN 邀請、建立必要的 AWS Glue 編目程式 資源，以及授予 AWS Lake Formation 管理員許可。

接受資源共享 ARN 邀請並啟用整合

1. 使用 CloudFormation 範本建立新 CloudFormation 堆疊。如需詳細資訊，請參閱[使用 CloudFormation 範本建立堆疊](#)。
2. 建立堆疊完成後，請選擇啟用整合以啟用 Detective 與 Security Lake 的整合。

## 使用 CloudFormation 範本建立堆疊

Detective 提供 CloudFormation 範本，可用來設定為 Security Lake 訂閱者建立和管理查詢存取所需的參數。

### 步驟 1：建立 AWS CloudFormation 服務角色

您必須建立 CloudFormation 服務角色，才能使用 CloudFormation 範本建立堆疊。若您沒有建立服務角色的所需許可，請連絡 Detective 管理員帳戶的管理員。如需 AWS CloudFormation 服務角色的詳細資訊，請參閱[AWS CloudFormation 服務角色](#)。

1. 登入 AWS 管理主控台 並開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
2. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
3. 對於 Select trusted entity (選取信任的實體) 區段，選擇 AWS service (AWS 服務)。
4. 選擇 CloudFormation。然後選擇下一步。
5. 輸入角色的名稱。例如 CFN-DetectiveSecurityLakeIntegration。
6. 將以下內嵌政策附加到角色。將 取代 <Account ID> 為 AWS 您的帳戶 ID。

### JSON

```
{
  "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::*:111122223333:role/*-ResourceShareAcceptorLamb-*",
        "arn:aws:iam::*:111122223333:role/*-SsmParametersLambdaRole-*",
        "arn:aws:iam::*:111122223333:role/*-GlueDatabaseLambdaRole-*",
        "arn:aws:iam::*:111122223333:role/*-GlueTablesLambdaRole-*",
        "arn:aws:iam::*:111122223333: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:*:111122223333:function:*"
    ]
},
{
    "Sid": "CloudwatchPermissions",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:DescribeLogGroups"
    ],
    "Resource": "arn:aws:logs:*:111122223333:log-group:*"
},
{
    "Sid": "KmsPermission",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
}
]
}

```

步驟 2：將許可新增至您的 IAM 主體。

您需要以下許可，才能使用您在上述步驟中建立的 CloudFormation 服務角色建立堆疊。將以下 IAM 政策新增至您旨在用來傳遞 CloudFormation 服務角色的 IAM 主體。您將擔任此 IAM 主體以建立堆疊。若您沒有新增 IAM 政策所需的許可，請聯絡 Detective 管理員帳戶的管理員。

### Note

在以下政策中，此政策中所使用的 CFN-DetectiveSecurityLakeIntegration 是您在上一個 Creating an AWS CloudFormation 服務角色步驟中建立的角色。如果不同，請將其變更為您在上一個步驟中輸入的角色名稱。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/CFN-DetectiveSecurityLakeIntegration"
    },
    {
      "Sid": "RestrictCloudFormationAccess",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:*:111122223333:stack/*",
      "Condition": {
        "StringEquals": {
          "cloudformation:RoleArn": [
            "arn:aws:iam::111122223333:role/CFN-DetectiveSecurityLakeIntegration"
          ]
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid": "CloudformationDescribeStack",
    "Effect": "Allow",
    "Action": [
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:GetStackPolicy"
    ],
    "Resource": "arn:aws:cloudformation:*:111122223333:stack/*"
  },
  {
    "Sid": "CloudformationListStacks",
    "Effect": "Allow",
    "Action": [
      "cloudformation:ListStacks"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CloudWatchPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:logs:*:111122223333:log-group:*"
  }
]
}
```

### 步驟 3：在 CloudFormation 主控台中指定自訂值

1. 從 Detective 前往 AWS CloudFormation 主控台。
2. (選用) 輸入堆疊名稱。堆疊名稱會自動填入。您可以將堆疊名稱變更為與現有堆疊名稱不衝突的名稱。
3. 輸入以下參數：
  - AthenaResultsBucket：如果您未輸入值，則此範本會產生 Amazon S3 儲存貯體。如果您想要使用自己的儲存貯體，請輸入儲存貯體名稱來儲存 Athena 查詢結果。若您使用自己的儲存貯

體，請確保儲存貯體與資源共享 ARN 位於相同的區域。如果您使用自己的儲存貯體，請確定您選擇的 `LakeFormationPrincipals` 具有將物件寫入儲存貯體和從中讀取物件的許可。如需儲存貯體許可的詳細資訊，請參閱《Amazon Athena 使用者指南》中的[查詢結果和最近查詢](#)。

- `DTRegion`：此欄位已預先填入。請勿變更此欄位中的值。
- `LakeFormationPrincipals` – 輸入您要授予使用 Security Lake 整合之存取權的 IAM 主體的 ARN (例如 IAM 角色 ARN)，並以逗號分隔。這些可能是使用 Detective 的安全分析師和安全工程師。

您僅能使用先前在步驟 [Step 2: Add the required IAM permissions to your account] 中連接 IAM 許可的 IAM 主體。

- `ResourceShareARN`：此欄位已預先填入。請勿變更此欄位中的值。

#### 4. 許可

**IAM 角色**：選取您在步驟 `Creating an AWS CloudFormation Service Role` 步驟中建立的角色。或者，如果您目前的 IAM 角色在步驟 `Creating an AWS CloudFormation Service Role` 中具有所有必要許可，則可以將其留空。

5. 檢閱並勾選所有我認可方塊，然後按一下建立堆疊按鈕。如需詳細資訊，請檢閱以下將建立的 IAM 資源。

```
* ResourceShareAcceptorCustomResourceFunction
  - ResourceShareAcceptorLambdaRole
  - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
  - SsmParametersLambdaRole
  - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
  - GlueDatabaseLambdaRole
  - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
  - GlueTablesLambdaRole
  - GlueTablesLogsAccessPolicy
```

步驟 4：將 Amazon S3 儲存貯體政策新增至 中的 IAM 主體 `LakeFormationPrincipals`

(選用) 如果您讓此範本為您產生 `AthenaResultsBucket`，則必須將以下政策附加至 `LakeFormationPrincipals` 中的 IAM 主體。

