aws

使用者指南

Amazon Detective

Amazon Detective: 使用者指南

Table of Contents

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 將這些更改與 GuardDuty 發現聯繫起來。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”。

Amazon Detective tor 透過自動彙總資料並提供視覺化工具，讓您能夠更快速、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 的特點

以下是 Amazon Detective ess 有助於調查 AWS 環境中的可疑活動並分析資源以識別安全問題根本原因的一些關鍵方法。

Detective, 尋找, 組

Detective 尋找群組可讓您檢查與潛在安全性事件相關的多個活動。您可以使用尋找群組來分析高嚴重性 GuardDuty 發現項目的根本原因。如果安全威脅執行者試圖入侵您的 AWS 環境，他們通常會執行一系列動作，以產生多個安全發現項目和異常行為。

Detective 中的尋找群組頁面會在「尋找群組」頁面中，顯示從行為圖表擷取的所有相關尋找結果群組。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。

Detective tor 提供每個尋找群組的互動式視覺化，以協助您更快、更徹底地調查安全性問題。視覺效果旨在顯示安全性事件中涉及的實體和發現項目，讓您更容易瞭解連線和根本原因。協助您以更少的努力更快、更徹底地調查問題。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。

Detective 調查分流結果

透過 Detective 調查，您可以使用入侵指標調查 IAM 使用者和 IAM 角色，以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，您可以將效率最大化、專注於安全性威脅，並強化事件回應能力。

Detective 調查使用機器學習模型和執行緒智慧，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，以識別潛在的入侵或可疑活動指標。這可讓您識別模式並了解哪些資源受到安全事件的影響，並提供主動式方法來識別和緩解威脅。

您可以通過運行 Detective 調查從 Detective 控制台使用開始 Detective 調查。若要以程式設計方式執行調查，請使用 Detective API 的StartInvestigation作業。如果您正在使用 AWS Command Line Interface （ AWS CLI ），請運行啟動調查命令。

Detective 整合 Amazon 安全湖

Detective 與 Amazon 安全湖集成，這意味著您可以查詢和檢索安全湖存儲的原始日誌數據。透過此整合，您可以從下列 Security Lake 原生支援的來源收集記錄檔和事件。

- AWS CloudTrail 管理事件
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌

將 Detective 與安全湖整合後，Detective 會開始從安全湖擷取與 AWS CloudTrail 管理事件和 Amazon VPC 流程日誌相關的原始日誌。您可以查詢原始記錄檔以檢視 Detective 中的記錄和事件。

調查 VPC 流量

您可以使用 Detective 以互動方式檢查 Amazon 彈性運算雲端 (Amazon EC2) 執行個體和 Kubernetes 網繭的虛擬私有雲 (VPC) 網路流程的活動詳細資料。Detective ess 會從您受監控的帳戶中自動收集 VPC 流程日誌，並依 EC2 執行個體彙總，並呈現有關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。

訪問 Amazon Detective

大多數都有 Amazon Detective AWS 區域。如需目前提供 Detective 的區域清單，請參閱 AWS 一般參考. 如需管理您的帳戶 AWS 區域 的相關資訊 AWS 帳戶，請參閱AWS Account Management 參考指南中的「指定 AWS 區域 您的帳戶可以使用的項目」。

在每個地區，您可以通過以下任何一種方式與 Detective 合作。

AWS Management Console

這 AWS Management Console 是一個基於瀏覽器的介面，您可以使用它來建立和管理 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 工作：檢閱潛在的安全威脅，以及分析、調查和識別安全發現項目的根本原因。

AWS 命令行工具

使用 AWS 命令行工具，您可以在系統的命令行中發出命令以執行 Detective 任務和 AWS 任務。使用命令行可以比使用控制台更快，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 提供兩組指令行工具： AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell. 若要取得有關安裝和使用的資訊 AWS CLI，請參閱《使AWS Command Line Interface 用指南》。若要取得有關安裝和使用的「工具」的資訊 PowerShell，請參閱《使AWS Tools for PowerShell 用指南》。

AWS 開發套件

AWS 提供包含各種程式設計語言和平台 (例如 Java、Go、Python、C++ 和 .NET) 的程式庫和範例程式碼的開發套件。SDK 提供方便、程式化的方式存取 Detective 和其他功能。 AWS 服務他們還處理諸如密碼編譯簽名請求，管理錯誤以及自動重試請求等任務。如需安裝和使用 AWS SDK 的詳細資訊，請參閱建置在其上 AWS的工具。

Amazon Detective 休息 API

Amazon Detective REST API 可讓您以程式化的方式全面存取 Detective 帳戶、資料和資源。使用此 API，您可以將 HTTPS 請求直接發送給 Detective。但是，與 AWS 命令行工具和 SDK 不同，

使用此 API 需要您的應用程序處理低級別的詳細信息，例如生成散列以簽署請求。如需有關此 API 的詳細資訊，請參閱 Detective API 參考資料。

Amazon Detective 的定價

與其他 AWS 產品一樣，使用 Amazon Detective tor 沒有合約或最低承諾。

Detective 定價以多種維度為基礎，無論來源為何，都會針對所有資料收取每 GB 的分層統一費率。如需詳細資訊，請參閱 Amazon Detective 定價。

為了幫助您了解並預測使用 Detective 的費用，Detective 會為您的帳戶提供估計的使用費用。您可以在 Amazon Detective 主控台上查看這些估計值，並使用 Amazon Detective API 存取這些估計值。根據您使用服務的方式，您可能會因為將其他 AWS 服務 功能與某些 Detective 功能（例如安全湖整合和 Detective 調查）結合使用而產生額外費用。

當您首次啟用 Detective 時，系統會自動註冊 Detective 的 30 天免費試用版。 AWS 帳戶 這包括在中作為組織一部分啟用的個別帳戶 AWS Organizations。在免費試用期間，在適用的情況下使用 Detective 不收取任何費用 AWS 區域。

為了幫助您了解並預測免費試用結束後使用 Detective 的費用，Detective 會根據您在試用期間使用 Detective 的情況為您提供估計的使用費用。您的使用量資料也會指出免費試用期結束前剩餘的時間長度。您可以在 Amazon Detective 主控台上檢閱這些資料，並使用 Amazon Detective API 存取這些資料。

Detective 如何運作？

Detective 會自動擷取以時間為基礎的事件，例如登入嘗試、API 呼叫和網路流量，以 AWS CloudTrail 及 Amazon VPC 流量日誌。它也會擷取由 GuardDuty偵測到的發現項目。

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連結集合。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 也集成在一起 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”。

管理員帳戶會使用行為圖表產生的分析和視覺效果來調查 AWS 資源和 GuardDuty 發現項目。使用與 GuardDuty和的 Detective 整合 AWS Security Hub，您可以從這些服務中的 GuardDuty 搜尋項目直接轉換至 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

為了在中進一步保護您的資料、工作負載和應用程式 AWS，請考慮將以下 AWS 服務 內容與 Amazon Detective ess 結合使用。

AWS Security Hub

AWS Security Hub 可讓您全面檢視 AWS 資源的安全狀態，並協助您根據安全性產業標準和最佳實務來檢查 AWS 環境。這部分原因是從多個 AWS 服務（包括 Detective）和支援的 AWS 合作夥伴網路 (APN) 產品中使用、彙總、組織和優先順序排列您的安全發現結果。Security Hub 可協助您分析安全性趨勢，並識別 AWS 環境中最優先順序的安全性問題。

若要進一步了解資訊 Security Hub，請參閱使AWS Security Hub 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 的 AWS CloudTrail 資料事件日誌和 CloudTrail 管理事件日誌。它會使用威脅情報摘要，例如惡意 IP 位址和網域清單，以及機器學習來識別您 AWS 環境中的未預期和潛在未經授權和惡意活動。

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，將來自環 AWS 境、SaaS 供應商、內部部署來源、雲端來源和第三方來源的安全性資料，自動集中至儲存在您帳戶中的專用資料湖。 AWS 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。

若要進一步了解安全湖，請參閱 Amazon 安全湖使用者指南。要了解有關使用 Detective 和安全湖的更多信息，請參閱與 Amazon Security Lake 整合。

若要瞭解其他 AWS 安全性服務，請參閱上的安全性、身分識別和合規性 AWS。

開始使用 Amazon Detective

本教程介紹了 Amazon Detective。您將學習如何為您的 AWS 帳戶啟用 Detective。您還將學習如何驗證 Detective ess 已經開始從您的 AWS 帳戶中擷取資料，並將其擷取到您的行為圖表中。

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 帳戶將其資料提供給行為圖表。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

開始之前

在啟用 Amazon Detective 之前，您必須具備 AWS 帳戶.

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。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。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console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)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

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 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 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 身分中心使用者登入的說明，請參閱使用AWS 登入 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

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

必要條件

請確定符合下列需求。

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受管政策附加到 IAM 主體，從而授予所有 Detective 動作的存取權。

帳戶資料量必須處於 Detective 配額範圍內

流入行為圖表的資料量必須小於 Detective 允許的最大值。

當您嘗試啟用 Detective 時，如果您帳戶的資料量太大，則無法啟用 Detective。Detective 主控台會顯示通知，說明資料量過大。

支援的 AWS Command Line Interface 版本

若要使用 AWS CLI 來執行 Detective 工作，最低所需的版本為 1.16.303。

建議

建議與 GuardDuty 和對齊 AWS Security Hub

如果您已註冊 GuardDuty 並且 AWS Security Hub，我們建議您的帳戶成為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 中，檢視發現項目的詳細資料時，您可以從 GuardDuty 尋找項目詳細資料旋轉至 Detective 尋結果設定檔。
- 在 Detective 中，調查 GuardDuty 發現項目時，您可以選擇封存該發現項目的選項。

如果您對 GuardDuty 和 Security Hub 有不同的管理員帳戶，建議您根據您經常使用的服務來對齊管理員帳戶。

- 如果您使用頻率 GuardDuty 較高，請使用 GuardDuty 系統管理員帳戶啟用 Detective。

  如果您使用 AWS Organizations 來管理帳號，請將管理 GuardDuty 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，請使用 Security Hub 管理員帳戶啟用 Detective。

  如果您使用組織來管理帳戶，請將 Security Hub 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 IAM 如何支援此類角色的詳細資訊，請參閱《IAM 使用者指南》中的另一個 AWS 帳戶中提供 IAM 使用者的存取權。

建議更新通 GuardDuty CloudWatch知頻率

在中 GuardDuty，偵測器設定為 Amazon CloudWatch 通知頻率，以報告發現的後續發生次數。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 接收這些更新所需的時間，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，變更組態不會影響使用成本 GuardDuty。

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 事件監控 GuardDuty 發現項目。

啟用 Amazon 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。

啟用 Detective (主控台)

您可以透過 AWS Management Console啟用 Amazon Detective。

若要啟用 Detective (主控台)

1. 登入 AWS Management Console。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，Align 管理員帳戶 (建議使用) 說明在 Detective 和 Amazon GuardDuty 和之間對齊管理員帳戶的建議 AWS Security Hub。請參閱the section called “建議與 GuardDuty 和對齊 AWS Security Hub”。
4. [附加 IAM 政策] 按鈕可讓您直接前往 IAM 主控台並開啟建議的政策。您可以選擇將建議的政策附加到您用於 Detective 的主體上。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 “邀請成員帳戶至行為圖表”。