```
{
```

```
"Sid": "S3ObjectPermissions",
"Effect": "Allow",
"Action": [
  "s3:GetObject",
  "s3:PutObject"
],
"Resource": [
  "arn:aws:s3:::<athena-results-bucket>",
  "arn:aws:s3:::<athena-results-bucket>/*"
]
}
```

以 AthenaResultsBucket 名稱取代 athena-results-bucket 。AthenaResultsBucket 您可以在 AWS CloudFormation 主控台上找到：

1. 在 <https://console.aws.amazon.com/cloudformation> 開啟 CloudFormation 主控台。
2. 按一下堆棧。
3. 按一下資源標籤。
4. 搜尋邏輯 ID AthenaResultsBucket 並複製其實體 ID。

## 變更 Detective 整合組態

如果您想要變更任何用來整合 Detective 與 Security Lake 的參數，您可以編輯此類參數，然後再次啟用整合。您可以編輯 CloudFormation 範本，針對下列案例重新啟用此整合：

- 若要更新 Security Lake 訂閱，您可以建立新訂閱用戶，或者 Security Lake 管理員可以更新現有訂閱的資料來源。
- 若要指定不同的 Amazon S3 儲存貯體來存放原始查詢日誌。
- 指定不同 Lake Formation 的主體。

當您重新啟用與 Security Lake 的 Detective 整合時，您可以編輯資源共享 ARN，並檢視 IAM 許可。若要編輯 IAM 許可，您可以從 Detective 前往 IAM 主控台。您也可以編輯先前在 CloudFormation 範本中輸入的值。您必須刪除現有 CloudFormation 堆疊並重新建立，才能重新啟用整合。

若要重新啟用 Detective 與 Security Lake 整合

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中選擇整合。

3. 您可以使用以下其中任一步驟來編輯整合：
  - 在 Security Lake 窗格中，選擇編輯。
  - 在 Security Lake 窗格中，選擇檢視。在檢視頁面中，選擇編輯。
4. 輸入新資源共享 ARN，以存取區域中的資料來源。
5. 檢視目前的 IAM 許可，如果您想要編輯 IAM 許可，請前往 IAM 主控台。
6. 編輯 CloudFormation 範本中的值。
  1. 先刪除現有堆疊，然後再建立新堆疊。如果您未刪除現有堆疊，而且嘗試在相同區域中建立新堆疊，則您的要求會失敗。如需詳細資訊，請參閱[刪除 CloudFormation 堆疊](#)。
  1. 若要建立新 CloudFormation 堆疊。如需詳細資訊，請參閱[使用 CloudFormation 範本建立堆疊](#)。
7. 選擇啟用整合。

## 支援將 Detective 與 Security Lake 整合 AWS 的區域


您可以在下列 AWS 區域中將 Detective 與 Security Lake 整合。

區域名稱	區域	Endpoint	通訊協定；
美國東部 (俄亥俄)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
美國東部 (維吉尼亞北部)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
美國西部 (奧勒岡)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
亞太區域 (孟買)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS

區域名稱	區域	Endpoint	通訊協定 ;
亞太區域 (首爾)	ap-northeast-2	securitylake.ap-northeast-2 .amazonaws.com	HTTPS
亞太區域 (新加坡)	ap-southeast-1	securitylake.ap-southeast-1 .amazonaws.com	HTTPS
亞太區域 (雪梨)	ap-southeast-2	securitylake.ap-southeast-2 .amazonaws.com	HTTPS
亞太區域 (東京)	ap-northeast-1	securitylake.ap-northeast-1 .amazonaws.com	HTTPS
加拿大 (中部)	ca-central-1	securitylake.ca-central-1.a mazonaws.com	HTTPS
歐洲 (法蘭克福)	eu-central-1	securitylake.eu-central-1.a mazonaws.com	HTTPS
歐洲 (愛爾蘭)	eu-west-1	securitylake.eu-west-1.amaz onaws.com	HTTPS
歐洲 (倫敦)	eu-west-2	securitylake.eu-west-2.amaz onaws.com	HTTPS
Europe (Paris)	eu-west-3	securitylake.eu-west-3.amaz onaws.com	HTTPS
Europe (Stockholm)	eu-north-1	securitylake.eu-north-1.ama zonaws.com	HTTPS
南美洲 (聖保羅)	sa-east-1	securitylake.sa-east-1.amaz onaws.com	HTTPS

## 在 Detective 中查詢原始日誌

將 Detective 與 Security Lake 整合之後，Detective 會開始從 Security Lake 提取與 AWS CloudTrail 管理事件和 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌相關的原始日誌。

 Note

在 Detective 內查詢原始日誌無須額外付費。其他 AWS 服務的使用費，包括 Amazon Athena，仍以公告費率計費。

AWS CloudTrail 管理事件可用於下列設定檔：

- AWS 帳戶
- AWS 使用者
- AWS 角色
- AWS 角色工作階段
- Amazon EC2 執行個體
- Amazon S3 儲存貯體
- IP 位址
- Kubernetes 叢集
- Kubernetes Pod
- Kubernetes 主體
- IAM 角色
- IAM 角色工作階段
- IAM 使用者

Amazon VPC Flow Logs 可用於下列設定檔：

- Amazon EC2 執行個體
- Kubernetes Pod

如需如何使用 Detective 主控台將 Amazon Detective 與 Amazon Security Lake 整合的示範，請觀看下列影片：[Amazon Detective 與 Amazon Security Lake 整合 - 如何使用-->](#)

#### 查詢 AWS 帳戶的原始日誌

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，選擇搜尋，然後搜尋 AWS account。
3. 在整體 API 呼叫量區段中，選擇顯示範圍時間的詳細資訊。
4. 您可以在這裡開始查詢原始日誌。

Detective > Search > AwsAccount/714603721603

**714603721603**  
AWS account [Info](#)

Scope time [Info](#)  
12/21/2023 18:00 UTC > 12/22/2023 18:00 UTC

Activity for time window: 12/21/2023 18:00 UTC - 12/22/2023 18:00 UTC [✎](#)

[Query raw logs](#)

[Observed IP addresses](#) | [API method by service](#) | [Resource](#)

IP address	Successful calls	Failed calls	Location	Actions
▶ [redacted]	6	2	[redacted]	
▶ [redacted]	2	1	-	
▶ [redacted]	1	0	[redacted]	

在原始日誌預覽資料表中，您可以檢視透過從 Security Lake 查詢資料擷取的日誌和事件。如需有關原始事件日誌的詳細資訊，您可以檢視 Amazon Athena 中顯示的資料。

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+)

date_time	requestor_arn	account_id	region	source_ip	service	apiL
2023-12-22 09:58:38.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	s3.amazonaws.com	GetF
2023-12-22 09:59:49.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	iam.amazonaws.com	GetI
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	sts.amazonaws.com	GetC
2023-12-22 10:00:13.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	autoscaling.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC	[redacted]	[redacted]	us-east-1	[redacted]	ec2.amazonaws.com	Desc

Close

您可以在查詢原始日誌資料表中取消查詢請求、在 Amazon Athena 中查看結果以及下載結果為逗號分隔值 (.csv) 設定檔。

如果您在 Detective 中查看日誌，但查詢未傳回任何結果，這可能因以下原因造成。

- 原始日誌可能會先在 Detective 中變成可用，然後才在 Security Lake 日誌表中顯示。請稍後再試。
- Security Lake 可能會缺少日誌。如果您等待了很久的時間，則表示 Security Lake 缺少日誌。請與您的 Security Lake 管理員聯絡以解決問題。

## 範例

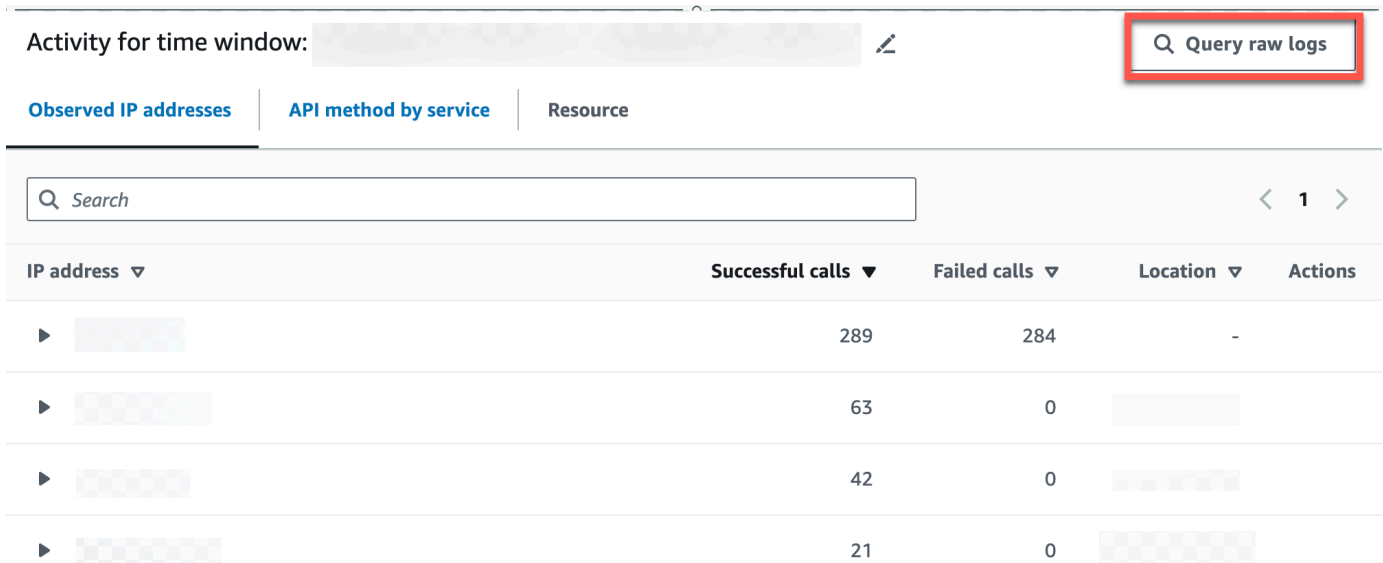
- [查詢 AWS 角色的原始日誌](#)
- [查詢 Amazon EKS 叢集的原始日誌](#)
- [查詢 Amazon EC2 執行個體的原始日誌](#)


## 查詢 AWS 角色的原始日誌

如果您想要了解新地理位置中 AWS 角色的活動，可以在 Detective 主控台中進行。

### 查詢 AWS 角色的原始日誌

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 從 Detective 摘要頁面新觀察到的地理位置區段中，記下 AWS 角色。
3. 在導覽窗格中，選擇搜尋，然後搜尋 AWS role。
4. 針對該 AWS 角色，展開 資源以顯示該資源從該 IP 地址發出的特定 API 呼叫。
5. 選擇您要調查的 API 呼叫旁邊的放大鏡圖示，以開啟原始日誌預覽表。



Activity for time window:  

[Observed IP addresses](#) | [API method by service](#) | [Resource](#)

< 1 >

IP address ▼	Successful calls ▼	Failed calls ▼	Location ▼	Actions
▶ <input type="text"/>	289	284	-	
▶ <input type="text"/>	63	0	<input type="text"/>	
▶ <input type="text"/>	42	0	<input type="text"/>	
▶ <input type="text"/>	21	0	<input type="text"/>	

## 查詢 Amazon EKS 叢集的原始日誌

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 從 Detective 摘要頁面 建立最多 Pod 的容器叢集區段中，導覽至 Amazon EKS 叢集。
3. 在 Amazon EKS 叢集詳細資訊頁面中，選取 Kubernetes API 活動索引標籤。
4. 在涉及此 Amazon EKS 叢集的整體 Kubernetes API 活動區段中，選擇範圍時間的顯示詳細資訊。
5. 您可以在此開始查詢原始日誌。

## 查詢 Amazon EC2 執行個體的原始日誌

1. 打開 Detective 主控台，網址為 <https://console.aws.amazon.com/detective/>。
2. 在導覽窗格中，選擇搜尋，然後搜尋 Amazon EC2 instance。
3. 在整體 VPC 流量區段中，選擇您要調查的 API 呼叫旁邊的放大鏡圖示，以開啟原始日誌預覽表。
4. 您可以在此開始查詢原始日誌。

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

<input type="checkbox"/>	IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Actions
<input type="checkbox"/>		22	-	44.7 kB	57.7 kB	TCP	Inbound	Accept	<input type="button" value="Q"/>
<input type="checkbox"/>		22	-	240 B	480 B	TCP	Inbound	Accept	<input type="button" value="Q"/>
<input type="checkbox"/>		22	-	61.1 kB	75 kB	TCP	Inbound	Accept	<input type="button" value="Q"/>
<input type="checkbox"/>		22	-	59.6 kB	70.8 kB	TCP	Inbound	Accept	<input type="button" value="Q"/>
<input type="checkbox"/>		22	-	240 B	540 B	TCP	Inbound	Accept	<input type="button" value="Q"/>

在原始日誌預覽資料表中，您可以檢視透過從 Security Lake 查詢資料擷取的日誌和事件。如需有關原始事件日誌的詳細資訊，您可以檢視 Amazon Athena 中顯示的資料。

您可以在查詢原始日誌資料表中取消查詢請求、在 Amazon Athena 中查看結果以及下載結果為逗號分隔值 (.csv) 設定檔。

## 停用 Detective 與 Security Lake 的整合

如果您停用與 Security Lake 的 Detective 整合，您將無法再從 Security Lake 查詢日誌和事件資料。

## 若要停用 Detective 與 Security Lake 整合

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Detective 主控台。
2. 在導覽窗格中選擇整合。
3. 刪除現有的堆疊。如需詳細資訊，請參閱[刪除 CloudFormation 堆疊](#)。
4. 在停用 Security Lake 整合窗格中，選擇停用。

## 刪除 CloudFormation 堆疊

如果您不刪除現有堆疊，則系統將無法在相同區域中建立新堆疊。您可以使用 CloudFormation 主控台或使用 AWS CLI 來刪除 CloudFormation 堆疊。

### 刪除 CloudFormation 堆疊 ( 主控台 )

1. 開啟位於 <https://console.aws.amazon.com/cloudformation> 的 AWS CloudFormation 主控台。
2. 在 CloudFormation 主控台的 Stacks (堆疊) 頁面上，選取您要刪除的堆疊。此堆疊目前必須正在執行。
3. 在 stack details (堆疊詳細資訊) 窗格中，選擇 Delete (刪除)。
4. 當系統提示時，選取 Delete stack (刪除堆疊)。

#### Note

堆疊刪除操作開始後將無法停止。堆疊繼續進行到 DELETE\_IN\_PROGRESS (正在刪除) 狀態。

在堆疊刪除完成之後，堆疊即處於 DELETE\_COMPLETE (刪除完成) 狀態。

### 堆疊刪除錯誤疑難排解

如果您在按一下 Delete 按鈕後看到訊息 (Failed to delete stack) 存在許可錯誤，表示您的 IAM 角色未具備刪除堆疊的 CloudFormation 許可。請聯絡您的帳戶管理員以刪除堆疊。

### 刪除 CloudFormation 堆疊 (AWS CLI)

在 CLI AWS 界面中輸入下列命令：

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

CFN-DetectiveSecurityLakeIntegration 是您在步驟 [Creating an AWS CloudFormation Service Role](#) 中建立的服務角色。

# 預測和監控 Detective 成本

為了協助您追蹤 Detective 活動，用量頁面會顯示擷取的資料量和預計成本。

- 針對管理員帳戶，用量頁面會顯示整個行為圖表中的資料量和預計成本。
- 針對成員帳戶，用量頁面會在其提供的行為圖表中顯示其帳戶的資料量和預計成本。

Detective 也支援 AWS CloudTrail 記錄。

## 目錄

- [關於行為圖表的免費試用](#)
- [監控 Detective 管理員帳戶的使用情況](#)
- [監控 Detective 會員帳戶的使用情況](#)
- [Amazon Detective 如何計算預計成本](#)

## 關於行為圖表的免費試用

Amazon Detective 為每個區域的各個帳戶提供 30 天的免費試用。首次發生以下動作之一時，帳戶的免費試用即開始。