啟用 Detective（Detective API， AWS CLI）

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

若要啟用 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"}'
```

啟用跨區域 Detective（開啟 Python 腳本 GitHub）

Detective 提供了一個開源腳本 GitHub ，其中執行以下操作：

- 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 腳本”。

檢查是否正在擷取資料

啟用 Detective 之後，它會開始從您的 AWS 帳戶擷取資料，並將其擷取到您的行為圖表中。

對於初始擷取，資料通常會在 24 小時內在行為圖表中提供。

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。

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

擁 AWS 帳戶 有行為圖且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 "邀請成員帳戶至行為圖表"。

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。

自治系统组织

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。

委派的管理員帳戶 (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爲委派的管理員帳戶。

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 服務的記錄，例如 AWS CloudTrail 日誌和 Amazon VPC 流程日誌
- GuardDuty 發現

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。

實體可以是您管理的 AWS 資源，也可以是與資源互動的外部 IP 位址。

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 檢測到的安全問題 GuardDuty。

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 証据

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，此類調查結果只能在 Detective 中檢視，不會傳送至 Security Hub。

尋找概述

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。

大容量實體

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

受邀將資料貢獻至行為圖的管理員帳戶。 AWS 帳戶 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

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。

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。

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。

行為圖表會使用來源資料來執行以下作業：

- 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。

如需管理員帳戶如何在行為圖表中管理成員帳戶的相關資訊，請參閱管理帳戶。

目錄

Amazon Detective 如何使用來源資料填入行為圖表

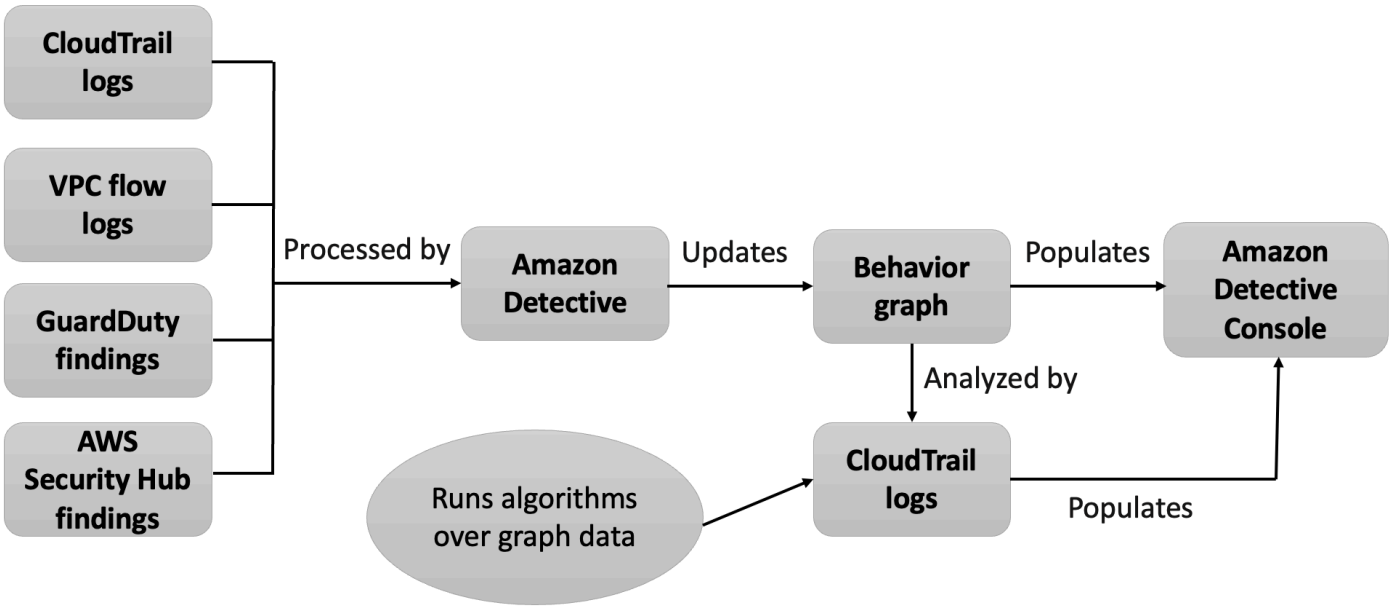
為了提供原始資料以供調查使用，Detective 將來自您 AWS 環境及其他環境的資料匯集在一起，包括以下內容：

- 日誌資料，包括 Amazon Virtual Private Cloud (Amazon VPC) 和 AWS CloudTrail
- Amazon 的發現 GuardDuty
- 來自的發現 AWS Security Hub

若要深入瞭解行為圖中使用的來源資料，請參閱行為圖中使用的來源資料。

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。範圍時間是實體隨時間推移的活動摘要。

隨著系統将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为正常以及異常活动。

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 後的前兩週将作為訓練期間。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
- 追蹤使用 AWS 者、角色和正在使用的帳戶
- 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？
- 以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

Amazon 發現的發現項目 GuardDuty 已輸入 Detective 來源資料。

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 地址

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 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

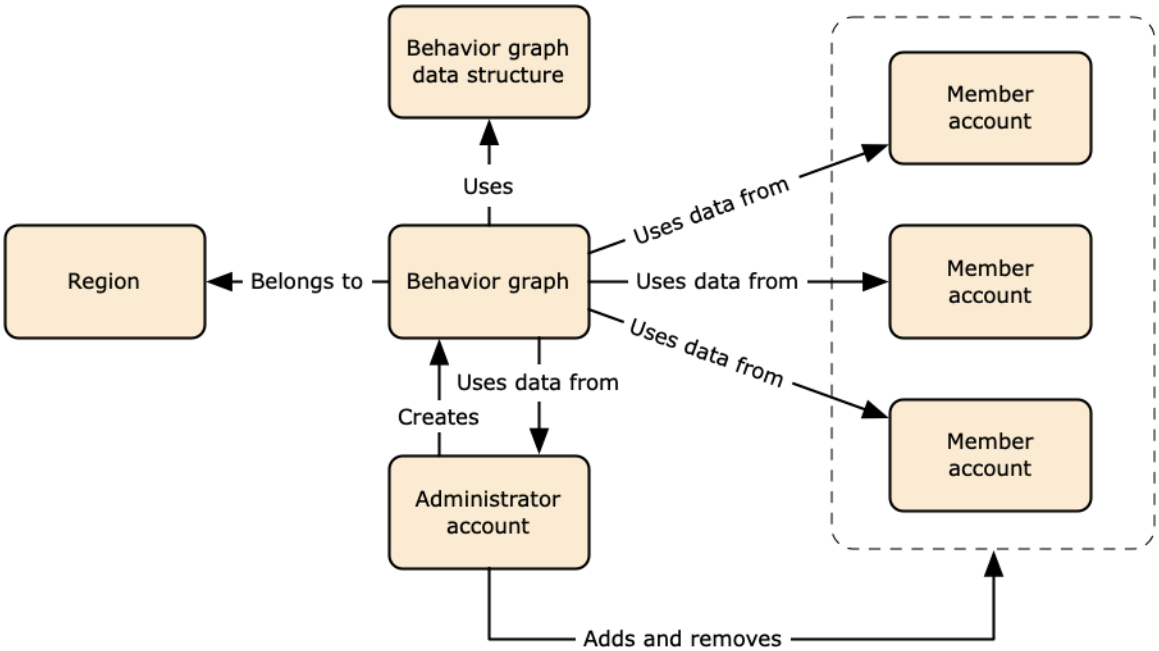
Detective 會針對每個主體回答以下問題：

- 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？

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 將這些更改與 GuardDuty 發現聯繫起來。



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 會從下列類型的 AWS 記錄擷取資料：

- AWS CloudTrail 日誌
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
  - 擷取 IPv4 和 IPv6 記錄，但不會擷取彈性網狀架構介面卡所產生的 MAC 記錄。
  - 當`log-status`欄位的值`OK`處於狀態時，擷取記錄檔記錄。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的流程記錄。
  - 僅擷取在這些 VPC 中執行的 Amazon 彈性運算雲端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。
  - 擷取已接受和拒絕的流量。
- 對於已註冊的帳戶 GuardDuty，Detective 還會收錄 GuardDuty 調查結果。

Detective 會使用獨立 CloudTrail 且重複的 VPC 流程記錄檔以及 VPC 流程記錄檔來消耗 CloudTrail 和 VPC 流程記錄事件。這些程序不會影響或使用您現有 CloudTrail 的 VPC 流程記錄組態。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 Detective 核心套件中提供的三個資料來源之外，還提供選用的原始碼套件 (核心套件包括 AWS CloudTrail 記錄檔、VPC 流程記錄和 GuardDuty發現項目)。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 可將使用者活動與 AWS CloudTrail 管理事件和網路活動與 Amazon VPC 流程日誌建立關聯，而不需要您手動啟用或存放這些日誌。如需詳細資訊，請參閱 針對 Detective 的 Amazon EKS 審核日誌。
- AWS 安全發現

透過選用的資料來源套件，Detective 可以從 Security Hub 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 安全發現。

啟動或停止選用的資料來源：

1. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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。

針對 Detective 的 Amazon EKS 審核日誌

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 中啟用 EKS 稽核日誌作為資料來源， GuardDuty 您將能夠從中查看 Kubernetes 發現項目的詳細資訊。 GuardDuty如需有關啟用此資料來源的詳細資訊， GuardDuty 請參閱 Amazon 中的 Kubernetes 保護。 GuardDuty

> **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. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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 安全發現

AWS 安全性發現項目是選擇性的資料來源套件，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。

透過啟用 AWS 安全調查結果，Detective 可以使用 Security Hub 從上游服務彙總的調查結果，採用稱為 AWS 安全格式 (ASFF) 的標準調查結果格式，便無需耗時的資料轉換工作。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 AWS 安全性發現項目做為選擇性資料來源：

> **Note**
>
> 預設會針對 2023 年 5 月 16 日之後建立的新行為圖表啟用 AWS 安全發現項目資料來源。針對 2023 年 5 月 16 日之前建立的行為圖表，必須手動啟用。

1. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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 安全性發現項目以啟用此資料來源。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 或擁有的服務中擷取安全中心中的所有 ASFF 發現。 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 未設為「符合性」狀態的「服務發現項目」，FAILED且不會擷取跨區域彙總發現項目。

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 AWS Support 以重新啟用資料。如果可能，在您聯絡之前 AWS Support，請嘗試移除成員帳戶，讓資料磁碟區低於配額。此舉可以簡化重新啟用行為圖表的資料擷取程序。

Amazon 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。如果您是 Detective 的新手，請參閱什麼是 Amazon Detective？ 以及 Amazon Detective 的概念和術語。

主題

Detective 調查

您可以使用 Amazon Detective 調查功能，使用入侵指標調查 IAM 使用者和 IAM 角色，以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，您可以將效率最大化、專注於安全性威脅，並強化事件回應能力。

Detective 調查使用機器學習模型和威脅情報來自動分析您 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 調查，您可以調查攻擊策略，不可能的旅行，不可能的 IP 地址和搜索組。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。

運行 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。產生的報告會詳細說明指出潛在危害的異常行為。

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，您有三種執行調查的方法。您可以選擇針對 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 推薦基於其在發現和發現組的活動資源. 若要針對 Detective 所建議的資源執行調查，請在「建議的資源」表格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 — 資源的 Amazon 資源名稱 (ARN)。 AWS
      - 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。如需有關資源 ARN 的詳細資訊，請參閱 IAM 使用者指南中的 Amazon 資源名稱 (ARN)。

   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」(Search) 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作業。如果您正在使用 AWS Command Line Interface （ AWS CLI ），請運行啟動調查命令。

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。

檢閱調查報告

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。

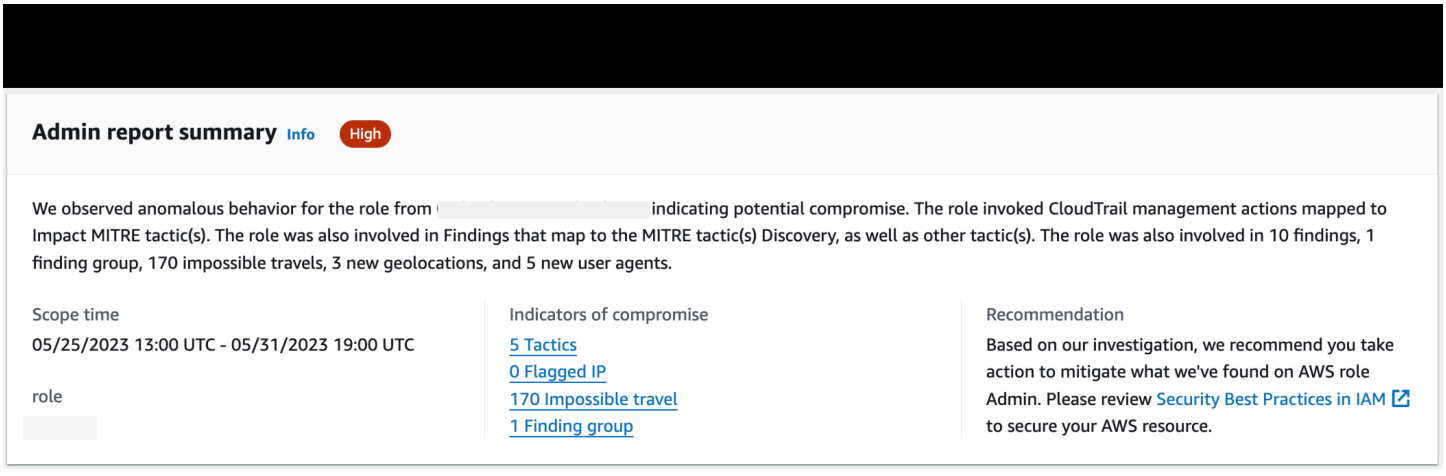
  嚴重性代表在指定範圍時間內對單一資源的調查所分析的處理方式。調查報告的嚴重性並不暗示或以其他方式表示受影響資源對您的組織可能具有的嚴重性或重要性。

  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 調查報告

Detective 調查報告會列出表示入侵的不常見行為或惡意活動摘要。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。

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。

調查報告總結

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。

下載調查報告

您可以下載 JSON 格式的 Detective 調查報告，進一步分析報告，或將其存放到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。

封存調查報告

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。

調查階段及起點

Amazon Detective 提供支援整體調查過程的工具。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。

調查階段

任何調查程序都包括以下階段：

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，您被分配到發現或發現的警報，如 Amazon GuardDuty 和亞馬 Amazon Inspector 服務發現。

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，您可能會被分配一個 Amazon GuardDuty 或 AWS Security Hub 發現進行調查。或者，您可能會擔心特定 IP 地址的異常活動。

調查的典型起點包括偵測到的發現項目，以 GuardDuty 及從 Detective 來源資料擷取的實體。

偵測的發現項目 GuardDuty

GuardDuty 使用您的日誌數據來發現惡意或高風險活動的可疑實例。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 也會顯示連線至發現項目的實體，例如 IP 位址和 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 安全性中樞彙總的安全性發現

AWS Security Hub 在單一位置彙總各種發現項目提供者的安全性發現項目，並提供您中 AWS安全性狀態的全面檢視。Security Hub 消除了處理來自多個提供者調查結果的複雜度。它可以減少管理和提高所有 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 也會顯示連線至發現項目的實體，例如 IP 位址和 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。

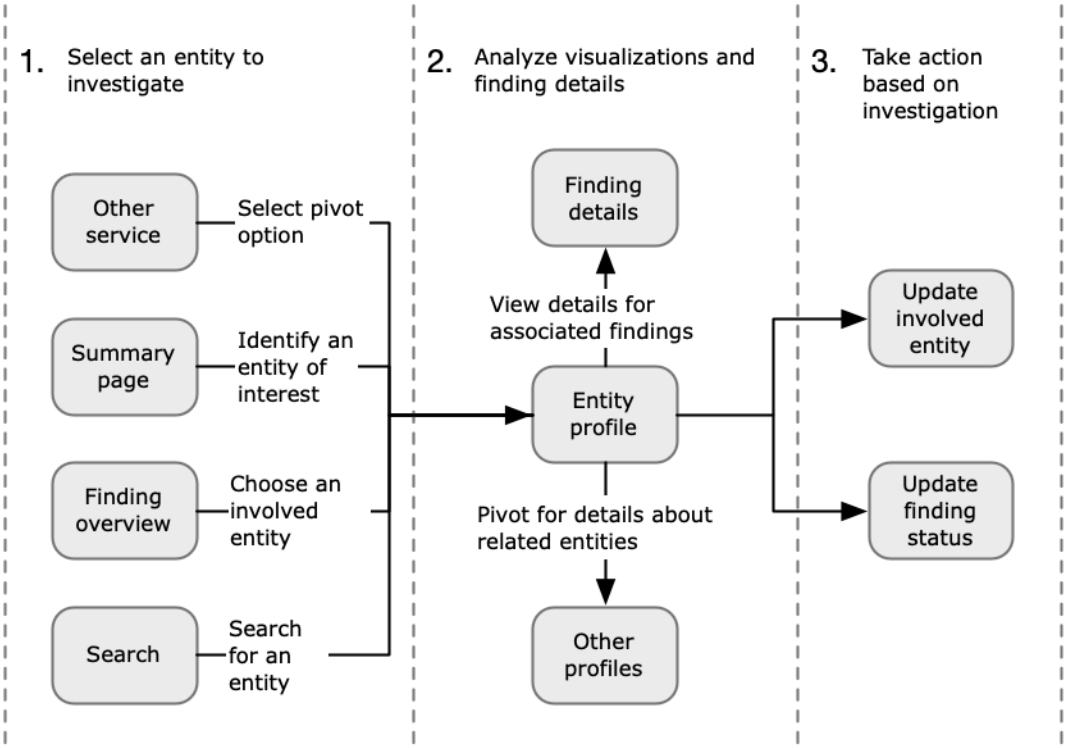
Detective 提供有關實體的一般詳細資訊，例如 IP 地址或使用者名稱。它還提供活動歷史記錄的詳細資訊。例如，Detective 可以報告實體已連線、曾連線或使用的其他 IP 地址。

如需詳細資訊，請參閱 分析實體。

Amazon Detective 調查流程

您可以使用 Amazon Detective 來調查 EC2 執行個體或使用 AWS 者等實體。您也可以調查安全調查結果。

在較高層次上，下圖顯示了 Detective 調查的過程。



步驟 1：選取要調查的實體

在查看中的發現時 GuardDuty，分析師可以選擇在 Detective ess 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。從 Detective，你可以存檔 GuardDuty 調查結果。請參閱the section called “封存 GuardDuty 發現項目”。

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。

分析 Amazon Detective 中的發現

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 AWS 安全發現項目會載入 Amazon Detective，以便您可以使用 Detective 來調查與相關實體相關聯的活動。 GuardDuty 調查結果是 Detective 核心軟件包的一部分，默認情況下攝入。由 AWS Security Hub 彙總的所有其他安全性發現項目會擷取為選用資料來源。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”。

目錄

分析發現項目概觀

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。請參閱the section called “封存 GuardDuty 發現項目”。

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詳細資訊，請參閱檢視帳戶清單。
- 確保您的管理員帳戶與 GuardDuty 和/或 Security Hub 對齊，以從這些服務轉到 Detective。如需建議，請參閱建議與 GuardDuty 和 Security Hub 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。如需有關 Detective 行為圖表中使用之來源資料的詳細資訊，請參閱行為圖中使用的來源資料。

- 若要允許 Detective 從 Security Hub 擷取資料，並將該資料新增至您的行為圖表，您必須啟用 AWS 安全性發現項目 Detective 作為資料來源封裝。如需詳細資訊，請參閱AWS 安全發現項目。

- 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。您可以使用尋找群組來分析高嚴重性 GuardDuty 發現項目的根本原因。如果威脅執行者試圖入侵您的 AWS 環境，他們通常

會執行一系列動作，導致多個安全發現項目和異常行為。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。

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 IP 位址或使用者代理程式之外的 AWS 資源。

> **Note**
>
> 發生與另一個發 GuardDuty 現項目相關的初始發現項目之後，會在 48 小時內建立具有所有相關發現項目及所有相關實體的尋找項目群組。

了解調查結果群組頁面

了解調查結果群組頁面會列出 Amazon Detective 從行為圖表中收集的所有調查結果群組。請注意以下調查結果群組的屬性：

群組的嚴重性

每個尋找項目群組都會根據關聯發現項目的 AWS 安全性發現項目格式 (ASFF) 嚴重性指派一個嚴重性。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。

您可以在鏈上選擇一種策略來查看戰術的描述。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：

- 身分識別 — IAM 主體 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 帳戶擁有與群組中發現項目有關的實體。 AWS 帳戶按名稱和 AWS ID 列出，因此您可以對涉及重要帳戶的活動進行調查的優先順序。

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。研究結果包括亞馬遜 GuardDuty 調查結果、Amazon Inspector 調查結果、 AWS 安全發現以及來自 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 核心軟件包的一部分，默認情況下攝入。由 AWS Security Hub 彙總的所有其他安全性發現項目會擷取為選用資料來源。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。證據發現只能在 Detective 中查看，不會發送到 AWS Security Hub。

Detective 使用 MaxMind GeoIP 數據庫確定請求的位置。 MaxMind 雖然準確性因國家/地區和 IP 類型等因素而異，但在國家/地區層面報告其數據的準確性非常高。如需相關資訊 MaxMind，請參閱 MaxMind IP 地理位置。如果您認為任何 GeoIP 數據不正確，可以通過「正確的 GeoIP2 數據」向 Maxmind 提交更MaxMind 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：

- 涉及的策略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表示入侵的異常行為。

群組中的設定檔面板

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。

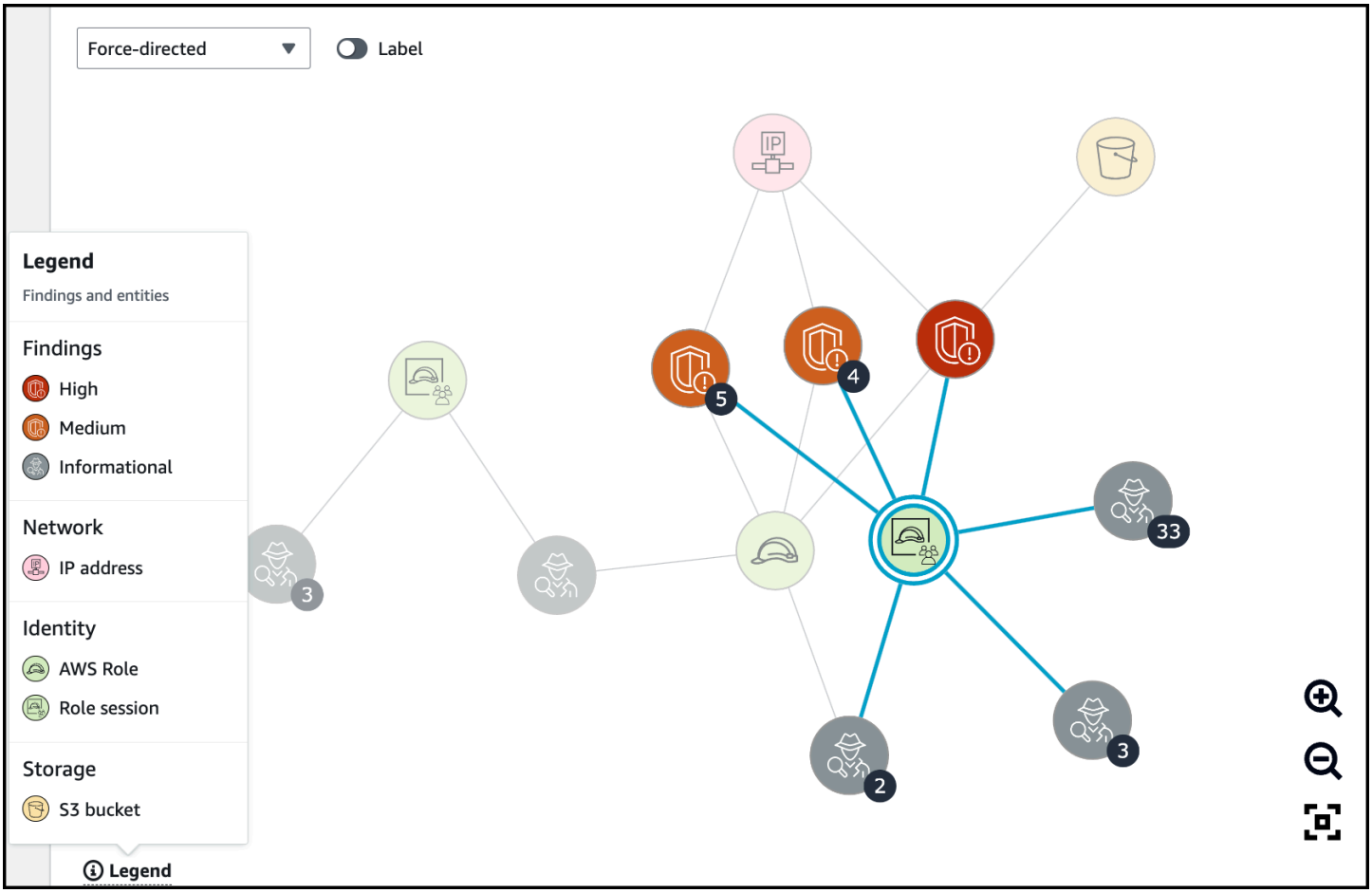
具有彙總調查結果的 Detective 調查結果群組是連線至相同類型資源的調查結果叢集。透過彙總的調查結果，您可以快速評估調查結果群組的組成，並更快地解釋安全問題。在調查結果群組詳細資訊面板中，系統會合併相似的調查結果，您可以展開調查結果，以一併檢視相對類似的調查結果。例如，對於具有相同類型資訊性調查結果和中等調查結果的證據節點，系統會將其進行彙總。目前，您可以檢視包含彙總調查結果的調查結果群組的標題、來源、類型和嚴重性。

在此互動面板中，您可以：

- 使用執行調查來產生調查報告。產生的報告會詳細說明表示入侵的異常行為。
- 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。

您可以選擇選取配置，以圓、強制導向或網格配置來檢視調查結果和實體。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。



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。

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

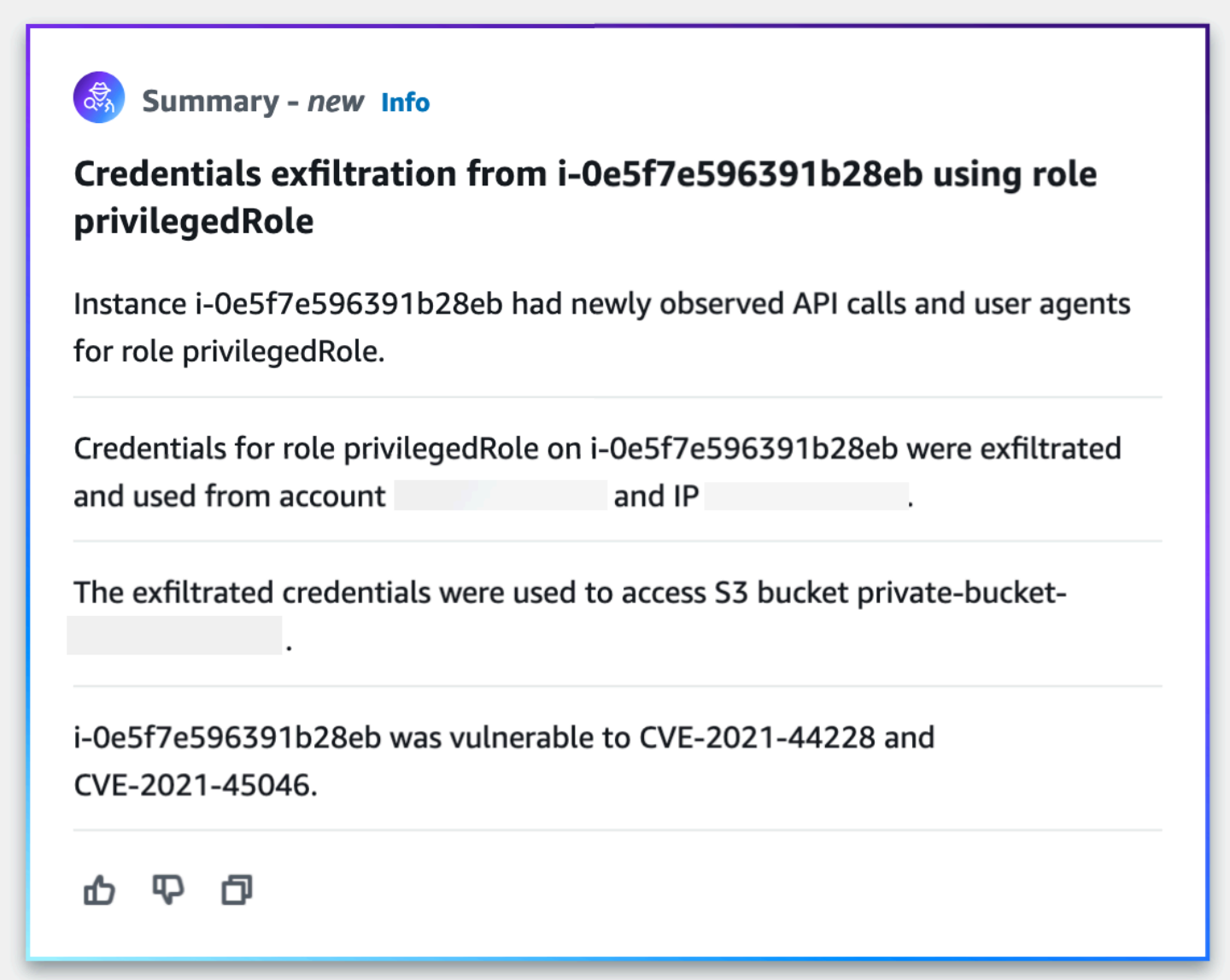
通過調查結果群組的調查結果群組摘要，您會獲得安全事件的清晰詳細說明。說明將以自然語言編寫，包括簡潔的標題，涉及資源的摘要以及有關此類資源的精選資訊。

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。



停用調查結果群組摘要

根據預設，調查結果群組會啟用調查結果群組摘要。您可以隨時停用調查結果群組摘要。如果您停用該功能，您可以在稍後再次啟用。

若要停用調查結果群組摘要

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。

啟用調查結果群組摘要

如果您先前已停用調查結果群組摘要，您可以隨時啟用。

啟用調查結果群組摘要

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。

支援地區

搜尋群組彙總可在下列 AWS 區域中使用。

- 美國東部 (維吉尼亞北部)
- 美國西部 (奧勒岡)
- 亞太區域 (東京)
- 歐洲 (法蘭克福)

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

使用摘要頁面來識別感興趣的實體

使用 Amazon Detective 中的摘要頁面來識別實體，以調查過去 24 小時內活動來源。Amazon Detective 摘要頁面可協助您識別與特定類型異常活動相關聯的實體。這是進行調查的數個可能起點之一。

若要顯示摘要頁面，請在 Detective 導覽窗格中選擇摘要。當您首次開啟 Detective 主控台時，系統按照預設也會顯示摘要頁面。

在摘要頁面中，您可以識別符合以下條件的實體：

- 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

您可以從每個摘要頁面面板錨定至所選實體的設定檔。

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。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 將這些更改與 GuardDuty 發現聯繫起來。

如需有關 Detective 中來源資料的詳細資訊，請參閱行為圖中使用的來源資料。

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 資源是否涉及可能指出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的 AWS 角色或使用者，您可以直接從「調查」面板轉換至該角色或使用者，以繼續調查。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 使用 MaxMind GeoIP 數據庫確定請求的位置。 MaxMind 雖然準確性因國家/地區和 IP 類型等因素而異，但在國家/地區層面報告其數據的準確性非常高。如需相關資訊 MaxMind，請參閱

MaxMind IP 地理位置。如果您認為任何 GeoIP 數據不正確，可以通過「正確的 GeoIP2 數據」向 Maxmind 提交更MaxMind 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。摘要頁面最多會顯示五個群組，依群組排序，群組包含最重要的調查結果，此類調查結果在上週處於作用中狀態。

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。服務連結角色可能會產生大量 AWS CloudTrail 活動，這會取代您要進一步調查的主參與者。您可以選擇關閉顯示服務連結角色，以便從摘要頁面檢視中篩選出服務連結角色。

您可以匯出包含此面板中資料的逗號分隔值 (.csv) 檔案。

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。

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 主 GuardDuty 控台中，選擇調查與所選發現項目相關的實體的選項。

  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 主控台中的 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之資料的相關資訊，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 “檢視設定檔面板並與之互動”。

檢視設定檔面板並與之互動

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。

目錄

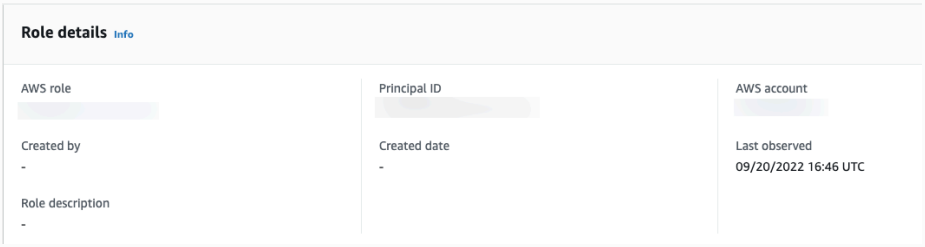
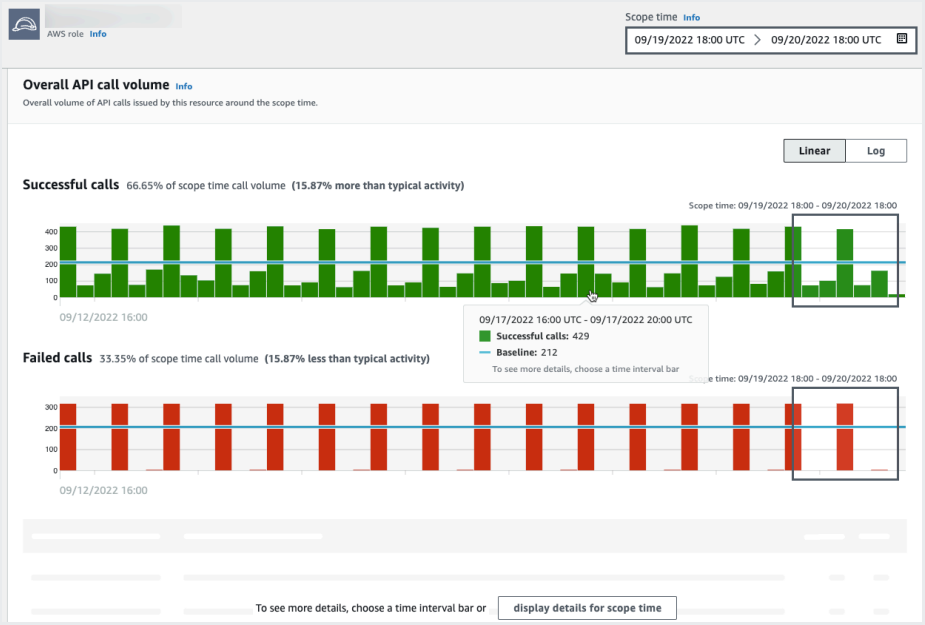
設定檔面板內容

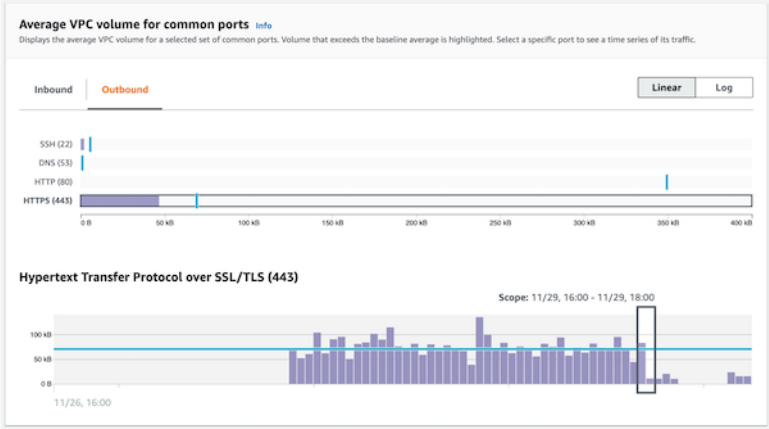
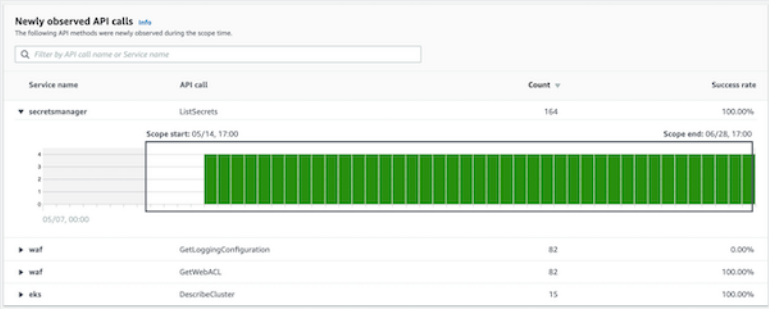
設定檔面板使用不同類型的視覺化來呈現不同類型的資訊。