- 帳戶會手動啟用 Detective，並成為行為圖表的管理員帳戶。
- 帳戶會被指定為 AWS Organizations 中組織的 Detective 管理員帳戶，且將首次啟用 Detective。
- 如果 Detective 管理員帳戶在指定 Detective 之前已啟用 Detective，則該帳戶不會開始全新 30 天免費試用。
- 帳戶接受邀請成為行為圖表中的成員帳戶，並啟用為成員帳戶。
- 組織帳戶會由 Detective 管理員帳戶啟用為成員帳戶。

屆時起，即開始 30 天的免費試用。該帳戶不會針對該期間內處理的任何資料收費。當試用結束時，Detective 會開始向帳戶針對它向行為圖表提供的資料收取費用。如需如何追蹤 Detective 活動、監控用量並查看預計成本的詳細資訊，請參閱 [預測和監控 Detective 成本](#)。如需定價的詳細資訊，請參閱 [Detective 定價](#)。

區域中的所有行為圖表都會使用相同的 30 天期間。例如，帳戶已啟用為行為圖表的成員帳戶。即開始 30 天的免費試用。10 天後，帳戶會在相同區域中啟用第二個行為圖表。對於第二個行為圖表，帳戶會收到 20 天的免費資料。

免費試用提供多種優勢：

- 管理員帳戶可以探索 Detective 功能，以驗證其價值。
- 管理員和成員帳戶可以在 Detective 開始向他們收取費用之前，監控資料量和估計費用。請參閱 [the section called “管理員帳戶用量和費用”](#) 和 [the section called “成員帳戶用量追蹤”](#)。

## 選用的資料來源的免費試用

Detective 還為選用的資料來源提供 30 天的免費試用。該免費試用與首次啟用 Detective 時為核心 Detective 資料來源提供的免費試用不同。

### Note

如果客戶在啟用選用的資料來源套件後 7 天內停用選用資料來源套件，則 Detective 會對該資料來源套件執行一次性自動重設免費試用 (如果再次啟用)。

若要啟用或停用選用的資料來源，請參閱 [Detective 中選用的資料來源的類型](#)。

## 監控 Detective 管理員帳戶的使用情況

Amazon Detective 會針對帳戶所屬的每個行為圖表中使用的資料，向每個帳戶收取費用。無論來源為何，Detective 都會針對所有資料按每 GB 收取分層統一費率。

對於管理員帳戶，透過 Detective 主控台的用量頁面，您可以依資料來源或依帳戶檢視過去 30 天內擷取的資料量。管理員帳戶還會查看其帳戶常規 30 天期間以及整個行為圖表的預計成本。

若要檢視 Detective 用量資訊

1. 登入 AWS 管理主控台。然後開啟 Detective 主控台的位置 <https://console.aws.amazon.com/detective/>。
2. 在 Detective 導覽窗格中的設定下，選擇用量。
3. 選擇標籤以依資料來源或依帳戶選取檢視用量。

## 為每個帳戶擷取的資料量

依成員帳戶擷取的資料量會在行為圖表中列出作用中帳戶。它不會列出已移除的成員帳戶。

針對每個帳戶，擷取的資料量清單會提供以下資訊。

- AWS 帳號識別碼和 root 使用者電子郵件地址。
- 帳戶開始向行為圖表提供資料的日期。

針對管理員帳戶，日期為帳戶啟用 Detective 的日期。

針對成員帳戶，日期為在接受邀請後啟用帳戶作為成員帳戶的日期。

- 過去 30 天內從帳戶擷取的資料量。總計包括所有來源類型。
- 該帳戶目前是否處於免費試用期。針對目前處於免費試用期的帳戶，清單會顯示剩餘天數。

如果無帳戶處於免費試用其，則系統不會顯示免費試用狀態欄位。

## 行為圖表的預計成本

此帳戶的預計成本會顯示管理員帳戶 30 天資料的預計成本。預計成本根據管理員帳戶的每日平均值而定。

### Important

此金額僅為預計成本。它會預測管理員帳戶資料在 30 天期間內的總常規成本。它基於前 30 天的用量。請參閱 [the section called “Detective 如何計算預計成本”](#)。

## 行為圖表的預計成本

所有帳戶的預計成本會針對整個行為圖表顯示 30 天資料的總預計成本。預計成本根據每個帳戶的每日平均值而定。

### Important

此金額僅為預計成本。它會預測行為圖表資料在 30 天期間內的總常規成本。它基於前 30 天的用量。預計成本不包括從行為圖表中移除的成員帳戶。請參閱 [the section called “Detective 如何計算預計成本”](#)。

## 來源套件擷取的資料量

選取依來源套件可檢視行為圖表中啟用的不同來源套件所列出的擷取資料量。

所有帳戶都可以檢視自己帳戶的此類資料。管理員帳戶可以查看列出每個成員來源套件用量的其他面板。它不會列出已移除的成員帳戶。

### Detective 核心

Detective 核心面板會顯示過去 30 天從 Detective 核心來源 (CloudTrail 記錄、VPC 流程記錄和 GuardDuty 發現項目) 擷取的資料量。

### EKS 稽核日誌

EKS 稽核記錄面板會顯示過去 30 天從 EKS 稽核記錄來源擷取的資料量。只有在您的行為圖表啟用 EKS 稽核記錄時，才能使用此來源套件的面板。

## 監控 Detective 會員帳戶的使用情況

Amazon Detective 會針對帳戶所屬的每個行為圖表中使用的資料，向每個帳戶收取費用。無論來源為何，Detective 都會針對所有資料按每 GB 收取分層統一費率。

針對成員帳戶，用量頁面僅顯示該帳戶的資料量和預計 30 天的費用。

若要檢視 Detective 用量資訊

1. 登入 AWS 管理主控台。然後開啟 Detective 主控台的位置 <https://console.aws.amazon.com/detective/>。
2. 在 Detective 導覽窗格中的設定下，選擇用量。

## 每個行為圖表的擷取量

此帳戶的擷取量會列出成員帳戶提供的行為圖表。它不包括您放棄的成員資格或管理員帳戶移除的成員資格。

針對每個行為圖表，清單包含以下資訊：

- 管理員帳戶的帳號
- 過去 30 天內從成員帳戶擷取的資料量。總計包括所有來源類型。

- 成員帳戶啟用行為圖表的日期。

## 跨行為圖表的預計成本

此帳戶的預計成本會在其提供的所有行為圖表中，顯示成員帳戶 30 天資料的預計成本。預計成本根據成員帳戶的每日平均值而定。

### Important

此金額僅為預計成本。它會預測管理員帳戶資料在 30 天期間內的總常規成本。它基於前 30 天的用量。請參閱[the section called “Detective 如何計算預計成本”](#)。

## Amazon Detective 如何計算預計成本

若要計算它顯示在用量頁面上顯示的預計成本值，Detective 會執行以下動作。

1. 若要在行為圖表中取得個別帳戶的預計成本，Detective 會執行以下動作。
  - a. 計算每天的平均值。它會在所有作用中日期中新增資料量，然後除以帳戶處於作用中狀態的天數。

如果帳戶在 30 天前已啟用，則天數為 30 天。如果帳戶的啟用時間短於 30 天，則天數為該帳戶自接受日期以來的天數。

例如，如果帳戶在 12 天前啟用，則 Detective 會新增 12 天內所擷取的資料量，然後將其除以 12。
  - b. 將帳戶的每日平均值乘以 30。所得即為帳戶的預計 30 天使用量。
  - c. 使用其定價模式來計算預計 30 天使用量的預計 30 天成本。
2. 若要取得行為圖表的總預計成本，Detective 會執行以下動作：
  - a. 在行為圖表中合併所有帳戶的預計 30 天使用量。
  - b. 使用其定價模式來計算總預計 30 天使用量的預計 30 天成本。
3. 若要跨行為圖表取得成員帳戶的總預計成本，Detective 會執行以下動作：
  - a. 在所有行為圖表中合併預計 30 天使用量。
  - b. 使用其定價模式來計算總預計 30 天使用量的預計 30 天成本。
4. 如果您使用共用 Amazon VPC，Detective 會根據監控活動計算預計成本。建議您檢閱您環境專屬調查的預計成本。

- a. 如果 Detective 成員帳戶擁有共用 Amazon VPC，而且還有其他非 Detective 帳戶使用共用 VPC，則 Detective 將監控來自該 VPC 的所有流量。用量和成本將會增加，而 Detective 會對 VPC 內的所有流量流程提供視覺效果。
- b. 如果您的共用 Amazon VPC 內有 EC2 執行個體，而共用擁有者不是 Detective 成員，則 Detective 不會監控來自 VPC 的任何流量，而且用量和成本也會減少。如果您想要檢視 VPC 內的流量流程，則必須將 Amazon VPC 擁有者新增為 Detective 圖形的成員。

# Amazon Detective 中的安全

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#) 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。

在 [AWS 合規計畫](#) 中，第三方稽核員會定期測試並驗證我們的安全功效。

若要了解適用於 Amazon Detective 的合規計畫，請參閱[合規計畫範圍內的 AWS 服務](#)。

- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Detective 時套用共同責任模型。以下主題說明如何將 Detective 設定為達到您的安全及法規遵循目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Detective 資源。

## 目錄

- [Amazon Detective 中的資料保護](#)
- [Amazon Detective 的身分和存取管理](#)
- [Amazon Detective 的合規驗證](#)
- [Amazon Detective 中的彈性](#)
- [Amazon Detective 的基礎設施安全](#)
- [Amazon Detective 和介面 VPC 端點 \(AWS PrivateLink\)](#)
- [Detective 的安全最佳實務](#)

## Amazon Detective 中的資料保護

所以此 AWS [共同責任模型](#) 適用於 Amazon Detective 中的資料保護。如本模型所述，AWS 負責保護運行所有的全球基礎設施 AWS 雲端。您有責任維持對託管在此基礎結構上的內容的控制權。您也必須負責 AWS 服務 您使用的。如需有關資料隱私權的詳細資訊，請參閱資料[隱私權FAQ](#)。如需歐洲資料保護的相關資訊，請參閱 [AWS 共同責任模型和GDPR](#) 博客文章 AWS 安全部落格。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM)。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱[使用 CloudTrail 系統線](#) AWS CloudTrail 使用者指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當你與 Detective 或其他工作 AWS 服務 使用控制台API，AWS CLI，或 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

Detective 會加密其處理和存儲在靜態和傳輸中的所有資料。

## 目錄

- [Amazon Detective 的金鑰管理](#)

## Amazon Detective 的金鑰管理

因為 Detective 不會儲存任何可識別個人身分的客戶資料，所以它會使用 AWS 受管金鑰。

此類型的 KMS 金鑰可跨多個帳戶使用。請參閱[開 AWS Key Management Service 發人員指南中 AWS 擁有金鑰的說明](#)。

此類型的 KMS 金鑰每年 (大約 365 天) 會自動輪換。請參閱[開 AWS Key Management Service 發人員指南中關於金鑰輪換的說明](#)。

# Amazon Detective 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可以控制完成身分驗證 (已登入) 和獲得授權 (具有許可) 而得以使用 Detective 資源的對象。IAM 是 AWS 服務 您可以免費使用的。

## 目錄

- [目標對象](#)
- [使用身分來驗證](#)
- [使用政策管理存取權](#)
- [Amazon Detective 如何搭配 IAM 運作](#)
- [Amazon Detective 身分型政策範例](#)
- [AWS Amazon Detective 的 受管政策](#)
- [使用 Detective 的服務連結角色](#)
- [Amazon Detective 身分識別和存取疑難排解](#)

## 目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [Amazon Detective 身分識別和存取疑難排解](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [Amazon Detective 如何搭配 IAM 運作](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [Amazon Detective 身分型政策範例](#))

## 使用身分來驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的 [如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [API 請求的AWS 第 4 版簽署程序](#)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的 [需要根使用者憑證的任務](#)。

## IAM 使用者和群組

IAM 使用者 [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html) 是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 [要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#) 會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 使用者的使用案例](#)。

## IAM 角色

IAM 角色 [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html) 的身分具有特定許可權，其可以提供臨時憑證。您可以透過 [從使用者切換到 IAM 角色（主控台）](#) 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

## 使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 [JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

## 身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

## 資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》中的[存取控制清單 \(ACL\) 概觀](#)。

## 其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

## 多種政策類型

當多種類型的政策套用到請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

## Amazon Detective 如何搭配 IAM 運作

根據預設，使用者和角色不具備建立或修改 Amazon Detective 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。Detective 管理員必須具有 AWS Identity and Access Management (IAM) 政策，授予 IAM 使用者和角色許可，以對他們所需的指定資源執行特定 API 操作。管理員接著必須將這些政策連接至需要此類許可的主體。

Detective 使用 IAM 身分型政策，為以下類型的使用者和動作授予許可：

- **管理員帳戶：**管理員帳戶是行為圖表的擁有者，可使用其帳戶中的資料。管理員帳戶可以邀請成員帳戶將其資料提供至行為圖表。管理員帳戶也可以使用行為圖表來分類和調查與這些帳戶相關聯的問題清單和資源。

您可以設定政策以允許管理員帳戶以外的使用者執行不同類型的工作。例如，來自管理員帳戶的使用者可能只有管理成員帳戶的許可。其他使用者可能只有使用行為圖表進行調查的許可。

- **成員帳戶：**成員帳戶是受邀為行為圖表提供資料的帳戶。成員帳戶會回應邀請。接受邀請後，成員帳戶可以從行為圖表中移除其帳戶。

若要全面了解 Detective 和其他 AWS 服務 如何使用 IAM，請參閱《IAM 使用者指南》中的[在 JSON 標籤上建立政策](#)。

## Detective 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Detective 支援特定動作、資源和條件金鑰。

若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的[JSON 政策元素參考](#)。

### 動作

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

政策陳述式必須包含 Action 或 NotAction 元素。Action 元素會列出政策允許的動作。NotAction 元素會列出不允許的動作。

針對 Detective 定義的動作反映了您可以使用 Detective 執行的工作。Detective 中的政策動作具有以下前綴：detective:。

例如，若要授予使用 CreateMembers API 操作邀請成員帳戶加入行為圖表的許可，您應在其政策中加入 detective:CreateMembers 動作。

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，對於成員帳戶，政策包括與管理邀請相關的一組動作：