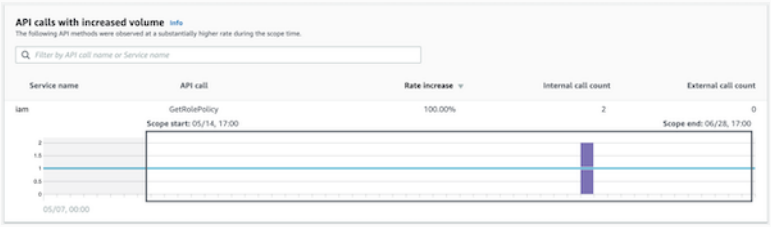
設定檔面板上的資訊類型

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	最簡單的面板類型提供有關實體的部分基本資訊。 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。

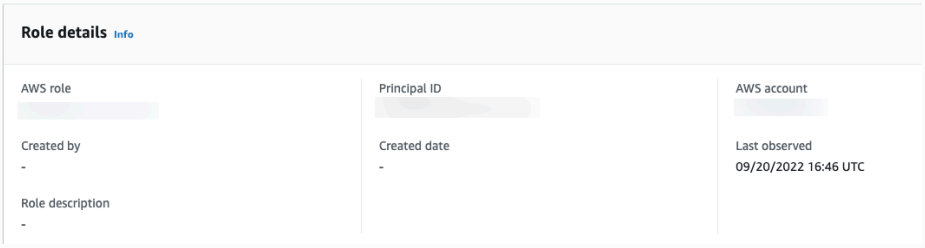
面板資料類型	描述
	 大多數實體設定檔都包含該實體的資訊面板。
活動在一段時間內的一般摘要	顯示實體在一段時間內的活動摘要。 此類型面板提供了實體在範圍時間內行為的整體檢視。  以下是在 Detective 設定檔面板上提供的部分摘要資料範例： • 失敗和成功的 API 呼叫 • 傳入和傳出 VPC 量

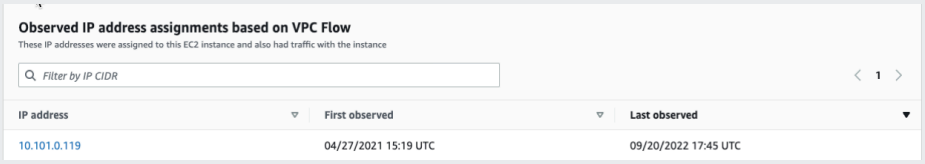
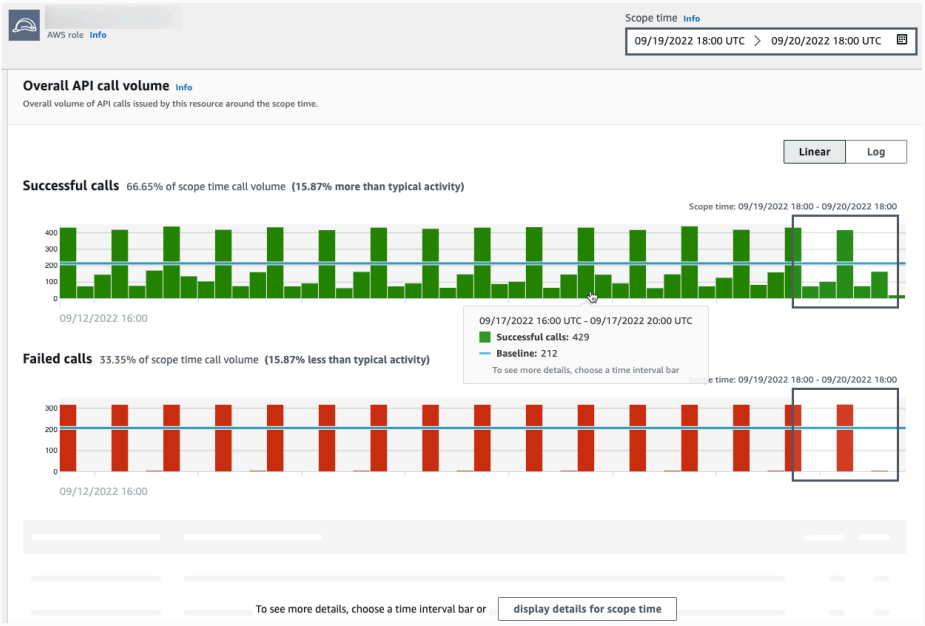
面板資料類型	描述
依值分組的活動摘要	顯示實體的活動摘要，依特定值分組。 您可以在 EC2 執行個體的設定檔上查看此類型的設定檔面板。設定檔面板顯示與特定類型服務相關聯的常用端口的 VPC 流程日誌資料到達和來自 EC2 執行個體的平均流量。 
只在範圍時間內開始的活動	在調查期間，查看在特定時間範圍內才開始發生的活動非常有幫助。 例如，是否存在以前未發現的 API 呼叫、地理位置或使用者代理程式？  如果行為圖表形仍處於訓練模式，則設定檔面板會顯示通知訊息。當行為圖表累積至少兩週的資料時，系統就會移除訊息。如需訓練模型的詳細資訊，請參閱 the section called “新行為圖表的訓練期間”。

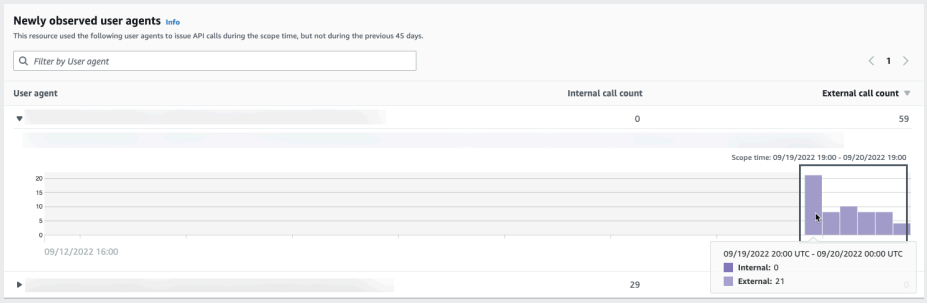
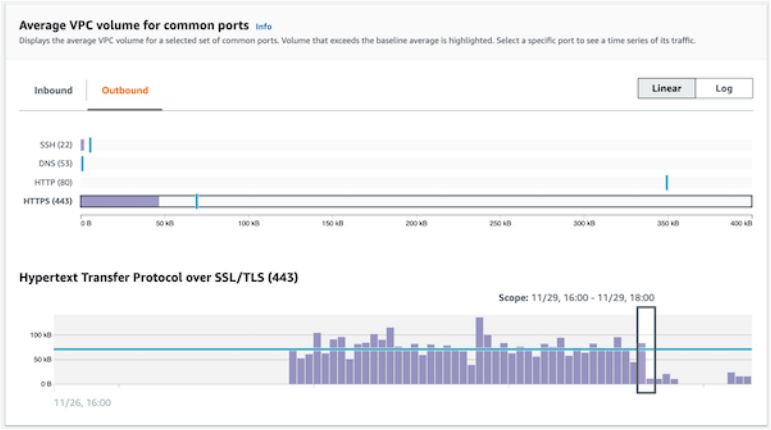
面板資料類型	描述
範圍時間內顯著變更的活動	與新活動面板類似，設定檔面板也可以顯示範圍時間內顯著變更的活動。 例如，使用者可能會每週定期發出數次特定 API 呼叫。如果同一位使用者在單日內突然發出多次相同呼叫，則可能是惡意活動的證據。  如果行為圖表形仍處於訓練模式，則設定檔面板會顯示通知訊息。當行為圖表累積至少兩週的資料時，系統就會移除訊息。如需訓練模型的詳細資訊，請參閱 the section called “新行為圖表的訓練期間”。

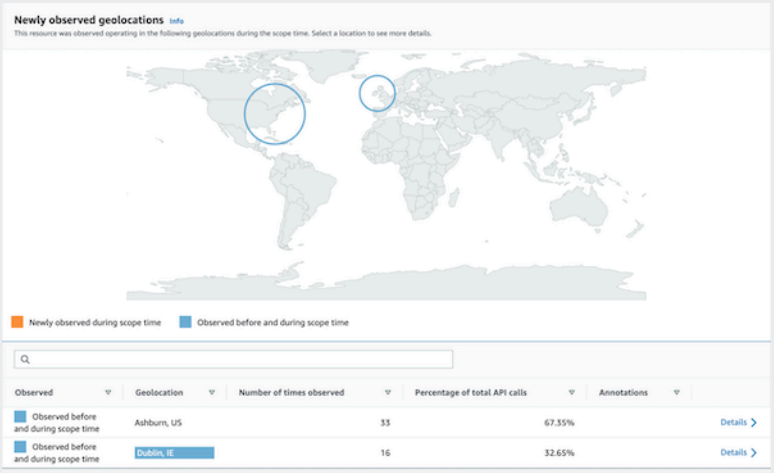
設定檔面板視覺化類型

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

視覺化類型	描述
	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。
資料表	資料表是項目的簡單多欄位清單。  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”。 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。
時間表	時間軸視覺化會顯示定義時間間隔的彙總值。  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。 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。

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
地理位置圖表	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。  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。

設定檔面板內容上的其他注意事項

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 針對 API 呼叫方式的表示變更

自 2021 年 7 月 14 日起，Detective 會追蹤每次進行 API 呼叫的服務。每當 Detective 顯示 API 方法時，它也會顯示相關的服務。在顯示 API 呼叫相關資訊的設定檔面板上，呼叫一律依服務分組。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。

從 2021 年 7 月 14 日開始，針對帳戶和角色，整體 API 呼叫量設定檔面板的活動詳細資訊將不再顯示發出呼叫的資源 AKID。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。

針對顯示 API 呼叫清單的設定檔面板，相關聯的時間軸會反白顯示此轉換發生的時間段。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

在 Detective 主控台中，您可以在偏好設定頁面上設定資料表長度和時間戳記的顯示方式。

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. 前往 https://console.aws.amazon.com/detective/ 開啟 Amazon Detective 主控台。
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. 選擇儲存。

設定時間戳記格式

針對設定檔面板，您可以設定將套用至 Detective 中每個 IAM 使用者或 IAM 角色的所有時間戳記設定時間戳記偏好設定。

> **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. 前往 https://console.aws.amazon.com/detective/ 開啟 Amazon Detective 主控台。
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，時間戳記格式設定為 UTC。按一下編輯以選擇您的當地時區。

   範例：

   Example

   UTC - 2022 年 9 月 20 日 16:39 UTC

   本地 - 2022 年 9 月 20 日上午 9:39 (UTC-07:00)
5. 選擇儲存。

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

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。

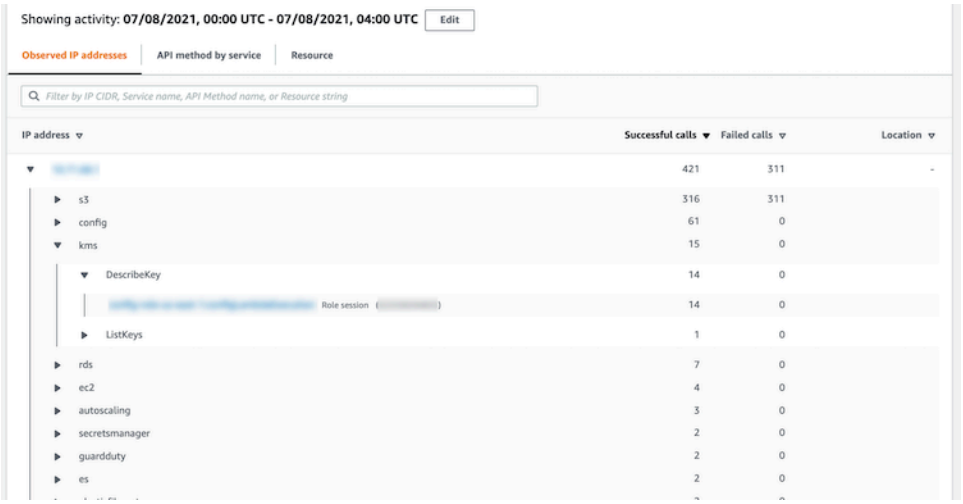
活動詳細資訊包含以下標籤：

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。

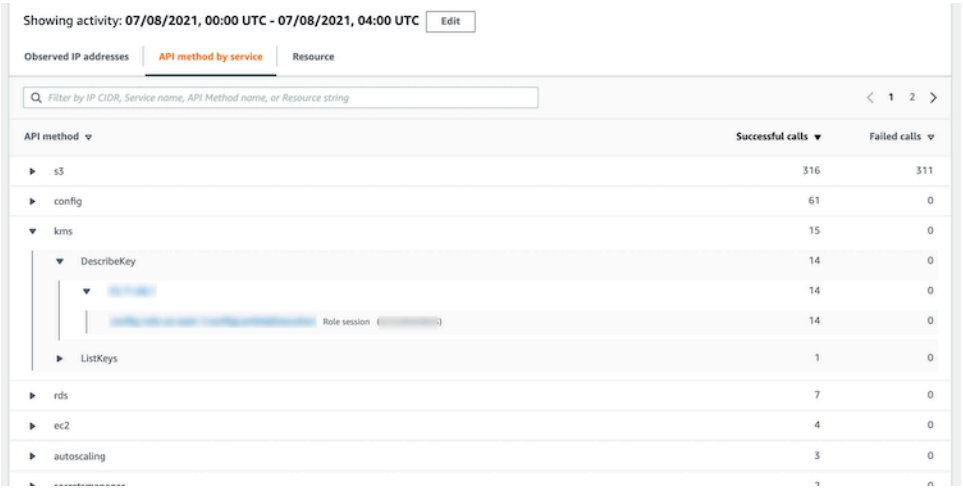


依服務分類的 API 方法

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。

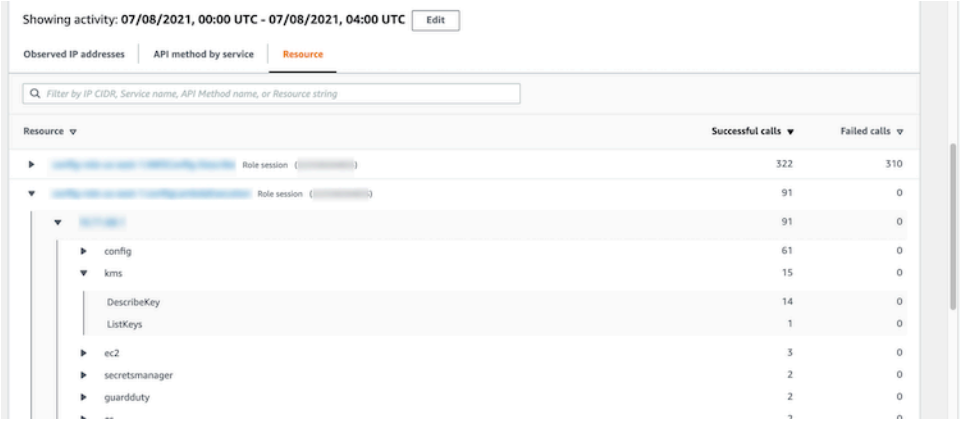


資源或存取金鑰 ID

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。



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。

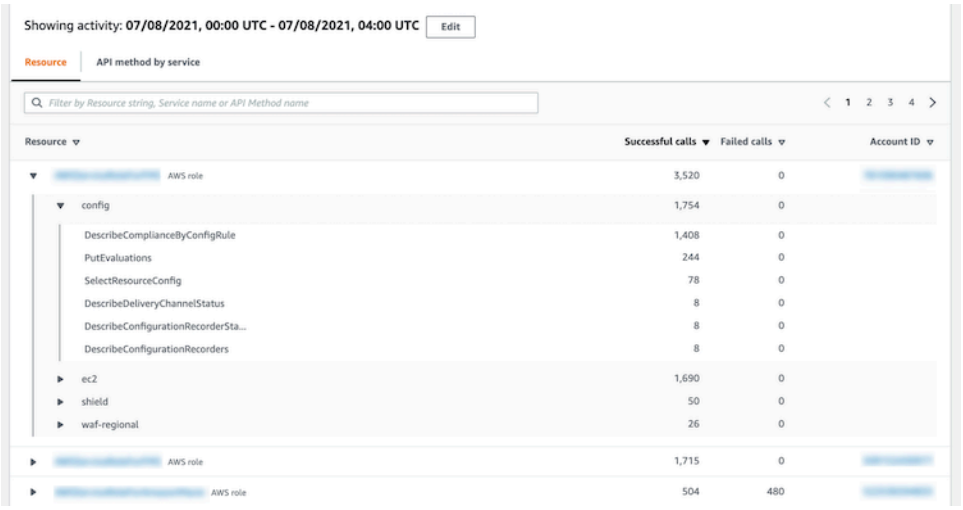
活動詳細資訊包含以下標籤：

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。

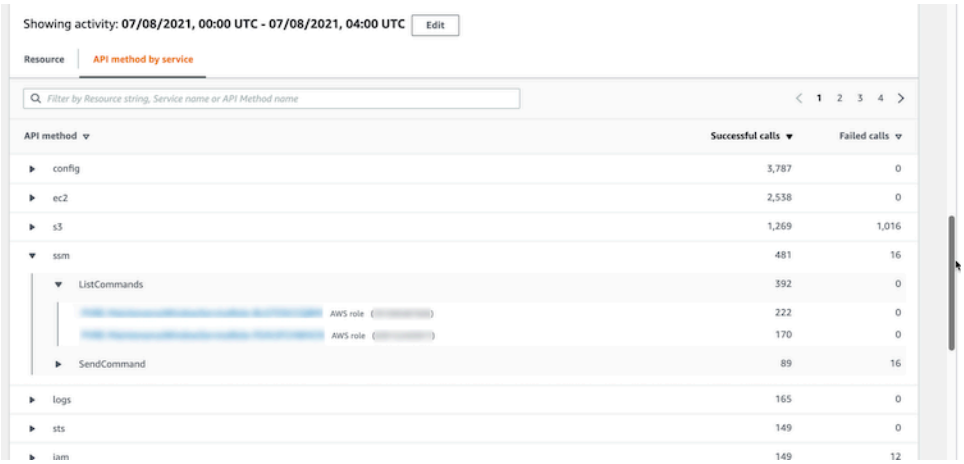
您可以展開每個資源，以顯示資源從 IP 地址發出的 API 呼叫清單。API 呼叫會依發出呼叫的服務分組。如果 Detective 無法判斷已發出呼叫的服務，則該呼叫會列在未知服務下。



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。



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。

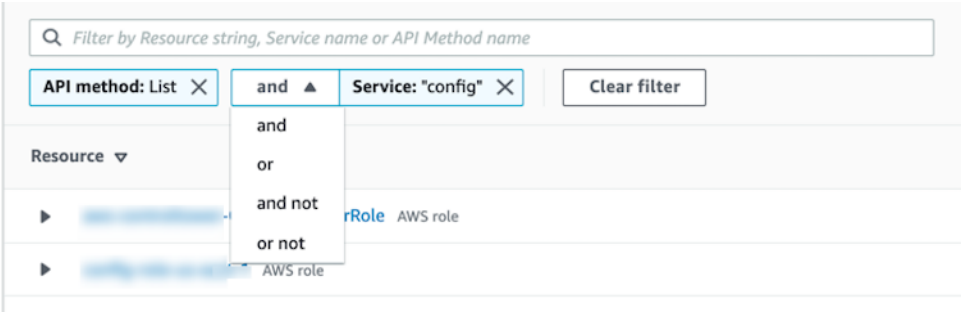
若要新增篩選條件

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. 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。



5. 若要移除篩選條件，請選擇右上角的 x 圖示。
6. 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。

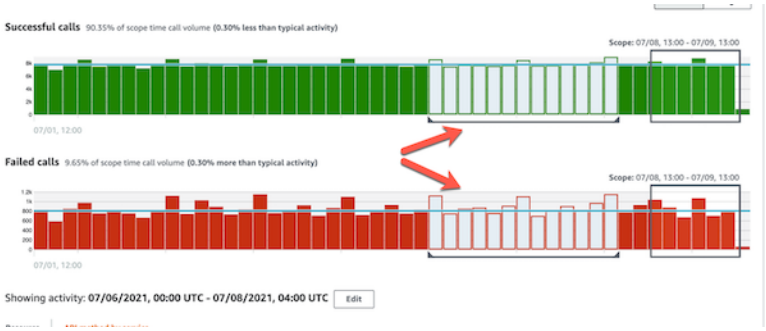
若要變更活動詳細資訊的時間範圍

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 Amazon Security Lake 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
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌

> **Note**
>
> 在 Detective 內查詢原始資料日誌無須額外收費。包括 Amazon Athena 在內的其他 AWS 服務的使用費用仍然按公佈費率收取。

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 使用 MaxMind GeoIP 數據庫確定請求的位置。 MaxMind 雖然準確性因國家/地區和 IP 類型等因素而異，但在國家/地區層面報告其數據的準確性非常高。如需相關資訊 MaxMind，請參閱 MaxMind IP 地理位置。如果您認為任何 GeoIP 數據不正確，可以通過「正確的 GeoIP2 數據」向 Maxmind 提交更MaxMind 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。

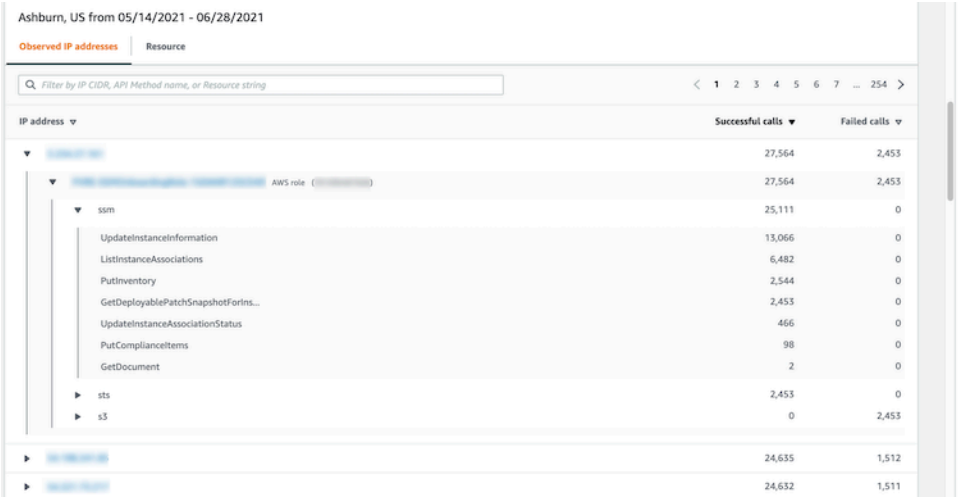
活動詳細資訊包含以下標籤：

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。

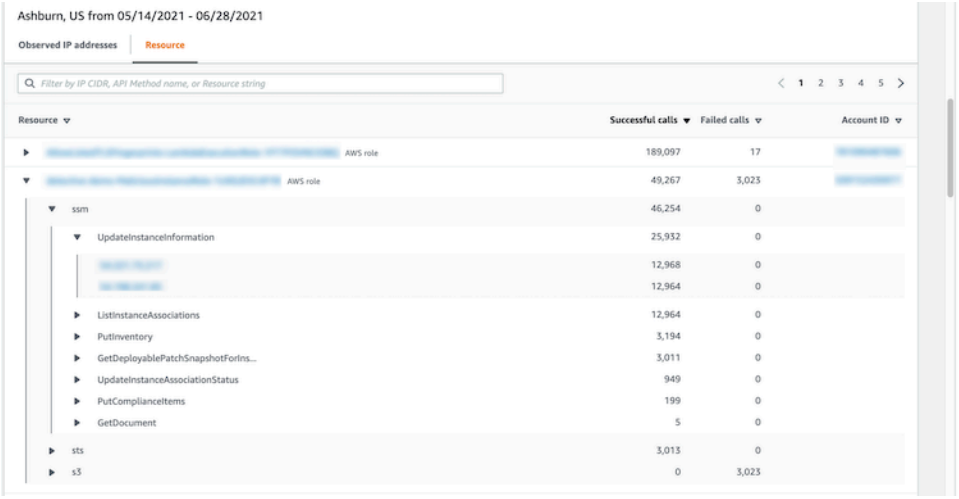


Resource

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。



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。

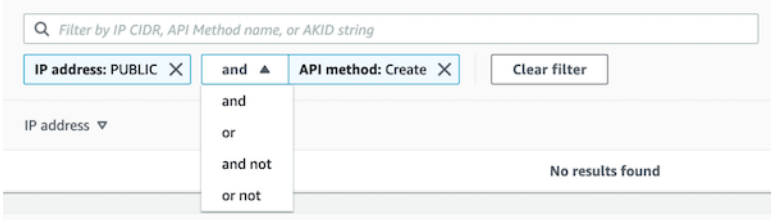
若要新增篩選條件

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. 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。



5. 若要移除篩選條件，請選擇右上角的 x 圖示。
6. 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。

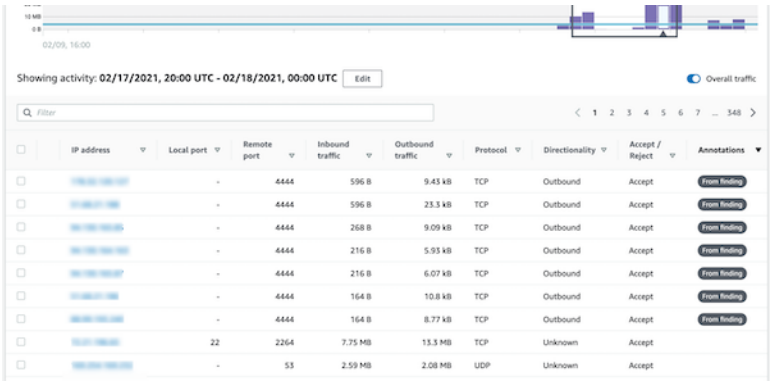
活動內容詳細資訊

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、傳入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。



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：

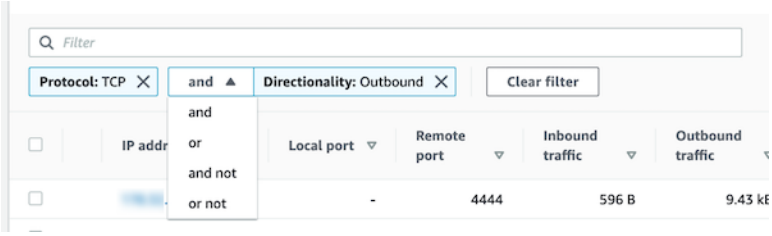
- IP 地址或 EC2 執行個體
- 本機或遠端連接埠
- Direction
- 通訊協定
- 請求是否被接受或拒絕

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。



5. 若要移除篩選條件，請選擇右上角的 x 圖示。
6. 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

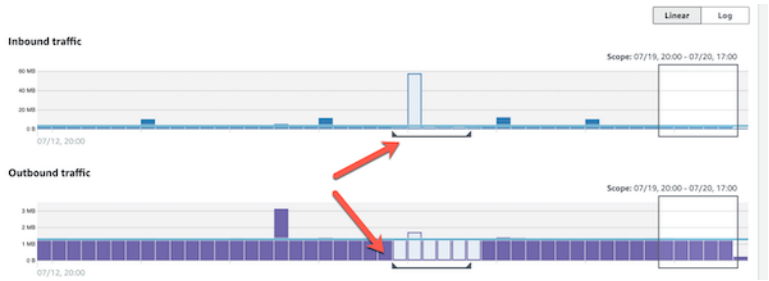
1. 選擇編輯。

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。

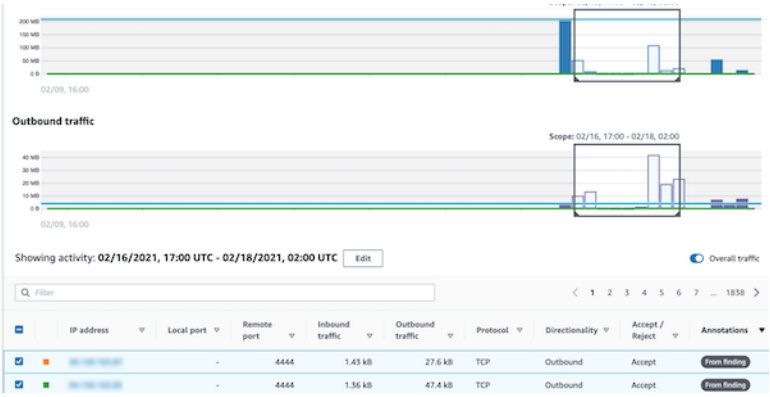
活動詳細資訊的時間範圍會在設定檔面板圖表上反白顯示。



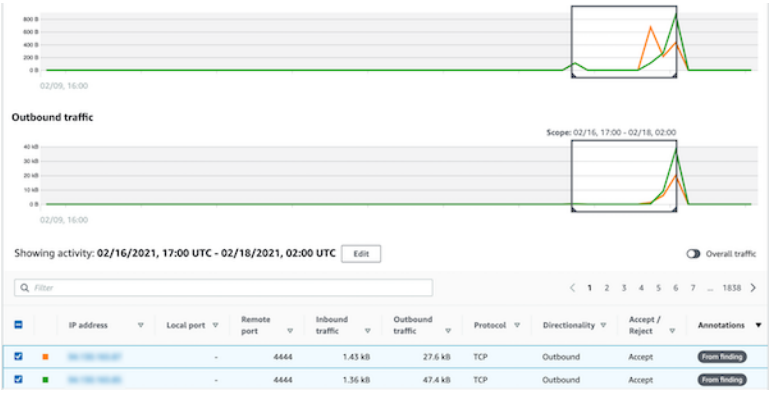
顯示所選列的流量

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：

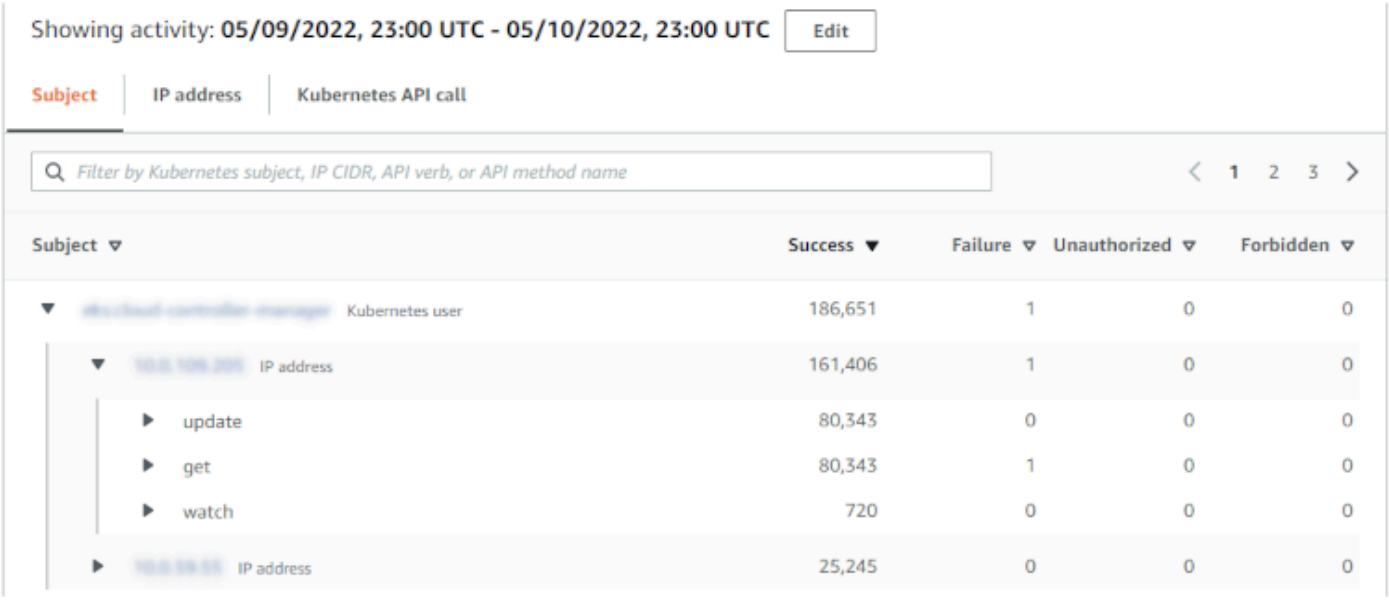
Subject

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。



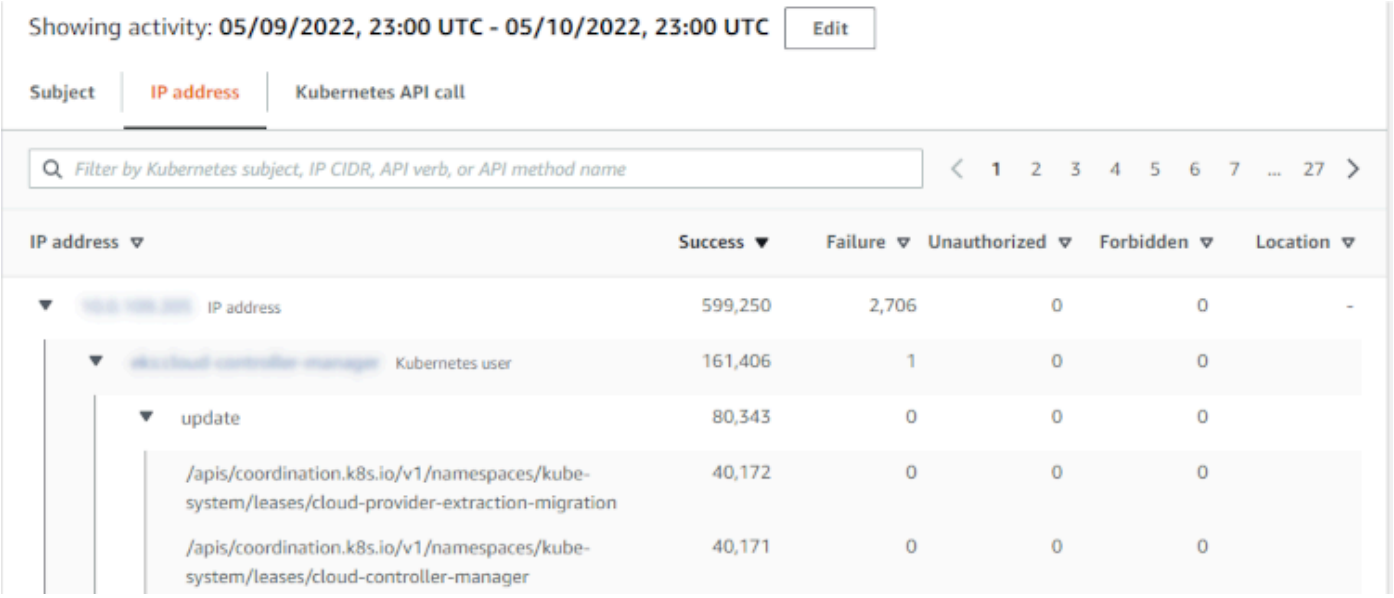
IP Address (IP 地址)

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。



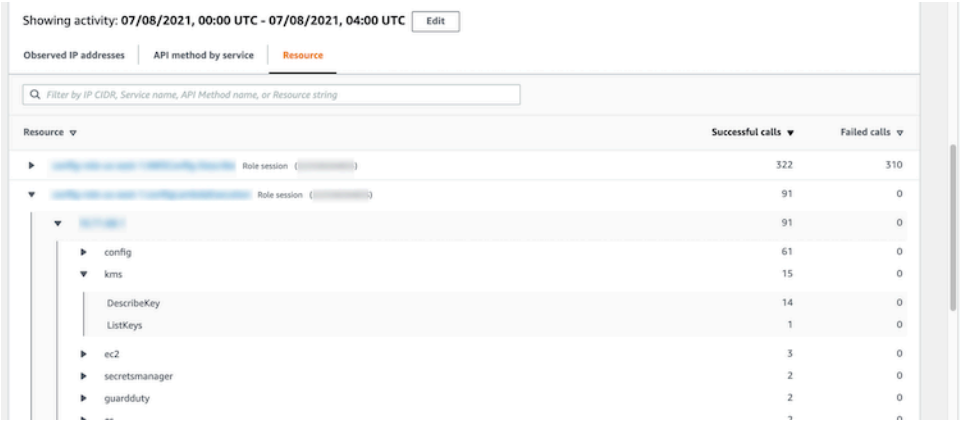
Kubernetes API 呼叫

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。



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

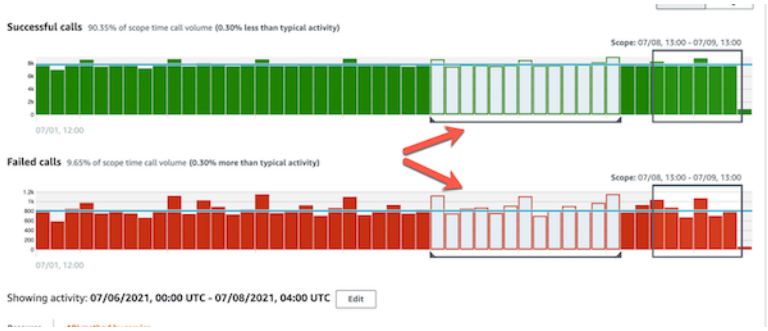
當您首次顯示活動詳細資訊時，時間範圍是範圍時間或選取的時間間隔。您可以變更活動詳細資訊的時間範圍。

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

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 或者 AWS Security Hub，您可以從 GuardDuty 發現轉向相應的 Detective 查找檔案。
- 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。

樞紐到實體設定檔或從 Amazon GuardDuty 或尋找概觀 AWS Security Hub

從 Amazon 主 GuardDuty 控台，您可以導覽至與發現項目相關的實體的實體設定檔。

您也可以從 GuardDuty 和 AWS Security Hub 主控台導覽至發現項目概觀。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

調查連結可用於所有 GuardDuty 發現項目。 GuardDuty 也可讓您選擇導覽至實體設定檔還是搜尋結果概觀。

從 GuardDuty 主控台旋轉至 [Detective]

1. 請在以下位置開啟 GuardDuty 主控台。 https://console.aws.amazon.com/guardduty/
2. 如有必要，請在左側導覽窗格中選擇調查結果。
3. 在「 GuardDuty 發現的項目」頁面上，選擇發現項目。

   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 顯示要在 Detective 中調查的可用項目清單。

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 主控台錨定至 Detective

1. 請在以下位置開啟 AWS Security Hub 主控台。 https://console.aws.amazon.com/securityhub/
2. 如有必要，請在左側導覽窗格中選擇調查結果。
3. 在「發現的 Security Hub」頁面上，選擇一個發 GuardDuty 現項目。
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。

如需調整管理員帳戶之建議的詳細資訊，請參閱建議與 Amazon GuardDuty 和一致 AWS Security Hub。

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 沒有收到存檔的調查結果 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。

- 針對發 GuardDuty 現項目，尋 GuardDuty 找項目識別碼。
- 對於 AWS 帳戶，則為帳戶 ID。
- 若為 AWS 角色和使用者，則為角色或使用者的主參與者識別碼。
- 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。
- 例如 FindingGroups，一個 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值。

- 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 沒有收到來自 Amazon 的存檔調查結果 GuardDuty。
- 在 Detective 開始將資料擷取至行為圖表之前，該调查結果或實體是否已出现？ 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 小號項目允許您將數據從 AWS 服務發送到 Splunk。

您可以配置喇叭項目以生成 Amazon GuardDuty 發現的 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。

小號項目可從以下 GitHub 位置獲得：https://github.com/splunk/ splunk-aws-project-trumpet。

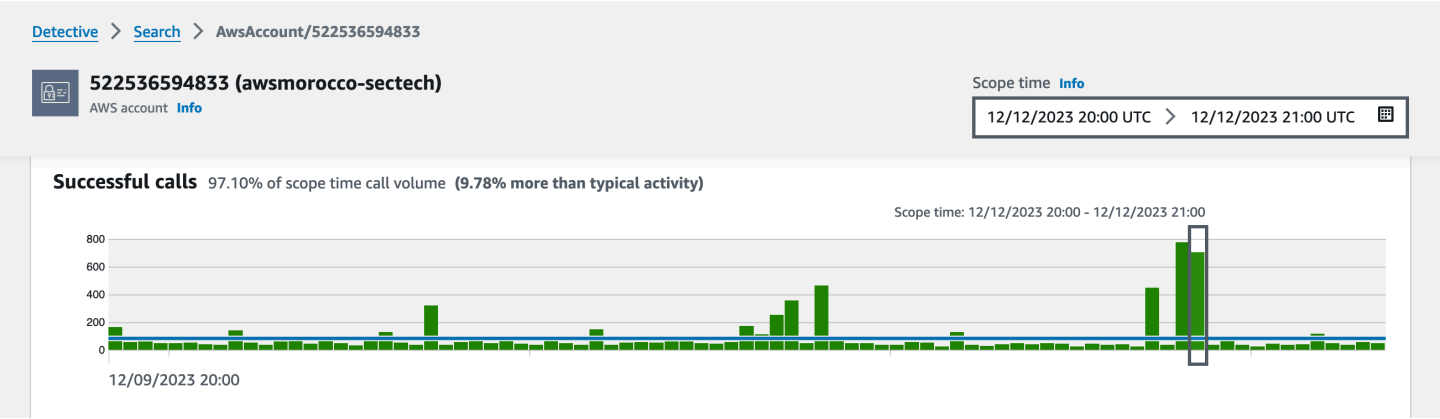
在喇叭專案的設定頁面上，從AWS CloudWatch 活動中選擇 Detective GuardDuty URL。

在設定檔中導覽

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



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時間長度。

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。如需有關 Detective 中來源資料的詳細資訊，請參閱行為圖中使用的來源資料。

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。

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。
- 與發現項 AWS 目相關聯的帳戶，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。請參閱the section called “封存 GuardDuty 發現項目”。

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，每個行為圖都會追蹤 AWS 使用者建立 AWS 角色的時間，以及 EC2 執行個體何時連線到 IP 位址。

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。

管理發現項目和實體

Amazon Detective 提供數個重要功能，協助您搜尋、匯出和管理發現項目。這些功能可協助您針對特定環境量身打造發現結果、減少低價值發現項目所產生的噪音，並協助您專注於獨特 AWS 環境的威脅。檢閱此頁面上的主題，瞭解如何使用這些功能來增加偵探發現的價值。

目錄

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。如需詳細資訊，請參閱 the section called “從 Detective 匯出資料”。

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：

- 針對調查結果，則為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，可以是主參與者識別碼、名稱或 ARN。
- 針對容器叢集，則為叢集名稱或 ARN。
- 針對容器映像，則為儲存庫或容器映像的完整摘要。
- 針對容器 Pod 或任務，則為 Pod 名稱或 Pod 的 UID。
- 針對 EC2 執行個體，則為執行個體識別符或 ARN。
- 針對調查結果群組，則為調查結果群組識別符。
- 針對 IP 地址，則為以 CIDR 或點符號表示的地址。
- 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
- 針對 S3 儲存貯體，則為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 Management Console。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。

針對調查結果、角色、使用者和 EC2 執行個體，搜尋結果包括相關帳戶。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 沒有收到來自 Amazon 的存檔調查結果 GuardDuty。
- 在 Detective 開始將資料擷取至行為圖表之前，該调查結果或實體是否已出现？ 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？ 每個行為圖都是特定於 AWS 區域. 行為圖表不包含來自其他區域的資料。

從 Detective 匯出資料

您可以從 Amazon Detective 摘要頁面和搜尋結果頁面匯出資料。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樣式 `detective-page-panel-yyyy-mm-dd.csv` 格式。您可以使用其他支援 CSV 匯入的 AWS 服務、第三方應用程式或試算表程式來操控資料，以豐富您的安全調查。

> **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。

您可以匯出逗點分隔值 (.csv) 檔案，其中包含來自以下面板和 Detective 頁面的資料：

- 摘要頁面
  - 具有最大 API 呼叫量的角色和使用者面板
  - 最高最大流量的 EC2 執行個體面板
  - 具有建立最多 Kubernetes Pod 的 EKS 叢集面版
- 搜尋頁面：如果您的搜尋傳回 10,000 個以上的結果，則只會匯出前 10,000 個結果。變更排序順序會變更傳回的結果。

歸檔 Amazon GuardDuty 發現

當您完成對 Amazon GuardDuty 發現的調查後，您可以存檔 Amazon Detective 的發現。這樣可以節省您不必返回進 GuardDuty 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 GuardDuty 發現項目相關聯帳戶的 GuardDuty管理員帳戶，則只能從 Detective 內封存發現項目。如果您不是 GuardDuty系統管理員帳戶，而您嘗試封存發現項目， GuardDuty 會顯示錯誤訊息。

若要封存 GuardDuty 發現項目

1. 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。
2. 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 發現項目。若要進一步了解，請參閱 Amazon GuardDuty 使用者指南中的抑制規則。

管理帳戶

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。

如果您與整合 AWS Organizations，則組織管理帳戶會指定組織的 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。

管理員帳戶也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。

Detective 會就其對各行為圖表提供的資料向每個帳戶收取費用。如需有關在行為圖表中追蹤每個帳戶資料量的資訊，請參閱預測和監控 Amazon Detective 費用。

目錄

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。

帳戶和區域

如果您使用 AWS Organizations 來管理帳號，組織管理帳戶會指定組織的 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。

將管理員帳戶與 Security Hub 和 GuardDuty

為了確保 AWS Security Hub 與 Amazon 的整合順利運 GuardDuty 作，我們建議所有這些服務中的管理員帳戶使用相同的帳戶。

請參閱the section called “建議與 GuardDuty 和對齊 AWS Security Hub”。

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。

轉換為使用組織來管理行為圖表帳戶

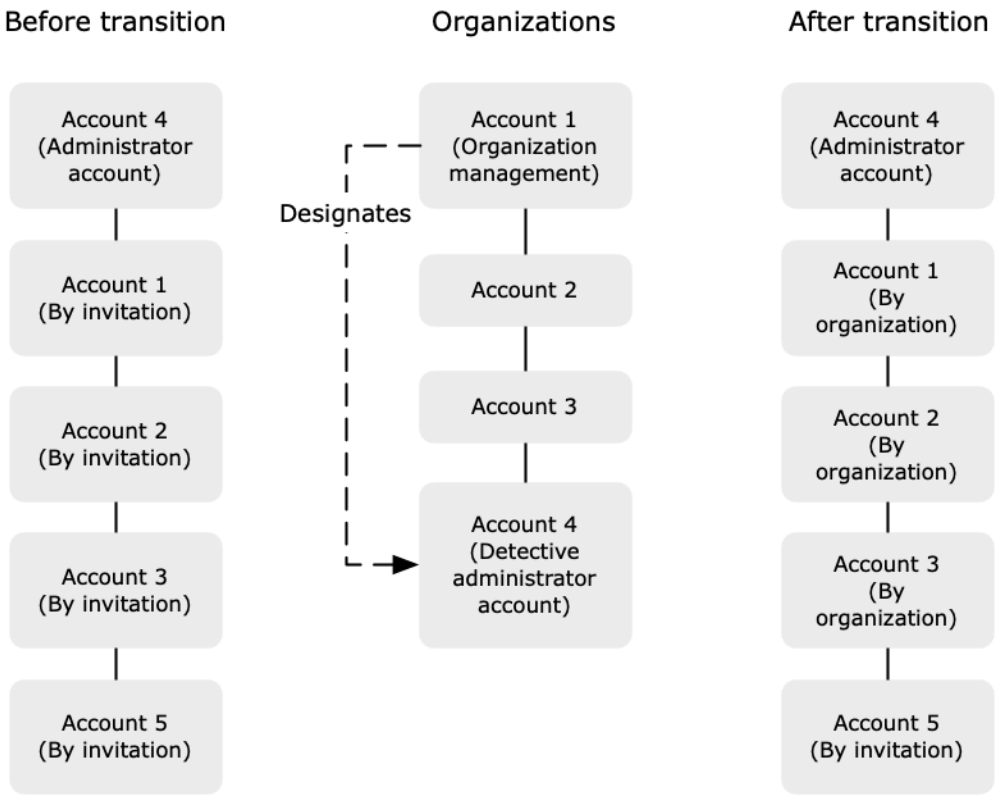
您可能具有現有行為圖表，其中包含接受手動邀請的成員帳戶。如果您已註冊 AWS Organizations，請使用下列步驟來使用「Organizations」來啟用和管理成員帳戶，而不是使用手動邀請程序：

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，則該行為圖表會成爲組織行為圖表。
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 管理員帳戶已經成爲行為圖表的管理員帳戶，則該行為圖表會成爲組織行為圖表。在該行為圖表中已經成爲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 “自動啟用新組織帳戶”。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。

為組織指定 Detective 管理員帳戶

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

組織管理帳戶會指定每個 AWS 區域組織的 Detective 管理員帳戶。

將 Detective 管理員帳戶設定為委派的管理員帳戶

Detective 管理員帳戶也會成為中 Detective 委派的管理員帳戶 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爲組織中委派的管理員。

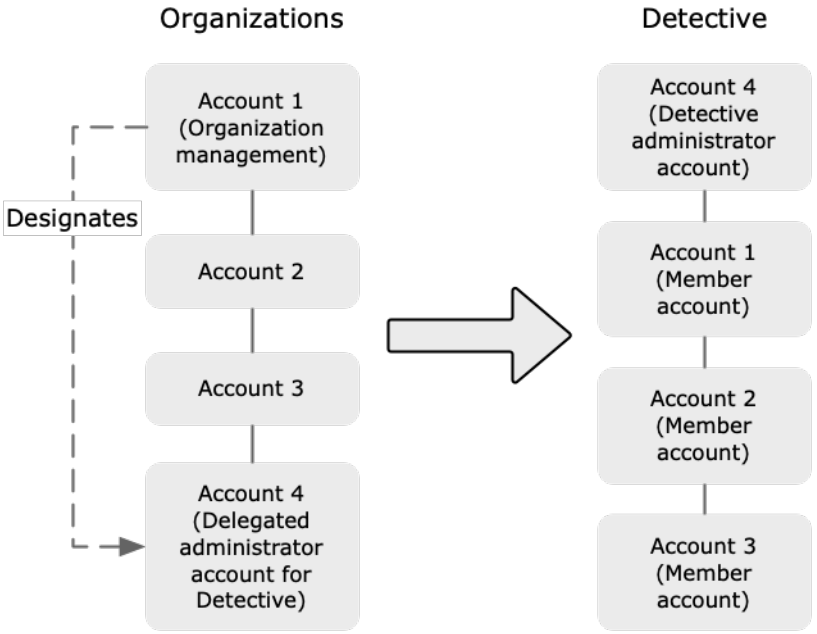
在組織中設定委派的管理員帳戶之後，組織管理帳戶只能選擇委派的管理員帳戶或他們自己的帳戶作為 Detective 管理員帳戶。我們建議您在所有區域中選擇委派的管理員帳戶。

建立及管理組織行為圖表

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，則該行為圖表會成爲組織行為圖表。

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 “管理受邀帳戶”。

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。

設定 Detective 管理員帳戶所需的許可

為了確保組織管理帳戶能夠設定 Detective 管理員帳戶，您可以將 AmazonDetectiveOrganizationsAccess 受管政策連接至您的 AWS Identity and Access Management (IAM) 實體。

指定 Detective 管理員帳戶 (主控台)

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。

若要指定 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 Amazon GuardDuty、 AWS Security Hub或 Amazon Macie 的 Organizations 中有委派的管理員帳戶，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。

若要指定 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 Amazon GuardDuty、 AWS Security Hub或 Amazon Macie 的 Organizations 中有委派的管理員帳戶，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。

指定 Detective 管理員帳戶 (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。

若要指定 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 (主控台)

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。

移除 Detective 管理員帳號 (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。

要刪除 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
```