```
"Action": [
    "detective:ListInvitations",
    "detective:AcceptInvitation",
    "detective:RejectInvitation",
    "detective:DisassociateMembership"
]
```

您可以使用萬用字元 (\*) 來指定多個動作。例如，若要管理其行為圖表中使用的資料，Detective 中的管理員帳戶必須能夠執行以下工作：

- 檢視他們的成員帳戶清單 (ListMembers)。
- 取得已選取成員帳戶的資訊 (GetMembers)。
- 邀請成員帳戶至其行為圖表 (CreateMembers)。
- 從成員的行為圖表 (DeleteMembers) 中移除成員。

您可以向以文字 Members 結尾的所有動作授予存取，而無需個別列出此類動作。該政策可能包括以下動作：

```
"Action": "detective:*Members"
```

若要查看 Detective 動作的清單，請參閱《服務授權參考》中的 [由 Amazon Detective 定義的動作](#)。

## Resources

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (\*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

如需 ARNs 格式的詳細資訊，請參閱 [Amazon Resource Name \(ARNs AWS 和服務命名空間\)](#)。

針對 Detective，唯一的資源類型是行為圖表。Detective 中的行為圖表資源具有以下 ARN：

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

例如，行為圖表具有以下值：

- 行為圖表的區域是 us-east-1。
- 管理員帳戶 ID 的帳戶 ID 為 111122223333。
- 行為圖表的圖表 ID 是 027c7c4610ea4aacaf0b883093cab899。

若要在 Resource 陳述式中識別此行為圖表，您可以使用以下 ARN：

```
"Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

若要在 Resource 陳述式中指定多項資源，請使用逗號進行分隔。

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

例如，同一個 AWS 帳戶可能會受邀成為多個行為圖表中的成員帳戶。在該成員帳戶的政策中，Resource 陳述式將列出帳戶被邀請使用的行為圖表。

```
"Resource": [  
    "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",  
    "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"  
]
```

建立行為圖表、列出行為圖表和列出行為圖表邀請等部分 Detective 動作不會在特定行為圖表上執行。對於此類動作，Resource 陳述式必須使用萬用字元 (\*)。

```
"Resource": "*"
```

針對管理員帳戶動作，Detective 一律會驗證提出要求的使用者是否屬於受影響行為圖表的管理員帳戶。對於成員帳戶動作，Detective 始終會驗證發出請求的使用者是否屬於該成員帳戶。即使 IAM 政策向行為圖表授予存取權，但如果使用者不屬於正確的帳戶，使用者也無法執行動作。

針對在特定行為圖表上執行的所有動作，IAM 政策應包含圖表 ARN。圖表 ARN 可以在以後新增。例如，當帳戶首次啟用 Detective 時，初始 IAM 政策會使用圖表 ARN 的萬用字元，向所有 Detective 動作提供存取。透過此舉，使用者可以立即開始管理其行為圖表中的成員帳戶並進行調查。建立行為圖表之後，您可以更新政策以新增圖表 ARN。

### 條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用[條件運算子](#)的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的[AWS 全域條件內容索引鍵](#)。

Detective 不會定義自己的條件金鑰組。其會支援使用某些全域條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的[AWS 全域條件內容金鑰](#)。

若要了解您可以搭配哪些動作和資源使用條件金鑰，請參閱 [Amazon Detective 定義的動作](#)。

### 範例

若要檢視 Detective 身分型政策範例，請參閱 [Amazon Detective 身分型政策範例](#)。

### Detective 資源型政策 (不支援)。

Detective 不支援資源型政策。

### 基於 Detective 行為圖表標籤的授權

每個行為圖表都可以分配標籤值。您可以在條件陳述式中使用此類標籤值，來管理行為圖表的存取權。

標籤值的條件陳述式使用以下格式。

```
{"StringEquals":{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

例如，當 Department 標籤值為 Finance 時，使用以下程式碼來允許或拒絕動作。

```
{"StringEquals":{"aws:ResourceTag/Department": "Finance"}}
```

如需使用資源標籤值的政策範例，請參閱 [the section called “管理員帳戶：根據標籤值限制存取許可”](#)。

## Detective IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

將臨時憑證與 Detective 搭配使用

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 [AssumeRole](#) 或 [GetFederationToken](#) 等 AWS STS API 操作來取得臨時安全登入資料。

Detective 支援使用臨時憑證。

### 服務連結角色

[服務連結角色](#)可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Detective 服務連結角色的詳細資訊，請參閱 [the section called “使用服務連結角色”](#)。

### 服務角色 (不支援)

此功能可讓服務代表您擔任[服務角色](#)。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Detective 不支援服務角色。

## Amazon Detective 身分型政策範例

根據預設，IAM 使用者和角色不具備建立或修改 Detective 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。

IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將此類政策附加至需要此類許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[在 JSON 索引標籤上建立政策](#)。

## 主題

- [政策最佳實務](#)
- [使用 Detective 主控台](#)
- [允許使用者檢視自己的許可](#)
- [管理員帳戶：在行為圖表中管理成員帳戶](#)
- [管理員帳戶：使用行為圖表進行調查](#)
- [成員帳戶：管理行為圖表邀請和成員資格](#)
- [管理員帳戶：根據標籤值限制存取許可](#)

## 政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Detective 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

## 使用 Detective 主控台

若要使用 Amazon Detective 主控台，使用者或角色必須能夠存取相關動作，此類動作與 API 中的對應動作相符。

若要啟用 Detective 並成為行為圖表的管理員帳戶，必須向使用者或角色授予 CreateGraph 動作的許可。

若要使用 Detective 主控台執行任何管理員帳戶動作，必須向使用者或角色授予 ListGraphs 動作的許可。這會授予擷取其帳戶為管理員帳戶行為圖表的許可。他們也必須獲得執行特定管理員帳戶動作的許可。

最基本的管理員帳戶動作是檢視行為圖表中的成員帳戶清單，並使用行為圖表進行調查。

- 若要檢視行為圖表中的成員帳戶清單，必須向主體授予 ListMembers 動作的許可。
- 若要在行為圖表中進行調查，必須向主體授予 SearchGraph 動作的許可。

若要使用 Detective 主控台執行任何成員帳戶動作，必須向使用者或角色授予 ListInvitations 動作的許可。這會授予檢視行為圖表邀請的許可。然後，他們可以被授予特定成員帳戶動作的許可。

## 允許使用者檢視自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
  "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": "*"
    }
  ]
}

```

## 管理員帳戶：在行為圖表中管理成員帳戶

此範例政策適用於僅負責管理行為圖表中使用的成員帳戶的管理員帳戶使用者。透過此政策，使用者也可以檢視用量資訊，並停用 Detective。此政策未授予使用行為圖表進行調查的許可。

## JSON

```

{"Version":"2012-10-17",
 "Statement":[
  {
    "Effect":"Allow",
    "Action":
    ["detective:ListMembers","detective:CreateMembers","detective>DeleteMembers","detective:D
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}

```

## 管理員帳戶：使用行為圖表進行調查

此範例政策適用於僅使用行為圖表進行調查的管理員帳戶使用者。他們無法檢視或編輯行為圖表中的成員帳戶清單。

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["detective:SearchGraph"],
      "Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
    },
    {
      "Effect": "Allow",
      "Action": ["detective:ListGraphs"],
      "Resource": "*"
    }
  ]
}
```

## 成員帳戶：管理行為圖表邀請和成員資格

此範例政策適用於屬於成員帳戶的使用者。在此範例中，成員帳戶屬於兩個行為圖表。此政策會授予回應邀請並從行為圖表中移除成員帳戶的許可。

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:RejectInvitation",
        "detective:DisassociateMembers"
      ],
      "Resource": [
        "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",

```

```

    "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"
  ]
},
{
  "Effect": "Allow",
  "Action": ["detective:ListInvitations"],
  "Resource": "*"
}
]
}

```

## 管理員帳戶：根據標籤值限制存取許可

如果行為圖表的 SecurityDomain 標籤符合使用者的 SecurityDomain 標籤，透過以下政策，使用者可以使用行為圖表進行調查。

## JSON

```

{
  "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": "*"
    }
  ]
}

```

```
    }  
  ]  
}
```

如果行為圖表的 SecurityDomain 標籤值為 Finance，以下政策可防止使用者使用行為圖表進行調查。

JSON

```
{  
  "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 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

## AWS 受管政策：AmazonDetectiveFullAccess

您可將 AmazonDetectiveFullAccess 政策連接到 IAM 身分。

此政策會授予管理許可，允許主體完整存取所有 Amazon Detective 動作。您可以將此政策附加到主體，然後再針對帳戶啟用 Detective。它還必須附加到用於執行 Detective Python 指令碼以建立和管理行為圖表的角色。

具有此類許可的主體可以管理成員帳戶、將標籤新增至其行為圖表，以及使用 Detective 進行調查。他們還可以封存 GuardDuty 調查結果。政策提供 Detective 主控台顯示所在帳戶的帳戶名稱所需的許可 AWS Organizations。

### 許可詳細資訊

此政策包含以下許可：

- `detective`：允許主體完整存取所有 Detective 動作。
- `organizations`：允許主體從組織中擷取針對帳戶的 AWS Organizations 資訊。如果帳戶屬於某個組織，除了帳號之外，此類許可還允許 Detective 主控台顯示帳戶名稱。
- `guarddduty`：允許主體從 Detective 內部取得和封存 GuardDuty 調查結果。
- `securityhub` – 允許主體從 Detective 中取得 Security Hub CSPM 問題清單。

### JSON

```
{
  "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 受管政策：AmazonDetectiveMemberAccess

您可將 AmazonDetectiveMemberAccess 政策附加至 IAM 實體。

此政策會向成員提供 Amazon Detective 的存取，以及主控台的特定範圍存取。

使用此政策，您可以：

- 檢視向 Detective 圖表成員發出的邀請，並接受或拒絕邀請。
- 在用量頁面查看您在 Detective 中的活動如何影響使用此服務的成本。
- 放棄圖表中的成員資格。

此政策授予唯讀許可，允許在一定範圍內存取 Detective 主控台。

### 許可詳細資訊

此政策包含以下許可：

- `detective` : 允許成員存取 Detective。

## JSON

```
{
  "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 受管政策：AmazonDetectiveInvestigatorAccess

您可將 AmazonDetectiveInvestigatorAccess 政策附加至 IAM 實體。

此政策向調查人員提供對 Detective 服務的存取，以及 Detective 主控台 UI 相依性的特定範圍存取。此政策授予在 Detective 中對 IAM 使用者和 IAM 角色啟用 Detective 調查的許可。您可以使用調查報告來調查以識別調查結果等入侵指標，該報告提供有關安全指標的分析和見解。該報告按嚴重性進行排名，由 Detective 的行為分析和機器學習決定。您可以使用報告來排定資源修補的優先順序。

### 許可詳細資訊

此政策包含以下許可：

- `detective`：允許主體調查者存取 Detective 動作，以啟用 Detective 調查，以及啟用調查結果群組摘要。
- `guardduty`：允許主體從 Detective 內部取得和封存 GuardDuty 調查結果。
- `securityhub` – 允許主體從 Detective 中取得 Security Hub CSPM 問題清單。
- `organizations` – 允許主體從中擷取組織中帳戶的相關資訊 AWS Organizations。如果帳戶屬於某個組織，則除了帳號之外，此類許可還允許 Detective 主控台顯示帳戶名稱。

JSON