移除委派的管理員帳戶 (Organizations API， AWS CLI)

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。

若要移除委派的管理員帳戶 (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，所有成員帳戶均爲受邀帳戶。

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 政策來進一步限制對 Detective 特徵和功能的存取。

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。

該狀態可能的發生原因如下：

- 會員帳戶至少 48 小時未成為 Amazon GuardDuty 客戶。
- 成員帳戶資料會導致行為圖表資料量超出 Detective 配額。

列出帳戶 (主控台)

您可以使用 AWS Management Console 來查看和篩選您的帳戶清單。

若要顯示帳戶清單 (主控台)

1. 登入 AWS Management Console。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 帳戶識別碼。
- 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，則爲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。

列出您的會員帳戶（Detective API， AWS CLI）

您可以使用 API 呼叫或檢 AWS Command Line Interface 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。

要檢索成員帳戶列表（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
```

要在行為圖表中擷取有關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
```

以成員帳戶身分管理組織帳戶

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。

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。

Detective 管理員帳戶也可以取消組織帳戶與組織行為圖表的關聯。

目錄

自動將新組織帳戶作為成員帳戶啟用

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 是否可以將組織帳戶作為成員帳戶啟用仰賴於以下情況：

- 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 無法啟用至少 48 小時未 GuardDuty 啟用 Amazon 的帳戶。
- 如果 Detective 會導致行為圖表資料量超過允許的最大值，則無法啟用帳戶。

自動啟用新組織帳戶 (主控台)

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。

自動啟用新的組織帳戶 (Detective API, AWS CLI)

若要判斷是否自動將新組織帳戶作為成員帳戶啟用，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
```

啟用組織帳戶作為成員帳戶

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。

當您啟用組織帳戶時，Detective 會檢查該帳戶是否為 Amazon GuardDuty 客戶至少 48 小時。如果達到該要求，Detective 會檢查帳戶資料是否會導致行為圖表的資料速率超出配額。此檢查需要 24 到 48 小時。

當 Detective 驗證資料速率時，成員帳戶狀態為未啟用。

如果成員帳戶通過這兩項檢查，則成員帳戶狀態會更新為已啟用。Detective 將開始從成員帳戶中擷取資料至行為圖表。

如果其中一項帳戶檢查失敗，則成員帳戶狀態將保持為未啟用。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。

將組織帳戶作為成員帳戶啟用 (主控台)

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。

啟用組織帳戶作為成員帳戶 (Detective API， AWS CLI)

您可以使用 Detective API 或在 AWS Command Line Interface 組織行為圖表中啟用組織帳戶作為成員帳戶。若要取得行為圖表的 ARN 以供在請求中使用，請使用 `ListGraphs` 操作。

若要將組織帳戶啟用為成員帳戶 (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。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
```

取消組織帳戶作為成員帳戶的關聯

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。

當您取消關聯組織帳戶時，狀態會變更為非成員。Detective 會停止從該帳戶擷取資料，但帳戶仍保留在清單中。

取消組織帳戶的關聯 (主控台)

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。

取消組織帳戶的關聯 (Detective API，) AWS CLI

您可以使用 Detective API 或在行為圖表中取消組織帳戶與成員帳戶的關聯。 AWS Command Line Interface

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

若要取消組織帳戶作為組織行為圖表的關聯 (Detective API， AWS CLI)

- 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
```

管理受邀成員帳戶

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，所有成員帳戶均爲受邀帳戶。

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。

管理員帳戶可以從行為圖表中移除受邀成員帳戶。

目錄

邀請成員帳戶至行為圖表

管理員帳戶可以邀請帳戶向行為圖表提供資料。行為圖表最多可容納 1,200 個成員帳戶。

在高層級中，邀請帳戶提供行為圖表的程序如下。

1. 對於要新增的每個成員帳戶，系統管理員帳戶都會提供 AWS 帳號識別碼和 root 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。

   Detective 不會在 AWS GovCloud (美國東部) 或 AWS GovCloud (美國西部) 區域執行此驗證。
3. 如果帳戶資訊有效，Detective 會將邀請傳送至成員帳戶。

   Detective 絕不會向 AWS GovCloud （美國東部）或 AWS GovCloud （美國西部）區域的會員帳戶發送電子郵件邀請。

   針對其他區域，Detective API 提供不向成員帳戶發送邀請的選項。

   此選項對於集中受管的帳戶非常有用。
4. 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。
5. 如果會員帳戶接受邀請，則 Detective 會檢查該會員帳戶是否為 Amazon GuardDuty 客戶至少 48 小時。

   如果達到該要求，Detective 會檢查成員帳戶資料是否會導致行為圖表的資料速率超出配額。

   此檢查可能需要 24 到 48 小時。

   當 Detective 驗證資料速率時，成員帳戶狀態為未啟用。
6. 如果成員帳戶通過這兩項檢查，則成員帳戶狀態會自動更新為已啟用。Detective 將開始從成員帳戶中擷取資料至行為圖表。

   如果其中一項檢查失敗，則成員帳戶狀態將保持為未啟用。成員帳戶不會將資料提供至行為圖表。
7. 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，如果成員帳戶啟用，則成員帳戶狀態會變更為 [已啟用]， GuardDuty 且 Detective 確認其資料磁碟區不是太大，或者管理員帳戶是否移除其他成員帳戶以為帳戶騰出空間。

   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。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。

邀請個別帳戶使用行為圖表 (主控台)

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。

手動選取要邀請的成員帳戶 (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 帳號 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)。

邀請成員帳戶清單至行為圖表 (主控台)

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。每個成員帳號項目都包含 AWS 帳號 ID 和帳戶的 root 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)。

邀請成員帳戶至行為圖表 (Detective API， AWS CLI)

您可以使用 Detective API 或邀請 AWS Command Line Interface 成員帳戶將他們的資料提供至行為圖表。若要取得行為圖表的 ARN 以供在請求中使用，請使用 `ListGraphs` 操作。

若要邀請成員帳戶至行為圖表 (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
```

新增跨區域的成員帳戶清單 (開啟 Python 指令碼 GitHub)

Detective 提供中的開放原始碼指令碼 GitHub ，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。

如需有關如何設定和使用 GitHub 指令集的資訊，請參閱the section called “Amazon Detective Python 腳本”。

啟用未啟用的成員帳戶

成員帳戶接受邀請後，Amazon Detective 會檢查是否可以啟用該成員帳戶。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。這種情況可能是由於下列其中一個原因而發生的。

- 會員帳戶至少 48 小時未成為 Amazon GuardDuty 客戶。
- Detective 正在驗證成員帳戶的資料量。
- 成員帳戶資料會導致行為圖表資料速率超出配額。

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。

啟用未啟用的成員帳戶 (主控台)

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。

啟用未啟用的成員帳戶 (Detective API, AWS CLI)

您可以使用 API 呼叫或啟 AWS Command Line Interface 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 帳戶識別碼。
- AWS CLI：在命令列中執行 `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
```

從行為圖表中移除成員帳戶

管理員帳戶可以隨時從行為圖表中移除成員帳戶。

Detective 會自動移除在中終止的成員帳戶 AWS，但在 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。

從行為圖表中移除成員帳戶 (主控台)

您可以使用從行為圖表中移除受邀的成員帳戶。 AWS Management Console

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。

從行為圖中移除受邀的成員帳戶 (Detective API, AWS CLI)

您可以使用 Detective API 或從您的 AWS Command Line Interface 行為圖表中移除受邀的成員帳號。若要取得行為圖表的 ARN 以供在請求中使用，請使用 `ListGraphs` 操作。

若要從您的行為圖表中移除受邀的成員帳號 (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
```

移除跨區域的受邀成員帳戶清單 (開啟 Python 指令碼 GitHub)

Detective 在中提供了一個開源腳本 GitHub。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。

如需有關如何設定和使用 GitHub 指令集的資訊，請參閱the section called “Amazon Detective Python 腳本”。

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

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>*。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
```

```
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

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 控制台、Detective API，或者 AWS Command Line Interface，會員帳戶可以看到他們的行為圖形邀請。

檢視行為圖表邀請 (主控台)

您可以從檢視行為圖邀請 AWS Management Console。

若要檢視行為圖表邀請 (主控台)

1. 登入 AWS Management Console。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。

  當 Detective 檢查您是否已啟用時，您的帳戶狀態最初設定為「未 GuardDuty 啟用」，如果是，則您的帳戶是否會導致行為圖表的資料量超過 Detective 配額。

  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。

若要擷取已開啟且已接受的行為圖表邀請清單 (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

當您接受邀請後，在 Detective 檢查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。為了讓 Detective 進行此檢查，您的帳戶必須 GuardDuty 啟用 Amazon 至少 48 小時。

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。Detective 會開始從日誌和調查結果中擷取資料，並自該時間點起擷取到行為圖表中。您的帳戶需要為資料付費。

如果新增您的帳戶會導致行為圖表的資料量超出 Detective 配額，或者您尚未 GuardDuty 啟用，則狀態會維持為「未啟用」。在這種情況下，除非您移除帳戶，否則只要行為圖表可以容納帳戶，Detective 就會自動啟用您的帳戶。管理員帳戶也可以手動啟用您的帳戶。

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 Management Console 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。

若要接受行為圖邀請 (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
```

若要拒絕行為圖邀請 (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 AWS Management Console 從行為圖表中移除您的帳戶。

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。

從行為圖中刪除您的帳戶（Detective API， AWS CLI）

您可以使用 Detective API 或從行為圖表中移除您的帳戶。 AWS Command Line Interface

要從行為圖中刪除您的帳戶（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

當系統管理員帳戶在中暫停時 AWS，帳戶會失去檢視 Detective 中行為圖形的權限。Detective 停止將資料擷取至行為圖表中。

當某個成員帳戶被暫停時 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 對關閉的回應如下。

- 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 自管理員帳戶關閉生效日起，保留帳戶的策略資料 90 天。在 90 天期限結束時，會 AWS 永久刪除該帳號的所有策略資料。

- 若要保留問題清單超過 90 天，您可以封存政策。您也可以搭配 EventBridge 規則使用自訂動作，將發現項目儲存在 S3 儲存貯體中。
- 只要 AWS 保留原則資料，當您重新開啟已關閉的帳戶時，會將帳戶 AWS 重新指派為服務管理員，並復原該帳戶的服務原則資料。
- 如需詳細資訊，請參閱關閉帳戶。

> **Important**
>
> 對於 AWS GovCloud (US) 地區的客戶：
>
> - 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 Amazon Detective Python 腳本管理帳戶

Amazon Detective 在 GitHub 存儲庫中提供了一組開源 Python 腳本amazon-detective-multiaccount-scripts。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

這些指令碼需要在管理員帳戶以及您新增或移除的所有成員帳戶中預先存在的 AWS 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：

- 偵探：CreateGraph
- 偵探：CreateMembers
- 偵探：DeleteGraph
- 偵探：DeleteMembers
- 偵探：ListGraphs
- 偵探：ListMembers
- 偵探：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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "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。
- 在上方新增必要的權限 (建議使用)，或選取AmazonDetectiveFullAccess受管理的原則。
- 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` AWS 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《適用於 Linux 的 Amazon EC2 使用者指南》中的 Amazon EC2 Linux 執行個體入門。
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` AWS CloudFormation 範本，則會建立具有名為`EnableDetective`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 腳本

平台	設定說明
Windows	1. 安裝 Python 3 (https://www.python.org/downloads/windows/)。 2. 開啟命令提示。 3. 若要安裝 Boto，請執行：`pip install boto3` 4. 請從 GitHub (https://github.com/aws-samples/ amazon-detective-multiaccount-scripts) 下載指令碼原始程式碼。
Mac	1. 安裝 Python 3 (https://www.python.org/downloads/mac-osx/)。 2. 開啟命令提示。 3. 若要安裝 Boto，請執行：`pip install boto3` 4. 請從 GitHub (https://github.com/aws-samples/ amazon-detective-multiaccount-scripts) 下載指令碼原始程式碼。
Linux	1. 若要安裝 Python 3，請執行以下其中一項： • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. 若要安裝 Boto，請執行：`sudo pip install boto3` 3. 從 https://github.com/aws-samples/ 克隆腳本源代碼amazon-detective-multiaccount-scripts。

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。每個成員帳號項目都包含 AWS 帳號 ID 和帳戶的 root 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 帳戶的帳號 ID。

roleName

管理員帳戶和每個成員帳戶中所承擔的 AWS 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 帳戶的帳號 ID。

roleName

管理員帳戶和每個成員帳戶中所承擔的 AWS 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。

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，將來自環 AWS 境、SaaS 供應商、內部部署來源、雲端來源和第三方來源的安全性資料，自動集中至儲存在您帳戶中的專用資料湖。 AWS 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 最多支持源版本 2（OCSF 1.1.0）。

- AWS CloudTrail 管理事件版本 1.0 及之後
- Amazon Virtual Private Cloud（Amazon VPC）流程日誌 1.0 版及之後
- Amazon Elastic Kubernetes Service（Amazon EKS）審計日誌 2.0 版。若要使用 Amazon EKS 稽核日誌做為來源，您必須新增`ram:ListResources`至 IAM 許可。如需詳細資訊，請參閱將所需的 IAM 許可新增至您的帳戶。

如需有關 Security Lake 如何自動將來自本機支援 AWS 服務的日誌和事件轉換為 OCSF 結構描述的詳細資訊，請參閱 Amazon 安全湖使用者指南。

將 Detective 與安全湖整合後，Detective 會開始從安全湖擷取與 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。

若要將 Detective 與 Security Lake 整合，請完成以下步驟：

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。確定已啟用安全湖，並確認 Security Lake 正在從 AWS CloudTrail 管理事件和 Amazon 虛擬私人雲端 (Amazon VPC) 流程日誌收集日誌和事件。

   為了配合安全參考架構，Detective 建議使用記錄封存帳戶，並延遲使用安全性工具帳戶進行 Security Lake 部署。

2. 建立 Security Lake 訂閱用戶

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. 將所需 AWS Identity and Access Management (IAM) 許可新增至您的 IAM 身分。
   - 新增下列權限以建立與安全湖的 Detective 整合：
     - 將這些 AWS Identity and Access Management (IAM) 許可附加至您的 IAM 身分。如需詳細資訊，請參閱將所需的 IAM 許可新增至您的帳戶一節。
     - 將此 IAM 政策新增至您打算用來傳遞 AWS CloudFormation 服務角色的 IAM 主體。如需詳細資訊，請參閱將許可新增至 IAM 主體一節。
   - 如果您已將 Detective 與安全湖整合，若要使用整合功能，請將這些 (IAM) 許可附加到您的 IAM 身分。如需詳細資訊，請參閱將所需的 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 範本來設定建立和管理 Security Lake 訂戶查詢存取權所需的參數。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。

有關如何使用 Detective 控制台將 Amazon Detective 與 Amazon 安全湖集成的演示，請觀看以下視頻：Amazon Detective 與 Amazon 安全湖集成-如何設置-->

開始之前

安全湖與 AWS Organizations 整合，可管理組織中多個帳戶的記錄收集。若要針對組織使用 Security Lake，您的 AWS Organizations 管理帳戶必須先為組織指定委派的 Security Lake 系統管理員。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。

在將 Security Lake 與 Detective 進行整合之前，請確定已為 Security Lake 管理員帳戶啟用 Security Lake。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，請確認安全湖正在從 AWS CloudTrail 管理事件和 Amazon 虛擬私有雲端 (Amazon VPC) 流程日誌收集日誌和事件。如需有關 Security Lake 中記錄收集的詳細資訊，請參閱 Amazon Security Lake 使用者指南中的從 AWS 服務收集資料。

步驟 1：建立 Security Lake 訂閱用戶

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 AAmazon Athena 等服務，直接在 Amazon 簡單儲存服務 (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。

請依照以下步驟將查詢存取權授予 Detective 帳戶管理員。

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：將 IAM 許可新增至您的帳戶

若要啟用與安全湖的 Detective 整合，您必須將下列 AWS Identity and Access Management (IAM) 許可政策附加至您的 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附加到 IAM 身分的必要許可，請聯絡您的 AWS 管理員。如果您擁有必要的許可但發生問題，請參閱《IAM 使用者指南》中的一般 IAM 問題疑難排解。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess",
        "ram:ListResources"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
        ]
    },
    {
      "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 邀請並啟用整合

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。

在下一個步驟中，您將使用 AWS CloudFormation 範本建立堆疊：接受 Resource Share ARN 邀請、建立必要的資 AWS Glue 編目程式 源，以及授予 AWS Lake Formation 系統管理員權限。

建立 AWS CloudFormation 堆疊的步驟

1. 使用 CloudFormation 範本建立新 CloudFormation 堆疊。如需詳細資訊，請參閱使用 AWS CloudFormation 範本建立堆疊。
2. 完成堆疊建立之後，請選擇啟用整合。

使用 AWS CloudFormation 範本建立堆疊

Detective 提供 AWS CloudFormation 範本，您可以使用此範本來設定建立和管理 Security Lake 訂閱者查詢存取權所需的參數。

步驟 1：建立 AWS CloudFormation 服務角色

您必須建立 AWS CloudFormation 服務角色，才能使用 AWS 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 Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。

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 AWS 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。請<Account ID>以您的 AWS 帳號 ID 取代。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
```

```
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
```

```
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

步驟 2：將許可新增至您的 IAM 主體

您需要下列權限，才能使用您在上一個步驟中建立的 CloudFormation 服務角色建立堆疊。將下列 IAM 政策新增至您打算用來傳遞 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。

```
 {
    "Version": "2012-10-17",
    "Statement": [
        {
             "Sid": "PassRole",
             "Effect": "Allow",
             "Action":
             [
                "iam:GetRole",
                "iam:PassRole"
             ],
             "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
        },
        {
            "Sid": "RestrictCloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:UpdateStack"
```

```
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
            "Condition": {
                "StringEquals": {
                    "cloudformation:RoleArn": [
                        "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                    ]
                }
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

步驟 3：在 AWS CloudFormation 控制台中指定自定義值

1. 從 Detective 轉到 AWS CloudFormation 控制台。

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— 輸入您要授與存取權以使用安全湖整合的 IAM 主體 (例如 IAM 角色 ARN) 的 ARN，以逗號分隔。這些可能是您使用 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 **LakeFormationPrincipals** 中的 IAM 主體

(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>/*"
  ]
}
```

athena-results-bucket以AthenaResultsBucket名稱取代。 AthenaResultsBucket可以在 AWS CloudFormation 控制台上找到：

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
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。

刪除堆 CloudFormation 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 刪除 CloudFormation 堆疊。

要刪除 AWS CloudFormation 堆棧（控制台）

1. 請在以下位置開啟 AWS CloudFormation 主控台。 https://console.aws.amazon.com/cloudformation
2. 在 CloudFormation 主控台的 [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Failed to delete stack後看到訊息的權限錯誤，表示您的 IAM 角色沒有刪除堆疊的 CloudFormation 權限。請聯絡您的帳戶管理員以刪除堆疊。

若要刪除 CloudFormation 堆疊 (AWS CLI)

在 AWS CLI 介面中輸入下列命令：

```
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。

變更整合組態

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 AWS CloudFormation 範本以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 AWS CloudFormation 樣板中輸入的值。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，請參閱刪除堆 CloudFormation 疊。

   1. 建立新 CloudFormation 堆疊。如需詳細資訊，請參閱使用 AWS CloudFormation 範本建立堆疊。
7. 選擇啟用整合。

停用整合

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，請參閱刪除堆 CloudFormation 疊。
4. 在停用 Security Lake 整合窗格中，選擇停用。

支援的 AWS 地區

您可以在以下 AWS 區域將 Detective 與安全湖整合。

區域名稱	區域	端點	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
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.amazonaws.com	HTTPS
歐洲 (法蘭克福)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
歐洲 (愛爾蘭)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS

區域名稱	區域	端點	通訊協定；
歐洲 (倫敦)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
歐洲 (巴黎)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
歐洲 (斯德哥爾摩)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
南美洲 (聖保羅)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

在 Detective 中查詢原始日誌

將 Detective 與安全湖整合後，Detective 會開始從安全湖擷取與 AWS CloudTrail 管理事件和亞馬遜虛擬私人雲端 (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。包括 Amazon Athena 在內的其他 AWS 服務的使用費用仍然按公佈費率收取。

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 角色會話
- Amazon EC2 執行個體
- Amazon S3 儲存貯體
- IP 地址
- 庫伯尼特斯叢集
- 庫伯涅茨吊艙