```
{
  "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 受管政策 : AmazonDetectiveOrganizationsAccess

您可將 AmazonDetectiveOrganizationsAccess 政策附加至 IAM 實體。

此政策授予在組織內啟用和管理 Amazon Detective 的許可。您可以在整個組織中啟用 Detective，並決定 Detective 的委派管理員帳戶。

## 許可詳細資訊

此政策包含以下許可：

- `detective`：允許主體存取 Detective 動作。
- `iam`：指定在 Detective 呼叫 `EnableOrganizationAdminAccount` 時建立服務連結角色。
- `organizations` – 允許主體從中擷取組織中帳戶的相關資訊 AWS Organizations。如果帳戶屬於某個組織，則除了帳號之外，此類許可還允許 Detective 主控台顯示帳戶名稱。啟用 AWS 服務的整合、允許以委派管理員身分註冊和取消註冊指定的成員帳戶，以及允許委託人擷取 Amazon Detective、Amazon GuardDuty、Amazon Macie 和 等其他安全服務中的委派管理員帳戶 AWS Security Hub CSPM。

## JSON

```
{
  "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 受管政策：AmazonDetectiveServiceLinkedRole

您無法將 AmazonDetectiveServiceLinkedRole 政策附加至 IAM 實體。此政策會附加到服務連結角色，透過該角色，Detective 可代表您執行動作。如需詳細資訊，請參閱 [the section called “使用服務連結角色”](#)。

此政策會授予管理許可，允許服務連結角色擷取組織的帳戶資訊。

許可詳細資訊

此政策包含以下許可：

- organizations：擷取組織的帳戶資訊。

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    }
  ]
}
```

## AWS 受管政策的偵測更新

檢視自此服務開始追蹤這些變更以來 Detective AWS 受管政策更新的詳細資訊。如需自動收到有關此頁面變更的提醒，請前往 [文件歷史記錄頁面](#) 上訂閱 RSS 摘要。

變更	描述	Date
<a href="#">AmazonDetectiveInvestigatorAccess</a> : 現有政策的更新	<p>在 AmazonDetectiveInvestigatorAccess 政策中新增了 Detective 調查和調查結果群組摘要動作。</p> <p>此類動作允許啟動，擷取和更新 Detective 調查結果並從 Detective 內部獲得調查結果群組的摘要。</p>	2023 年 11 月 26 日
<a href="#">AmazonDetectiveFullAccess</a> 和 <a href="#">AmazonDetectiveInvestigatorAccess</a> – 對現有政策的更新	<p>Detective 已將 Security Hub CSPM GetFindings 動作新增至 AmazonDetectiveFullAccess 和 AmazonDetectiveInvestigatorAccess 政策。</p> <p>這些動作允許從 Detective 內取得 Security Hub CSPM 調查結果。</p>	2023 年 5 月 16 日
<a href="#">AmazonDetectiveOrganizationsAccess</a> – 新政策	<p>Detective 新增了 AmazonDetectiveOrganizationsAccess 政策。</p> <p>此政策授予在組織內啟用和管理 Detective 的許可</p>	2023 年 3 月 2 日
<a href="#">AmazonDetectiveMemberAccess</a> – 新政策	<p>Detective 新增了 AmazonDetectiveMemberAccess 政策。</p> <p>此政策會向成員提供 Detective 的存取，以及主控台 UI 依存關係的特定範圍存取。</p>	2023 年 1 月 17 日
<a href="#">AmazonDetectiveFullAccess</a> : 現有政策的更新	<p>Detective 向 AmazonDetectiveFullAccess 政策新增了 GuardDuty GetFindings 動作。</p>	2023 年 1 月 17 日

變更	描述	Date
	透過此類動作，可從 Detective 內部取得 GuardDuty 調查結果。	
<a href="#">AmazonDetectiveInvestigator Access</a> – 新政策	Detective 新增了 AmazonDetectiveInvestigator Access 政策。  透過此類政策，主體可在 Detective 中進行調查。	2023 年 1 月 17 日
<a href="#">AmazonDetectiveServiceLinkedRole</a> – 新政策	Detective 為其服務連結角色新增了新政策。  透過政策，服務連結角色可以擷取組織中帳戶的相關資訊。	2021 年 12 月 16 日
Detective 開始追蹤變更	Detective 開始追蹤其 AWS 受管政策的變更。	2021 年 5 月 10 日

## 使用 Detective 的服務連結角色

Amazon Detective 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Detective 的一種特殊 IAM 角色類型。服務連結角色由 Detective 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可簡化 Detective 的設定，因為您不必手動新增必要的許可。Detective 定義其服務連結角色的許可，除非另有定義，否則僅有 Detective 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。如此可保護您 Detective 的資源，避免您不小心移除資源的存取許可。

如需支援服務連結角色的其他服務資訊，請參閱[可搭配 IAM 運作的 AWS 服務](#)，並尋找服務連結角色欄位顯示是的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

## Detective 的服務連結角色許可

Detective 使用名為 `AWSServiceRoleForDetective` 的服務連結角色 – 允許 Detective 代表您存取 AWS Organizations 資訊。

`AWSServiceRoleForDetective` 服務連結角色信任以下服務可擔任該角色：

- `detective.amazonaws.com`

`AWSServiceRoleForDetective` 服務連結角色會使用受管政策，即 [AmazonDetectiveServiceLinkedRolePolicy](#)。

如需 `AmazonDetectiveServiceLinkedRolePolicy` 政策更新的詳細資訊，請參閱 [Amazon Detective AWS 受管政策的更新](#)。如需此政策變更的自動提醒，請訂閱 [Detective 文件歷史記錄](#) 頁面上的 RSS 摘要。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。

### 為 Detective 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS CLI、或 AWS API 中為組織指定 Detective AWS 管理主控台管理員帳戶時，Detective 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您為組織指定 Detective 管理員帳戶時，Detective 可再次為您建立服務連結角色。

### 為 Detective 編輯服務連結角色

Detective 不允許您編輯 `AWSServiceRoleForDetective` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

### 為 Detective 刪除服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

**Note**

若 Detective 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後，然後再次嘗試操作。

若要刪除 AWSServiceRoleForDetective 所使用的 Detective 資源

1. 移除 Detective 管理員帳戶。請參閱 [the section called “指定 Detective 管理員帳戶”](#)。
2. 在您指定 Detective 管理員帳戶的每個區域中重複此程序。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、或 AWS API 來刪除 AWSServiceRoleForDetective 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

Detective 服務連結角色支援的區域

Detective 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 [AWS 區域與端點](#)。

## Amazon Detective 身分識別和存取疑難排解

請參考以下資訊，診斷及修正使用 Detective 和 IAM 時可能發生的常見問題。如果您在使用 AWS Identity and Access Management(IAM) 時遇到存取遭拒問題或類似困難，請參閱 [《IAM 使用者指南》中的疑難排解](#) IAM 主題。

我未獲授權，不得在 Detective 中執行動作

如果 AWS 管理主控台告知您無權執行動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

以下範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台接受成為行為圖表成員帳戶的邀請，但卻無 `detective:AcceptInvitation` 許可時發生。

```
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
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `arn:aws:detective:us-east-1:444455556666:graph:567856785678` 動作存取 `detective:AcceptInvitation` 資源。

## 我未獲得執行 `iam:PassRole` 的授權

如果錯誤訊息告知您未獲得授權，無法執行 `iam:PassRole` 動作，您必須更新政策，以允許您將角色傳遞給 Detective。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 Detective 中執行動作時，會發生以下範例所示的錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想要允許 AWS 帳戶外的人員存取我的 Detective 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Detective 是否支援此類功能，請參閱 [Amazon Detective 如何搭配 IAM 運作](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 [《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 [《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 [《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

## Amazon Detective 的合規驗證

Amazon Detective 位於 AWS 保證計畫的範圍內。如需詳細資訊，請參閱 [Health Information Trust Alliance Common Security Framework \( HITRUST \) CSF](#)。

如需特定合規計畫範圍內 AWS 的服務清單，請參閱依 [AWS 合規計畫範圍內的合規計畫](#) 如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 [AWS Artifact 中](#) 下載 Artifact 中下載。

AWS 提供下列資源以協助合規：

- [安全與合規快速入門指南](#) – 安全與合規指南討論架構考量，並提供在 上部署以安全與合規為重點的基準環境的步驟 AWS。
- 使用 AWS Config 開發人員指南 中的 [規則評估資源](#) – AWS Config 服務會評估資源組態是否符合內部實務、產業準則和法規。
- [AWS Security Hub CSPM](#) – AWS 此服務提供安全狀態的全面檢視 AWS ，可協助您檢查是否符合安全產業標準和最佳實務。

## Amazon Detective 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置的。AWS 區域提供多個實體隔離和隔離的可用區域，這些區域以低延遲、高輸送量和高度備援的網路連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施之外，Detective 還使用 Amazon DynamoDB 和 Amazon Simple Storage Service (Amazon S3) 內建的彈性。如需詳細資訊，請參閱 [Amazon DynamoDB 中的彈性和災難復原](#)，以及 [Amazon Simple Storage Service 中的彈性](#)。

Detective 架構也可以抵禦單一可用區域的故障。彈性內置於 Detective 中，不需要任何組態。

## Amazon Detective 的基礎設施安全

Amazon Detective ； 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Detective。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

## Amazon Detective 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 VPC 和 Amazon Detective 之間建立私有連線。介面端點採用 [AWS PrivateLink](#) 技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連接的情況下私下存取 Detective APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Detective APIs 通訊。VPC 和 Detective 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

## Detective VPC 端點的考量事項

設定 Detective 的介面 VPC 端點之前，請務必檢閱 AWS PrivateLink 指南中的[介面端點屬性和限制](#)。

Detective 支援從您的 VPC 呼叫其所有 API 動作。

Detective 在下列區域中支援 FIPS：

- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 加拿大 (中部)

## 建立 Detective 的介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface ( ) 為 Detective 服務建立 VPC 端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「[建立介面端點](#)」。

使用下列服務名稱為 Detective 建立 VPC 端點：

- com.amazonaws.*region*.detective
- com.amazonaws.*region*.detective-fips

如果您為端點啟用私有 DNS，您可以使用區域的預設 DNS 名稱向 Detective 提出 API 請求，例如 api.detective.*us-east-1*.amazonaws.com。如需詳細資訊，請參閱《》中的 [Amazon Detective 端點](#) Amazon Web Services 一般參考。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[透過介面端點存取服務](#)。

## 為 Detective 建立 VPC 端點政策

您可以將端點政策連接至控制 Detective 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[使用 VPC 端點控制對服務的存取](#)。

範例：Detective 動作的 VPC 端點政策

以下是 Detective 端點政策的範例。連接到端點時，此政策會授予所有資源上所有委託人的所列 Detective 動作的存取權。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "detective:ListGraphs",
        "detective:ListMembers"
      ]
    }
  ]
}
```

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

## 共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。如需有關 VPC 子網路共用的資訊，請參閱《Amazon VPC 使用者指南》中的[與其他帳戶共用 VPC](#)。

## Detective 的安全最佳實務

開發和實作自己的安全性政策時，不妨考慮使用 Detective 提供的多種安全性功能。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

針對 Detective，安全最佳實務與在行為圖表中管理帳戶相關聯。

### Detective 管理員帳戶的最佳實務

邀請成員帳戶加入 Detective 行為圖表時，只邀請您監督的帳戶。

限制存取行為圖表。具有 [AmazonDetectiveFullAccess](#) 政策的使用者可以授予所有 Detective 動作的存取權。具有此類許可的主體可以管理成員帳戶、將標籤新增至其行為圖表，以及使用 Detective 進行調查。當使用者可以存取行為圖表時，他們可以查看成員帳戶的所有調查結果。此類調查結果可能會暴露敏感的安全諮詢。

### 成員帳戶最佳實務

當您收到邀請以查看行為圖表時，請務必驗證邀請的來源。

檢查傳送邀請之管理員帳戶 AWS 的帳戶識別符。確認您知道該帳戶的所屬資訊，以及邀請帳戶有合理理由監控您的安全資料。

# 使用 記錄 Amazon Detective API 呼叫 AWS CloudTrail

Detective 與 整合 AWS CloudTrail，該服務提供 Detective AWS 中使用者、角色或服務所採取動作的記錄。會將 Detective 的所有 API 呼叫 CloudTrail 擷取為事件。擷取的呼叫包括從 Detective 主控台呼叫，以及對 Detective API 操作的程式碼呼叫。

- 如果您建立追蹤，則可以啟用 CloudTrail 事件連續交付至 Amazon S3 儲存貯體，包括 Detective 的事件。
- 如果您未設定追蹤，仍然可以在 事件歷史記錄 中 CloudTrail 檢視主控台當中的最新事件。

使用 收集的資訊 CloudTrail，您可以判斷下列事項：

- 對 Detective 提出的請求
- 提出請求的 IP 地址
- 提出要求的人員
- 所提出的時間
- 有關請求的其他詳細資訊

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

## 中的偵測資訊 CloudTrail

CloudTrail 當您建立 AWS 帳戶時，會在您的帳戶上啟用。當活動在 Detective 中發生時，該活動會在 CloudTrail 事件歷史記錄 中記錄，以及其他 AWS 服務事件。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱 [檢視具有事件歷史記錄 CloudTrail 的事件](#)。

如需 AWS 帳戶中事件的持續記錄，包括 Detective 的事件，請建立追蹤。追蹤可讓 CloudTrail 將日誌檔案傳遞至 Amazon S3 儲存貯體。

根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。追蹤會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。您也可以設定其他服務 AWS，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。

如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)

- [CloudTrail 支援的服務和整合](#)
- [設定的 Amazon SNS Notifications CloudTrail](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)，並從[多個帳戶接收 CloudTrail 日誌檔案](#)

CloudTrail 會記錄 Detective [API參考](#) 中記錄的所有 Detective 操作。

例如，呼叫 CreateMembers、AcceptInvitation 和 DeleteMembers 操作會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根還是 AWS Identity and Access Management ( IAM ) 使用者憑證提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 該請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱[CloudTrail userIdentity](#)元素。

## 了解 Detective 日誌檔案項目

追蹤是一種組態，可讓您將事件作為日誌檔案交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。

事件代表來自任何來源的單一請求。事件包含有關請求動作、動作日期和時間、請求參數等資訊。CloudTrail log 檔案不是公開API呼叫的有序堆疊追蹤，因此項目不會以任何特定順序顯示。

下列範例顯示示範 AcceptInvitation 動作的 CloudTrail 日誌項目。

```
{
  "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 區域和配額

使用 Amazon Detective 時，請注意以下配額。

## Detective 區域與端點

若要查看 Detective AWS 區域 可用的清單，請參閱 [Detective 服務端點](#)。

## Detective 配額

Detective 具有以下配額，無法設定。

資源	配額	說明
成員帳戶的數量	1,200	管理員帳戶可新增至行為圖表的成員帳戶數目。
行為圖表資料量：量警告	每天 9 TB	如果行為圖表資料量大於每天 9 TB，則 Detective 會顯示警告，告知行為圖表已接近允許的最大資料量。
行為圖表標資料量：無新增帳戶	每天 10 TB	如果行為圖表資料量大於每天 10 TB，則無法將新成員帳戶新增至行為圖表。
行為圖表資料量：停止資料擷取至行為圖表	每天 15 TB	<p>如果行為圖表資料量大於每天 15 TB，則 Detective 會停止將資料擷取至行為圖表中。</p> <p>每天 15 TB 反映正常資料量和資料量峰值。</p> <p>若要重新啟用資料擷取，您必須連絡支援。</p>

## 不支援 Internet Explorer 11

您無法透過 Internet Explorer 11 使用 Detective。

## 管理行為圖表的標籤

標籤是可選的標籤，您可以定義並指派給 AWS 資源，包括特定類型的 Detective 資源。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。例如，您可以使用標籤來套用原則、分配成本、區分資源版本，或識別支援特定合規性需求或工作流程的資源。

您可以將標籤指派給您的行為圖表。然後，您可以使用 IAM 策略中的標籤值來管理對 Detective 中行為圖函數的存取。請參閱 [the section called “基於 Detective 行為圖表標籤的授權”](#)。

您也可以使用標籤作為成本報告的工具。例如，若要追蹤與安全性相關的成本，您可以將相同的標籤指派給 Detective 行為圖表、AWS Security Hub CSPM 中樞資源和 Amazon GuardDuty 偵測器。然後 AWS Cost Explorer，您可以在中搜尋該標籤，以查看這些資源中成本的合併檢視。

## 檢視行為圖的標籤

您可以從一般頁面管理行為圖表的標籤。

### Console

若要檢視指派給行為圖表的標籤清單

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。

### Detective API, AWS CLI

您可以使用 Detective API 或 AWS Command Line Interface 取得行為圖的標籤清單。

若要取得行為圖的標籤清單 (DetectiveAPI, AWS CLI)

- DetectiveAPI：使用 [ListTagsForResource](#) 操作。您必須提供您的 ARN 的行為圖。
- AWS CLI：在命令列中執行 `list-tags-for-resource` 命令。

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

### 範例

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

## 將標籤新增至行為圖

### Console

從一般頁面的標籤清單中，您可以將標籤值新增至行為圖表。

若要將標籤新增至行為圖表

1. 選擇 Add new tag (新增標籤)。
2. 針對金鑰，輸入標籤的名稱。
3. 針對值，輸入標籤值。

### Detective API, AWS CLI

您可以使用 Detective API 或將標籤值新增 AWS CLI 至您的行為圖表。

若要將標籤新增至行為圖表 (DetectiveAPI , AWS CLI)

- DetectiveAPI：使用 [TagResource](#) 操作。您可以提供行為圖ARN和要加入的標籤值。
- AWS CLI：在命令列中執行 tag-resource 命令。

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph ARN> --tags '{"TagName":"TagValue"}
```

### 範例

```
aws detective tag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}
```

# 從行為圖中移除標籤

## Console

若要從一般頁面的清單中移除標記，請選擇該標記的移除選項。

## Detective API, AWS CLI

您可以使用 Detective API 或從行為圖中移除標籤值。AWS CLI

若要從行為圖中移除標籤 (DetectiveAPI, AWS CLI)

- DetectiveAPI：使用 [UntagResource](#) 操作。您可以提供行為圖ARN，以及要移除的標籤名稱。
- AWS CLI：在命令列中執行 `untag-resource` 命令。

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys  
"TagName"
```

## 範例

```
aws detective untag-resource --resource-arn arn:aws:detective:us-  
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

# 停用 Amazon Detective

行為圖表的管理員帳戶可以通過 Detective 主控台、Detective API 或 AWS Command Line Interface 停用 Amazon Detective。當您停用 Detective 後，行為圖表及其相關聯的 Detective 資料都會刪除。

一旦刪除行為圖表，其就無法恢復。

## 目錄

- [停用 Detective \(主控台\)](#)
- [停用 Detective \(Detective API\) AWS CLI](#)
- [停用跨區域的 Detective \(GitHub 上的 Python 指令碼\)](#)

## 停用 Detective (主控台)

您可以透過 AWS 管理主控台停用 Amazon Detective。

### 停用 Amazon Detective (主控台)

1. 前往 <https://console.aws.amazon.com/detective/> 開啟 Amazon Detective 主控台。
2. 在 Detective 導覽窗格中，於設定下選擇通用。
3. 在一般頁面的停用 Amazon Detective 下，選擇停用 Amazon Detective。
4. 出現提示時，請輸入 **disable**。
5. 選擇停用 Amazon Detective。

## 停用 Detective (Detective API) AWS CLI

您可以透過 Detective API 或 AWS Command Line Interface 停用 Amazon Detective。若要取得行為圖表的 ARN 以供在請求中使用，請使用 [ListGraphs](#) 操作。

### 停用 Detective (Detective API) AWS CLI

- Detective API：使用 [DeleteGraph](#) 操作。您必須提供圖表 ARN。
- AWS CLI：在命令列中執行 [delete-graph](#) 命令。

```
aws detective delete-graph --graph-arn <graph ARN>
```

範例：

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

## 停用跨區域的 Detective (GitHub 上的 Python 指令碼)

Detective 在 GitHub 中提供了開源指令碼，您可以借此在指定的區域清單中停用管理員帳戶的 Detective。

如需如何設定和使用 GitHub 指令碼的相關資訊，請參閱 [the section called “Amazon Detective Python 指令碼”](#)。

## 使用者指南的文件歷史記錄

以下資料表說明自上次發行 Detective 後，文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- 文件最近更新時間：2025 年 2 月 20 日

變更	描述	日期
<a href="#">新功能 - 新增對 VPC 端點的支援</a>	Detective 現在已與 整合 AWS PrivateLink ，並支援 VPC 端點。如需 AWS PrivateLink 整合的詳細資訊，請參閱 <a href="#">Amazon Detective 和界面 VPC 端點 (AWS PrivateLink)</a> 。	2025 年 9 月 30 日
<a href="#">新增對 Amazon GuardDuty 攻擊序列調查結果的支援</a>	Detective 新增了對與 GuardDuty 延伸威脅偵測相關聯之調查結果類型的支援。當 API 活動和 GuardDuty 調查結果偵測等多個動作的特定序列符合潛在可疑活動時，GuardDuty 會偵測攻擊序列。如需有關擴充威脅偵測和攻擊序列調查結果類型的資訊，請參閱《Amazon GuardDuty 使用者指南》中的 <a href="#">擴充威脅偵測</a> 。	2025 年 2 月 20 日
<a href="#">新增對 Amazon GuardDuty IAM 調查結果的支援</a>	Detective 新增了對新 GuardDuty 調查結果類型的支援，當針對 AWS 帳戶 您環境中列出的 建立的限制使用者登入資料被用於向 提出請求時，會提醒您 AWS 服務。如需詳細資訊，請參閱《Amazon GuardDuty 使用	2025 年 2 月 4 日

者指南[Policy:IAMUser/ShortTermRootCredentialUsage](#)》中的。

## 新功能

已將[時間軸配置](#)新增至 Detective Finding 群組視覺化。針對問題清單引進播放按鈕功能和嚴重性型篩選。這些增強功能可協助您進一步了解事件進展、排定關鍵問題的優先順序，以及進行更有效率的安全調查。

2024 年 12 月 27 日

## 新增對 Amazon GuardDuty 調查結果的支援

Detective 新增了對以下三種 GuardDuty 調查結果類型的支援，在 Amazon EC2 執行個體或 AWS 環境中的容器工作負載上執行可疑命令時通知您：

2024 年 11 月 6 日

- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)

## 新增對 Amazon GuardDuty 調查結果的支援

Detective 現在支援下列 [GuardDuty 執行期監控調查結果類型](#)。

2024 年 8 月 27 日

- Execution:Runtime/SuspiciousShell
- PrivilegeEscalation:Runtime/ElevationToRoot

### [新增對 Amazon GuardDuty 調查結果的支援](#)

Detective 現在支援 [S3 的 GuardDuty 惡意軟體保護](#)。這可協助您將新上傳的物件掃描到 Amazon S3 儲存貯體中是否有潛在的惡意軟體和可疑的上傳，並在它們被導入下游程序之前採取行動將其隔離。

2024 年 7 月 9 日

### [已更新的功能](#)

Detective 已將新的放射配置新增至 [調查結果群組視覺化面板](#)，以改善視覺化效果，更輕鬆地解讀資料。

2024 年 6 月 26 日

### [新的 Security Lake 來源版本](#)

除了來源版本 1 (OCSF 1.0.0-rc.2) 之外，Detective 現在會從來源版本 2 (OCSF 1.1.0) 擷取 Detective 支援之 [Security Lake 來源](#) 的資料。

2024 年 5 月 15 日

### [新的 Security Lake 日誌來源](#)

您可以使用 Detective 與 Security Lake 整合，從 [Amazon EKS 稽核](#) 日誌收集日誌和事件。

2024 年 5 月 15 日

### [文件更新](#)

Amazon Detective 管理指南中的內容現在已合併至 Amazon Detective 使用者指南。Amazon Detective 管理指南將於 2024 年 5 月 8 日終止標準支援。

2024 年 4 月 15 日

### [新增對 Amazon GuardDuty 調查結果的支援](#)

Detective 現在支援下列 [GuardDuty 執行期監控調查結果類型](#)。

2024 年 4 月 5 日

- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/SuspiciousTool
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand

### [已移除 Amazon GuardDuty 成員資格需求](#)

您不再需要成為 GuardDuty 客戶，即可啟用 Amazon Detective。在啟用 Detective 之前，您的帳戶需要啟用 GuardDuty 48 小時。

2024 年 2 月 2 日

### [新增對 Amazon GuardDuty 調查結果的支援](#)

Detective 將 [GuardDuty EC2 執行期監控](#) 調查結果類型的支援擴展至 ECS 和 EC2 資源。

2024 年 1 月 30 日

## [已更新的功能](#)

您現在可以從調查頁面針對要調查的特定資源執行 Detective 調查。Detective 會根據在調查結果和調查結果群組中的活動建議資源。[Detective Investigations](#) 可讓您使用入侵指標調查 IAM 使用者和 IAM 角色，這可協助您判斷資源是否涉及安全事件。

2024 年 1 月 16 日

## [已更新的功能](#)

您現在可以從所建議資源的「調查」頁面執行 Detective 調查。Detective 會根據在調查結果和調查結果群組中的活動建議資源。[Detective Investigations](#) 可讓您使用入侵指標調查 IAM 使用者和 IAM 角色，這可協助您判斷資源是否涉及安全事件。

2023 年 12 月 26 日

## [Detective 讀取共用 VPC 流程流量的方式變更](#)

如果您使用共用 Amazon VPC，可能會發現 Detective 監控的流量有所變更。我們建議您檢閱[整體 VPC 流量的活動詳細資訊](#)中的變更，以了解對您的覆蓋範圍可能造成哪些影響，並檢閱[Detective 如何計算預計成本](#)，以了解它對您的服務成本有何影響。

2023 年 12 月 20 日

## [區域可用性](#)

將歐洲（斯德哥爾摩）、歐洲（巴黎）和加拿大（中部）區域新增至可使用 [Detective 與 Security Lake 整合](#) AWS 的區域清單。

2023 年 12 月 8 日

<a href="#">新功能</a>	<a href="#">Detective 調查</a> 可讓您調查表示有危害情形的 IAM 使用者和 IAM 角色，以協助您判斷資源是否涉及安全事件。	2023 年 11 月 26 日
<a href="#">新功能</a>	根據預設，Detective 會自動為調查結果群組產生 <a href="#">調查結果群組摘要</a> (由生成式人工智慧 (生成式 AI) 提供支援)。調查結果群組摘要會快速分析調查結果與受影響資源之間的關係，然後以自然語言彙總潛在威脅。	2023 年 11 月 26 日
<a href="#">新功能</a>	<a href="#">Detective 與 Security Lake 整合</a> 可讓您查詢和擷取 Security Lake 儲存的原始日誌資料。使用此整合，您可以從 CloudTrail 管理事件和 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌收集日誌和事件。	2023 年 11 月 26 日
<a href="#">已將受管政策資訊新增至安全性章節</a>	在 AmazonDetectiveInvestigatorAccess 政策中新增了 Detective 調查和調查結果群組摘要動作。	2023 年 11 月 26 日
<a href="#">檢視調查結果概觀</a>	如果調查結果與較大活動相關，Detective 會通知您導覽至該調查結果群組。	2023 年 9 月 18 日
<a href="#">Amazon Detective 端點和配額</a>	Detective 現在可於以色列 (特拉維夫) 區域使用。	2023 年 8 月 25 日
<a href="#">增強調查結果群組視覺化</a>	Detective 調查結果群組視覺化現在包括具有彙總調查結果的調查結果群組，因此能夠更有效率地分析相關證據、實體和調查結果。	2023 年 8 月 8 日

<a href="#">增強調查結果群組</a>	調查結果群組現在包含來自 Amazon Inspector 的漏洞調查結果。	2023 年 6 月 13 日
<a href="#">新增了對 Amazon GuardDuty Lambda 保護的支援</a>	Detective 現在提供 GuardDuty Lambda 保護的支援。	2023 年 5 月 26 日
<a href="#">新增 AWS 安全性問題清單做為新的選用資料來源套件。</a>	Detective 現在提供 AWS 安全調查結果做為選用的資料來源套件。此選用的資料來源套件可讓 Detective 從 Security Hub CSPM 擷取資料，並將該資料新增至您的行為圖表。	2023 年 5 月 16 日
<a href="#">新增了對 Amazon GuardDuty EKS 執行期監控調查結果類型的支援</a>	Detective 現已提供對 GuardDuty EKS 執行期監控調查結果類型的支援。	2023 年 5 月 3 日
<a href="#">新增了對 Amazon GuardDuty RDS 保護調查結果類型的支援</a>	Detective 現已提供對 GuardDuty RDS 保護調查結果類型的支援。	2023 年 4 月 20 日
<a href="#">新增了對其他 Amazon GuardDuty 調查結果類型的支援</a>	Detective 現在提供以下其他 GuardDuty 調查結果類型的設定檔：DefenseEvasion: EC2UnusualDNSResolver、DefenseEvasion: EvasionEC2UnusualDoHActivity 和 DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity	2023 年 4 月 12 日
<a href="#">在 Detective 主控台中新增了新的主控面板，以協助使用者針對其特定使用案例選取適當的 AWS 受管政策。</a>	Detective 提供受管政策，以安全選擇您需要的許可。	2023 年 4 月 3 日

<a href="#">顯示 EKS 叢集的 VPC 流量</a>	使用 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集新增了 Amazon Virtual Private Cloud (Amazon VPC) 新流量區段。	2023 年 3 月 2 日
<a href="#">調查結果群組現在包含 Detective 行為圖表的動態視覺化呈現</a>	Detective 調查結果群組現在包含 Detective 行為圖表的動態視覺化呈現，以強調實體與調查結果群組中調查結果之間的關係。	2023 年 2 月 28 日
<a href="#">從 Detective 摘要頁面和搜索結果頁面匯出資料。資料會以逗號分隔值 (CSV) 格式匯出。</a>	Detective 現在提供從 Detective 主控台將資料匯出至瀏覽器的選項。	2023 年 2 月 7 日
<a href="#">為 EKS Amazon EKS 工作負載新增了整體 VPC 流量</a>	Detective 現在從 Amazon Elastic Kubernetes Service Amazon EKS 工作負載新增有關 Amazon 虛擬私有雲端 (VPC) 流程日誌的視覺摘要和分析。	2023 年 1 月 19 日
<a href="#">已將受管政策資訊新增至安全性章節</a>	Detective 現在支援 GuardDuty 透過 AmazonDetectiveFullAccess 政策取得調查結果動作。安全行章節現在為 Detective 提供有關以下新受管政策的詳細資訊：AmazonDetectiveMemberAccess 和 AmazonDetectiveInvestigatorAccess。	2023 年 1 月 17 日
<a href="#">新增了資料保留</a>	使用 Detective，您可以訪問長達一年的歷史事件資料。	2022 年 12 月 20 日

<a href="#">在摘要頁面上新增了調整範圍時間的選項。</a>	Detective 現在提供了調整範圍時間的選項，以便查看過去 365 天內任何 24 小時時間範圍的活動。	2022 年 10 月 5 日
<a href="#">搜尋調查結果或實體</a>	Detective 現在提供不區分大小寫的搜尋。	2022 年 10 月 3 日
<a href="#">新增了設置範圍時間戳記的功能</a>	Detective 現在提供設定範圍時間戳記格式偏好設定的方法。此偏好設定將套用至 Detective 中的所有時間戳記。	2022 年 10 月 3 日
<a href="#">新增了與調查結果群組相關的術語</a>	Detective 現在支援在單一顯示器中將相關調查結果連接在一起的調查結果群組，以協助您調查環境中潛在的惡意活動。從調查結果群組設定檔中，您可以錨定至實體設定檔和與該群組相關的調查結果概觀。	2022 年 8 月 3 日
<a href="#">已新增與 Amazon EKS 稽核日誌相關聯的新設定檔</a>	Detective 現在提供設定檔，可供您調查與以下容器相關實體相關聯的活動：Amazon EKS 叢集、容器映像、Kubernetes Pod 和 Kubernetes 主體。	2022 年 7 月 26 日
<a href="#">添加了新選用的資料來源</a>	Detective 現在支援 EKS 稽核日誌作為選用資料來源套件。管理員帳戶可以為其現有行為圖表啟用此新資料來源。在此日期之後建立的圖表預設會啟用此資料來源。管理員可以隨時手動停用此資料來源。	2022 年 7 月 26 日

<a href="#">適用於 Detective 的新服務連結角色和受管政策</a>	Detective 現在有服務連結角色，即 <code>AWSServiceRoleForDetective</code> 。服務連結角色用於代表您存取組織資料。角色使用新 <code>AmazonDetectiveServiceLinkedRolePolicy</code> 受管政策。	2021 年 12 月 16 日
<a href="#">新增與的整合 AWS Organizations</a>	Detective 現已與組織整合。組織管理帳戶會指定組織的 Detective 管理員帳戶。Detective 管理員帳戶可以檢視組織中的所有帳戶，並在組織行為圖表標中啟用此類帳戶作為成員帳戶。	2021 年 12 月 16 日
<a href="#">使用調查結果概觀取代調查結果設定檔</a>	調查結果設定檔包含分析相關資源活動的視覺化。新調查結果概觀包含從 GuardDuty 擷取的調查結果詳細資訊，以及相涉及的實體的清單。從調查結果概觀中，您可以錨定至相關實體的設定檔。	2021 年 9 月 20 日
<a href="#">移除了所支援 GuardDuty 調查結果類型的限制</a>	Detective 不再限於已選取的一組 GuardDuty 調查結果類型。Detective 會自動收集所有調查結果類型的調查結果詳細資訊，並提供相關實體之實體設定檔的存取權。	2021 年 9 月 20 日
<a href="#">從相關調查結果設定檔面板至調查結果詳細資訊的連結</a>	在實體設定檔上，當您在相關聯調查結果清單中選擇調查結果時，調查結果詳細資訊會顯示在右側的面板中。範圍時間設定為調查結果時間範圍。	2021 年 9 月 20 日

[在 Detective 中將 S3 儲存貯體新增至可用的實體類型](#)

Detective 現在提供 S3 儲存貯體的設定檔。S3 儲存貯體設定檔提供與 S3 儲存貯體互動主體以及它們在 S3 儲存貯體上執行的 API 操作的詳細資訊。

2021 年 9 月 20 日

[在 Splunk 中產生 Detective 網址的新選項](#)

Splunk Trumpet 專案可讓您將 AWS 內容傳送至 Splunk。透過此專案，您現在可以新增 Detective URL，以導覽至 GuardDuty 調查結果的設定檔。

2021 年 9 月 8 日

[已在帳戶和角色的活動詳細資訊中取代 AKID](#)

在帳戶設定檔上，整體 API 呼叫量的活動詳細資訊現在會顯示使用者或角色，而非存取金鑰識別符 (AKID)。在角色設定檔上，整體 API 呼叫量的活動詳細資訊現在會顯示角色工作階段，而非 AKID。對於在此變更之前發生的活動，呼叫者會列為未知資源。

2021 年 7 月 14 日

[已將呼叫服務新增至 API 呼叫的相關資訊](#)

在 Detective 主控台上，API 呼叫的相關資訊現在包含發出呼叫的服務。在整體 API 呼叫量、新觀察到的 API 呼叫和增加量的 API 呼叫上的清單中新增了服務欄位。在整體 API 呼叫量和新觀察到的地理位置的活動詳細資訊上，API 方法會在發出此類方法的服務下進行分組。針對在此變更之前發生的活動，API 方法會以未知服務進行分組。

2021 年 7 月 14 日

<a href="#">新增使用者、角色和角色工作階段的資源互動標籤</a>	使用者、角色和角色工作階段的資源互動標籤包含與此類實體相關之角色承擔活動的相關資訊。針對角色工作階段，這是新標籤。針對使用者和角色而言，這是包含新內容的現有標籤。	2021 年 6 月 29 日
<a href="#">更新了行為圖表資料量的配額值</a>	增加了行為圖表標的資料量配額。Detective 發出警告 (每天 3.24 TB)。無法添加新帳戶 (每天 3.6 TB)。Detective 停止將資料擷取至行為圖表中 (每天 4.5 TB)。	2021 年 6 月 10 日
<a href="#">在 Python 指令碼選項中添加了標籤值</a>	當您使用 Detective Python 指令碼 ( <code>enableDetective.py</code> ) 啟用 Detective 後，您可以將標籤指派給行為圖表。	2021 年 5 月 19 日
<a href="#">增加了通過資料量檢查的成員帳戶的自動啟用</a>	當成員帳戶接受邀請時，其狀態為已接受 (未啟用)，直到 Detective 確認其資料不會導致行為圖表標資料量超出配額為止。如果資料量不是問題，則 Detective 會自動將狀態變更為已接受 (已啟用)。請注意，目前已接受 (未啟用) 的現有成員帳戶無法自動啟用。	2021 年 5 月 12 日
<a href="#">已將受管政策資訊新增至安全性章節</a>	安全性章節中的新章節提供有關 Detective 受管政策的詳細資訊。Detective 目前提供單一受管政策，即 <code>AmazonDetectiveFullAccess</code> 。	2021 年 5 月 10 日

### [變更了成員帳戶清單中的資料量值](#)

在帳戶管理頁面上，成員帳戶清單現在會顯示每個成員帳戶的每日資料量。之前，清單以允許總量的百分比顯示。

2021 年 4 月 29 日

### [管理成員帳戶的修訂選項](#)

將管理帳戶功能表取代為動作功能表。結合了從 .csv 檔案新增個別帳戶和新增帳戶的選項。將啟用帳戶從管理帳戶移動至動作旁的個別選項。

2021 年 4 月 5 日

### [新增了行為圖表標籤和基於標籤的授權](#)

啟用 Detective 後，您可以新增標籤至行為圖表。您可以從一般頁面管理行為圖表的標籤。Detective 還支援基於標籤值的授權。

2021 年 3 月 31 日

### [新增了对其他 Amazon GuardDuty 调查结果类型的支援](#)

Detective 现在提供以下其他 GuardDuty 调查结果类型的设定档：CredentialAccess:IAMUser/AnomalousBehavior、DefenseEvasion:IAMUser/AnomalousBehavior、Discovery:IAMUser/AnomalousBehavior、Exfiltration:IAMUser/AnomalousBehavior、Impact:IAMUser/AnomalousBehavior、InitialAccess:IAMUser/AnomalousBehavior、Persistence:IAMUser/AnomalousBehavior 和 PrivilegeEscalation:IAMUser/AnomalousBehavior

2021 年 3 月 29 日

### [新增 AWS GovCloud \(US\) 区域的差异](#)

Detective 现在可在 AWS GovCloud (US) 区域中使用。在 AWS GovCloud (美国东部) 和 AWS GovCloud (美国西部)，Detective 不会传送邀请电子邮件给成员帐户。Detective 也不会自动移除 AWS 中关闭的成员帐户。

2021 年 3 月 24 日

[添加了根據成員帳戶狀態篩選成員帳戶清單的標籤](#)

成員帳戶清單現在可顯示標籤，您可以使用此類標籤來根據成員帳戶狀態篩選清單。您可以檢視所有成員帳戶、狀態為已接受 (已啟用) 的帳戶，或狀態非已接受 (已啟用) 的成員帳戶。

2021 年 3 月 16 日

[新增了對其他 Amazon GuardDuty 調查結果類型的支援](#)

Detective 現在提供以下其他 GuardDuty 調查結果類型的設定檔：Backdoor:EC2/C&CActivity.B、Impact:EC2/PortSweep、Impact:EC2/WinRMBruteForce 和 PrivilegeEscalation:IAMUser/AdministrativePermissions

2021 年 3 月 4 日

[向 Python 添加了指令碼的選項，以抑制邀請電子郵件](#)

Detective enableDetective.py 指令碼現在提供了 --disable\_email 選項。當您包含該選項時，Detective 不會向成員帳戶發送邀請電子郵件。

2021 年 2 月 26 日

[已將「主帳戶」一詞變更為「管理員帳戶」。](#)

「主帳戶」一詞變更為「管理員帳戶」。還變更了 Detective 主控台和 API 中所用術語。

2021 年 2 月 25 日

[已將「主帳戶」一詞變更為「管理員帳戶」。](#)

「主帳戶」一詞變更為「管理員帳戶」。還變更了 Detective 主控台和 API 中所用術語。

2021 年 2 月 25 日

### [已新增設定檔面板 VPC 流量往返調查結果 IP 地址的活動詳細資訊](#)

透過設定檔面板往返調查結果 IP 地址的 VPC 流量，您可以顯示活動詳細資訊。只有在調查結果與單一 IP 地址相關聯時，才能使用活動詳細資訊。活動詳細資訊會顯示每個連接埠、通訊協定和方向組合的量。

2021 年 2 月 25 日

### [添加了選擇不向成員帳戶發送邀請電子郵件的 API 選項](#)

使用 Detective API 新增成員帳戶時，管理員帳戶可以選擇不向成員帳戶傳送邀請電子郵件。

2021 年 2 月 25 日

### [IP 地址設定檔上整體 API 呼叫量設定檔面板的新增活動詳細資訊](#)

您現在可以從整體 API 呼叫量設定檔面板顯示 IP 地址的活動詳細資訊。活動詳細資訊會顯示從 IP 地址發出呼叫的每個資源的成功和失敗呼叫次數。

2021 年 2 月 23 日

### [IP 地址設定檔上的新增整體 VPC 流量設定檔面板](#)

IP 地址設定檔現在包含整體 VPC 流量設定檔面板。設定檔面板會顯示往返 IP 地址的 VPC 流量。您可以顯示活動詳細資訊，以顯示與 IP 地址通訊之每個 EC2 執行個體的量。

2021 年 1 月 21 日

### [新增了 Detective 摘要頁面](#)

Detective 摘要頁面包含視覺化，可根據地理位置、API 呼叫數目和 Amazon EC2 流量，引導分析師找到感興趣的實體。

2021 年 1 月 21 日

### [更新了從 Amazon GuardDuty 錨定為 Detective 的選項](#)

在 GuardDuty 中，在 Detective 中調查選項會從動作功能表移至調查結果詳細資訊面板。它會顯示相關實體清單。如果支援調查結果類型，清單也會包含調查結果。然後，您可以選擇導覽至實體設定檔或調查結果設定檔。

2021 年 1 月 15 日

### [新增了將活動詳細資訊窗口設置為預設範圍時間的選項](#)

在整體 API 呼叫量和整體 VPC 流量的活動詳細資訊上，您可以將活動詳細資訊的時間範圍設定為設定檔的預設範圍時間。

2021 年 1 月 15 日

### [新增了對實體大量時間間隔的處理](#)

新增了就指出實體何時具有一或多個大量時間間隔的通知。新大量實體頁面會顯示目前範圍時間的所有大量間隔。

2020 年 12 月 18 日

### [成員帳戶限額已增加至 1,200](#)

主帳戶現在可以邀請最多 1,200 個成員帳戶加入其行為圖表。以前的配額為 1,000。

2020 年 12 月 11 日

### [新增了行為圖表資料量的配額值](#)

更新了行為圖表資料量配額的相關資訊，以新增特定配額值。

2020 年 12 月 11 日

### [在整體 API 呼叫量設定檔面板上新增了活動詳細資訊的時間範圍選擇](#)

在整體 API 流量面板上，您現在可以顯示任何選取時間範圍的活動詳細資訊。面板最初顯示用於顯示範圍時間的活動詳細資訊的選項。

2020 年 9 月 29 日

### [在整體 VPC 流量設定檔面板上新增了活動詳細資訊的時間間隔選項](#)

在整體 VPC 流量面板上，您可以從圖表中顯示單一時間間隔的活動詳細資訊。若要顯示時間間隔的詳細資訊，請選擇時間間隔。

2020 年 9 月 25 日

### [新角色工作階段和聯合身分使用者實體](#)

透過 Detective，您現在可以探索和調查聯合身分驗證。您可以查看哪些資源扮演了各個角色，以及此類驗證的發生時間。

2020 年 9 月 17 日

### [針對範圍時間管理的更新](#)

移除鎖定或解除鎖定範圍時間的選項。系統總將其鎖定。在調查結果設定檔上，如果範圍時間與調查結果時間範圍不同，則系統會顯示警告。

2020 年 9 月 4 日

### [當您捲動設定檔時，設定檔標題仍然可見](#)

在設定檔上，當您捲動標籤上的設定檔面板時，類型、識別符和範圍時間仍然可見。當標籤不可見時，您可以使用頁面導覽路徑中的標籤下拉清單導航到其他標籤。

2020 年 9 月 4 日

### [搜尋一律顯示搜尋結果](#)

當您進行搜尋時，結果現在會在搜尋頁面上顯示。從結果中，您可以錨定至調查結果或實體設定檔。

2020 年 8 月 27 日

### [已新增至允許的搜尋條件](#)

系統已展開允許的搜尋條件。您可以依名稱搜尋 AWS 使用者和 AWS 角色。您可以使用 ARN 來搜尋問題清單、AWS 角色、AWS 使用者和 EC2 執行個體。

2020 年 8 月 27 日

<a href="#">從設定檔面板連結至其他主控台</a>	在 EC2 執行個體詳細資訊設定檔面板上，EC2 執行個體識別符會連結至 Amazon EC2 主控台。在使用者詳細資訊和角色詳細資訊設定檔面板上，使用者名稱和角色名稱會連結至 IAM 主控台。	2020 年 8 月 14 日
<a href="#">VPC 流程資料的活動詳細資訊</a>	透過整體 VPC 流量設定檔面板，您現在可存取活動詳細資訊。活動詳細資訊顯示所選時段內 IP 地址和 EC2 執行個體之間的流量。	2020 年 7 月 23 日
<a href="#">成員帳戶現在可以查看他們的用量和預計成本</a>	成員帳戶現在可以檢視自己的用量資訊。針對成員帳戶，用量頁面會顯示它們提供的每個行為圖表中擷取的資料量。成員帳戶還可以查看其預計 30 天的費用。	2020 年 5 月 26 日
<a href="#">現在每個帳戶 (而非每個行為圖表) 均可免費試用</a>	現在，每個 Amazon Detective 帳戶都會在每個區域內獲得單獨的免費試用。免費試用會在帳戶啟用 Detective 時開始，或者首次啟用該帳戶作為成員帳戶時開始。	2020 年 5 月 26 日
<a href="#">GitHub 上的新開放原始 Python 指令碼</a>	GitHub 上的新 <a href="#">amazon-detective-multiaccount-scripts</a> 儲存庫提供開放原始碼 Python 指令碼，以便您此類指令碼來管理跨區域的行為圖表標。您可以啟用 Detective，新增成員帳戶，移除成員帳戶，以及停用 Detective。	2020 年 1 月 21 日

## [介紹 Amazon Detective](#)

Detective 使用機器學習和專門建置的視覺化，協助您分析和調查整個 Amazon Web Services (AWS) 工作負載的安全問題。

2019 年 12 月 2 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。