- 库伯涅茨主题
- IAM 角色
- IAM 角色工作階段
- IAM 使用者

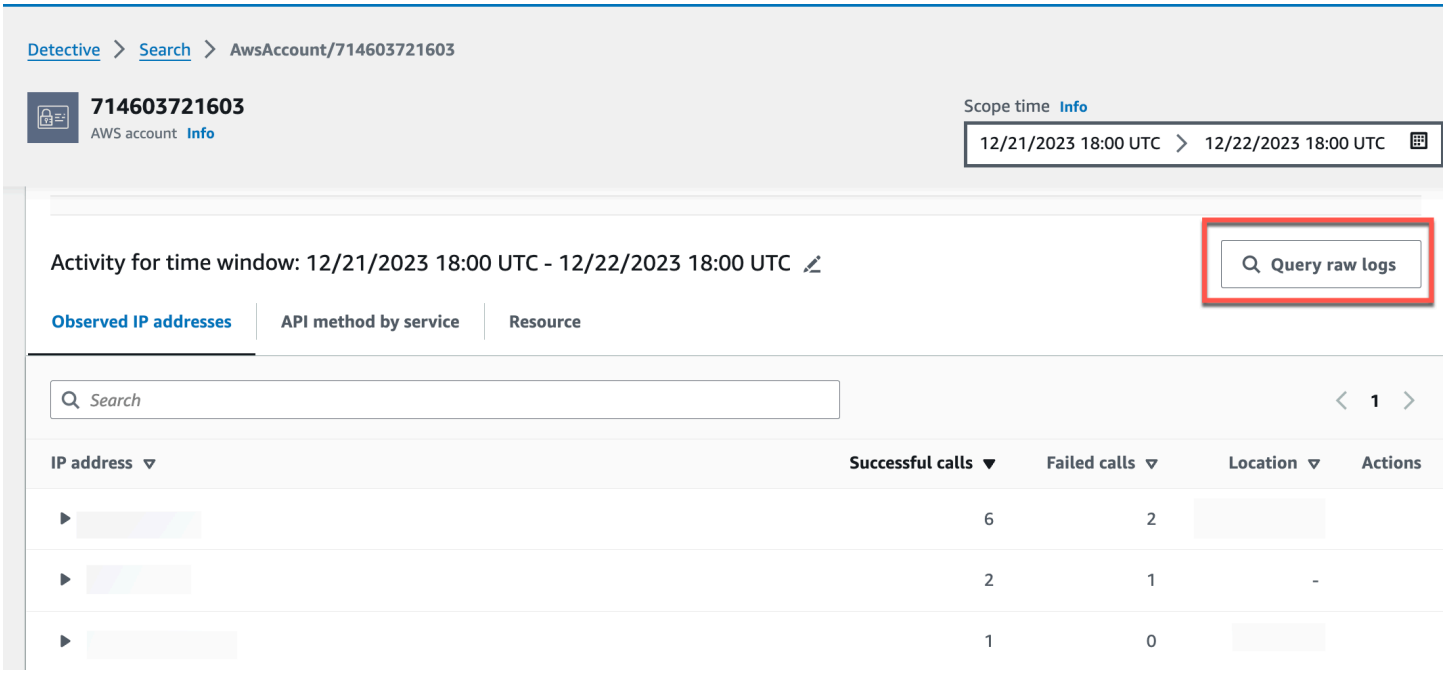
Amazon VPC Flow Logs 可用於下列設定檔：

- Amazon EC2 執行個體
- Kubernetes Pod

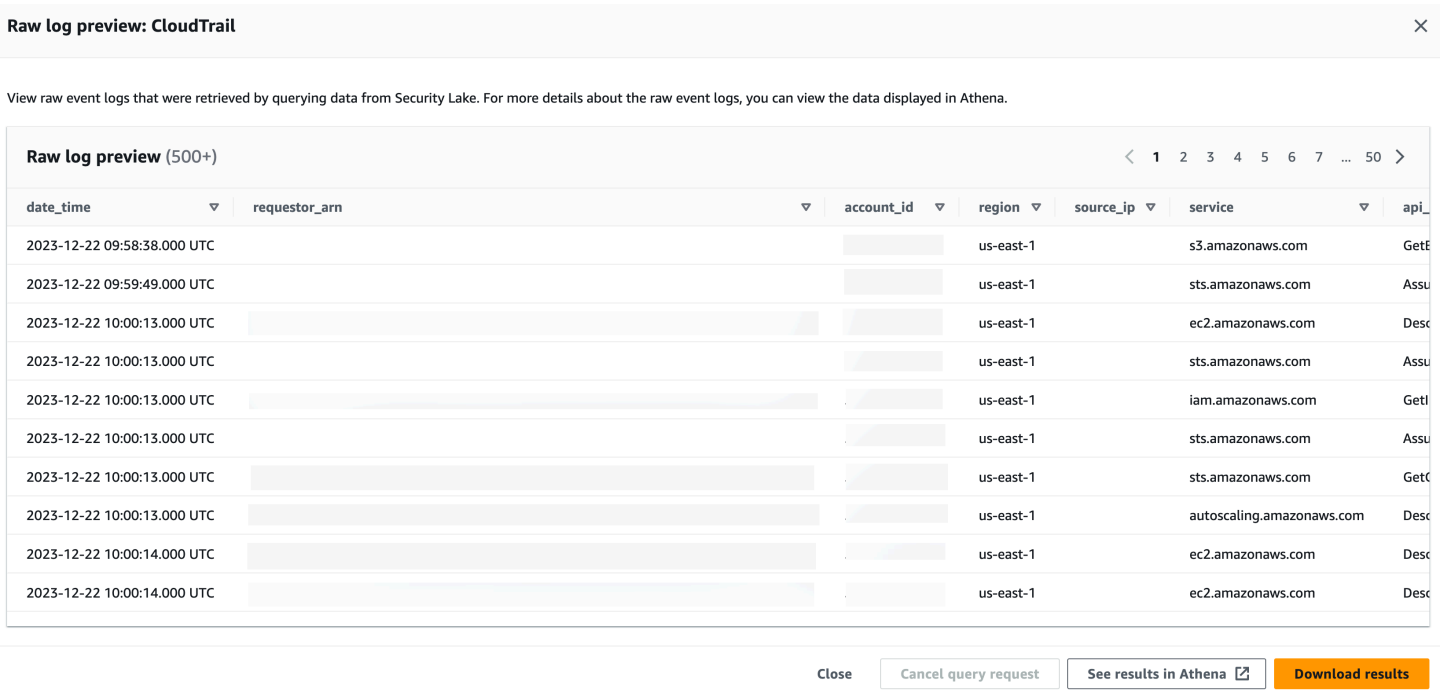
有關如何使用 Detective 控制台將 Amazon Detective 與 Amazon 安全湖集成的演示，請觀看以下視頻：Amazon Detective 與 Amazon 安全湖集成-如何使用-->

查詢 AWS 帳戶的原始日誌

1. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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. 您可以在此開始查詢原始日誌。



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。

範例

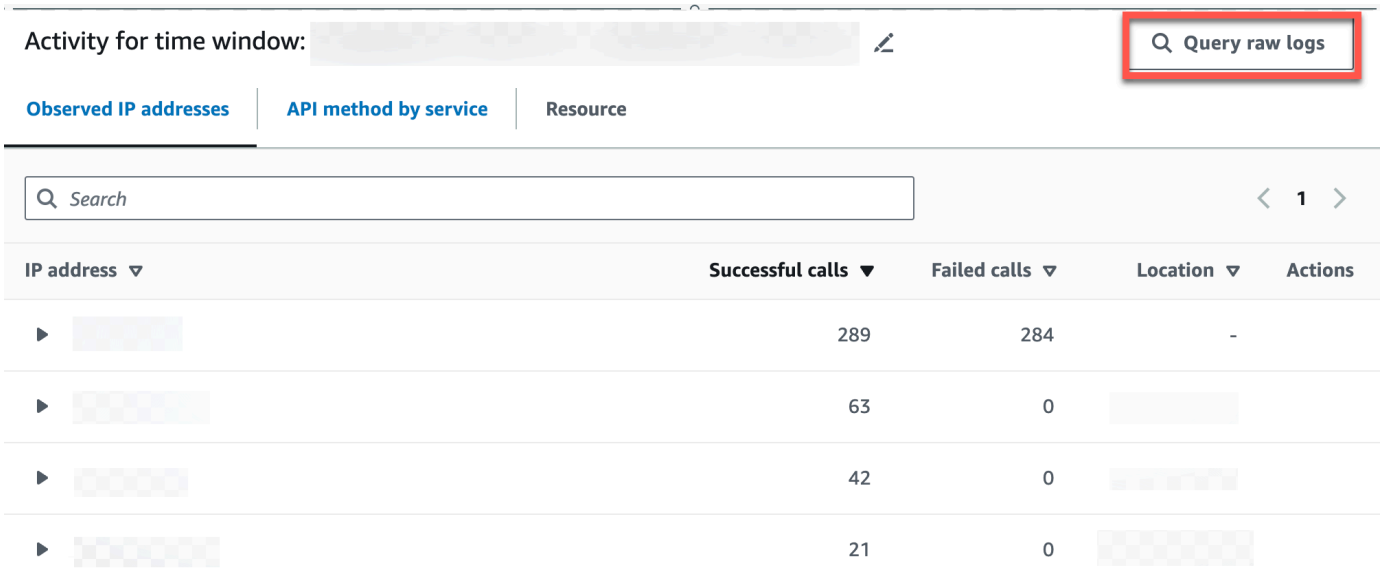
- 查詢 AWS 角色的原始記錄
- 查詢 Amazon EKS 叢集的原始日誌
- 查詢 Amazon EC2 執行個體的原始日誌

查詢 AWS 角色的原始記錄

如果您想了解 AWS 角色在新地理位置中的活動，可以在 Detective 控制台中進行此操作。

查詢 AWS 角色的原始日誌

1. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
2. 從 [Detective 摘要] 頁面 [新觀察的地理位置] 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. 對於 AWS 角色，展開資源以顯示該資源從該 IP 位址發出的特定 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。

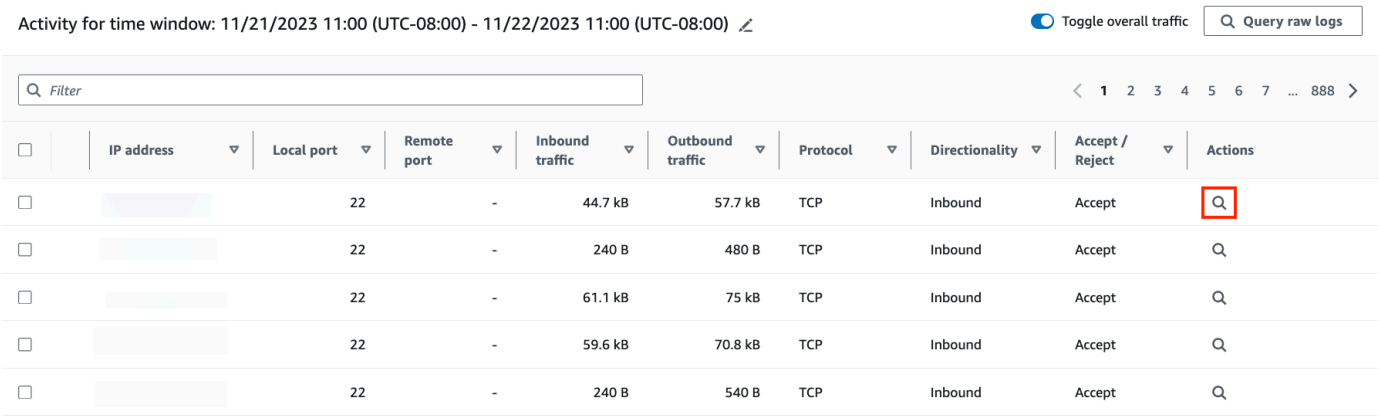


查詢 Amazon EKS 叢集的原始日誌

1. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
2. 從 [Detective 摘要] 頁面建立最多網繭的容器叢集區段中，導覽至 Amazon EKS 叢集。
3. 在 Amazon EKS 叢集詳細資料頁面中，選取 Kubernets API 活動索引標籤。
4. 在涉及此 Amazon EKS 叢集的整體 Kubernets API 活動區段中，選擇範圍時間的顯示詳細資料。
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. 前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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。



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。

Amazon Detective 中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。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 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。

  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 的合規計劃，請參閱合規計劃範圍內的AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 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。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 Detective 資源。

目錄

Amazon Detective 中的資料保護

AWS 共同責任模型適用於 Amazon Detective 中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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。這包括當您 AWS 服務 使用主控台、API 或 AWS SDK 與 Detective 或其他 AWS CLI人合作時。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。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

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

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) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 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。您可以使用 IAM AWS 服務 ，無需額外付費。

目錄

物件

您如何使用 AWS Identity and Access Management （ IAM ），具體取決於您在 Detective 中所做的工作。

服務使用者：如果使用 Detective 服務執行工作，管理員會為您提供所需的憑證和許可。隨著您為了執行作業而使用的 Detective 功能數目增多，您可能會需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。若您無法存取 Detective 中的某項功能，請參閱 Amazon Detective 身分識別和存取疑難排解。

服務管理員：如果您負責公司內的 Detective 資源，您可能具備 Detective 的完整存取許可。您的任務是判斷服務使用者應存取的 Detective 功能及資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司可搭配 Detective 使用 IAM 的方式，請參閱 Amazon Detective 如何搭配 IAM 運作。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 Detective 存取的詳細資訊。若要檢視您可以在 IAM 中使用的範例 Detective 身分型政策，請參閱 Amazon Detective 身分型政策範例。

使用身分來驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料

都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或

AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 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。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 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 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，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 Management Console AWS CLI、或 AWS API 執行工作。Detective 管理員必須擁有 AWS Identity

and Access Management (IAM) 政策，以授予 IAM 使用者和角色權限，才能在所需的指定資源上執行特定 API 作業。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。管理員帳號也可以使用行為圖表來分類和調查與這些帳號相關聯的發現項目和資源。

  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。

若要深入瞭解 Detective 和其他人如何 AWS 服務 使用 IAM，請參閱 IAM 使用者指南中的 JSON 索引標籤上建立政策。

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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 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，可能會邀請同一個 AWS 帳戶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:056d2a9521xi2bbluw1d164680eby416"
]
```

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哪些內容。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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。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。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。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。

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或等 AWS STS API 作業來取得臨時安全登入資料GetFederationToken。

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 Management Console AWS CLI、或 AWS API 執行工作。

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

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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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。

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "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。

```
{"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。

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
```

```
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "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。

```
{
    "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。

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

```
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

AWS Amazon Detective 的管理政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略：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。他們也可以封存 GuardDuty 發現項目。此原則會提供 Detective 主控台需要的權限，才能顯示所在帳號的帳號名稱 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。
- `guardduty`— 允許校長從「Detective」中取得及封存 GuardDuty發現項目。
- `securityhub`：允許主體從 Detective 中取得 Security Hub 調查結果。

```
{
    "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 受管理的策略：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。

```
{
  "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— 允許校長從「Detective」中取得及封存 GuardDuty發現項目。
- securityhub：允許主體從 Detective 中取得 Security Hub 調查結果。
- organizations— 允許主參與者從 AWS Organizations中擷取組織中帳號的相關資訊。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。

```
{
  "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 受管理的策略： 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— 允許主參與者從 AWS Organizations中擷取組織中帳號的相關資訊。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，以及允許主體在其他安全服務 (例如 Amazon Detective ent GuardDuty、Amazon Macie 和) 中擷取委派管理員帳戶。 AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS 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。

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS 受管理政策的 Detective 更新

檢視由於此服務開始追蹤這些變更以來，Detective 的 AWS 受管理原則更新詳細資料。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	日期
AmazonDetectiveInvestigatorAccess：現有政策的更新	在 `AmazonDetectiveInvestigatorAccess` 政策中新增了 Detective 調查和調查結果群組摘要動作。 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。	2023 年 11 月 26 日
AmazonDetectiveFullAccess 和 AmazonDetectiveInvestigatorAccess – 對現有政策的更新	Detective 將 Security Hub `GetFindings` 動作新增到 `AmazonDetectiveFullAccess` 和 `AmazonDetectiveInvestigatorAccess` 政策中。 透過此類動作，可從 Detective 內部取得 Security Hub 調查結果。	2023 年 5 月 16 日
AmazonDetectiveOrganizationsAccess – 新政策	Detective 新增了 `AmazonDetectiveOrganizationsAccess` 政策。 此政策授予在組織內啟用和管理 Detective 的許可	2023 年 3 月 2 日
AmazonDetectiveMemberAccess – 新政策	Detective 新增了 `AmazonDetectiveMemberAccess` 政策。	2023 年 1 月 17 日

變更	描述	日期
	此政策會向成員提供 Detective 的存取，以及主控台 UI 依存關系的特定範圍存取。	
AmazonDetectiveFullAccess：現有政策的更新	Detective 在`AmazonDetectiveFullAccess` 政策中加入了 GuardDuty `GetFindings` 動作。 這些動作允許從 Detective 內部獲取 GuardDuty 調查結果。	2023 年 1 月 17 日
AmazonDetectiveInvestigatorAccess – 新政策	Detective 新增了 `AmazonDetectiveInvestigatorAccess` 政策。 透過此類政策，主體可在 Detective 中進行調查。	2023 年 1 月 17 日
AmazonDetectiveServiceLinkedRole – 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 管理政策的變更。	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，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

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 使用名為的服務連結角色 AWSServiceRoleForDetective— 允許 Detective 代表您存取 AWS Organizations 資訊。

服 AWSServiceRoleForDetective 務連結角色會信任下列服務擔任該角色：

- `detective.amazonaws.com`

AWSServiceRoleForDetective 服務連結角色使用受管理的策略`AmazonDetectiveServiceLinkedRolePolicy`。

如需`AmazonDetectiveServiceLinkedRolePolicy`政策更新的詳細資訊，請參閱 Amazon Detective 更新 AWS 受管政策。如需有關此原則變更的自動警示，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 Management Console、或 AWS API 中指定組織的 Detective 管理員帳戶時 AWS CLI，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。

若要刪除使用的 Detective 資源 AWSServiceRoleForDetective

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 主控台或 AWS API 刪除 AWSServiceRoleForDetective服務連結角色。 AWS CLI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的困難，請參閱 IAM 使用者指南中的 IAM 疑難排解主題。

我未獲授權，不得在 Detective 中執行動作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是提供您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。

我沒有授權執行 iam：PassRole

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 允許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 沒有將角色傳遞至該服務的許可。

```
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。

我想允許我 AWS 帳號以外的人員存取我的 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。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。

- 若要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)。
- 若要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 角色與資源型政策的差異。

在 Amazon Detective 中記錄和監控

Amazon Detective 被集成 AWS CloudTrail。 CloudTrail 將 Detective 的所有 API 呼叫擷取為事件。

有關如何使用 Detective CloudTrail 記錄的詳細資訊，請參閱the section called “記錄 Detective API 呼叫 CloudTrail”。

Amazon Detective 的合規驗證

Amazon Detective 在 AWS 保證計劃的範圍內。如需詳細資訊，請參閱健康資訊信任聯盟公共安全架構 (HITRUST) CSF 。

如需特定合規計劃範圍的 AWS 服務清單，請參閱合規計劃 AWS 服務範圍內的合規計。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載 AWS Artifact 中的報告。

AWS 提供下列資源以協助遵循法規：

- 安全與合規快速入門指南：這些部署指南討論架構考量，並提供在 AWS上部署以安全及合規為重心之基準環境的步驟。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

Amazon Detective 中的彈性

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎設施之外，Detective 還利用 Amazon DynamoDB 和亞馬遜簡單儲存服務 (Amazon S3) 中內建的彈性。

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

作為一項託管服務，Amazon Detective; 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以透過網路使用 AWS 已發佈的 API 呼叫來存取 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。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

Amazon 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。

管理員帳戶的最佳實務

邀請成員帳戶加入您的行為圖表時，僅會邀請您監督的帳戶。

限制存取行為圖表。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咨詢。

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 AWS 送邀請之管理員帳戶的帳戶識別碼。確認您知道該帳戶的所屬資訊，以及邀請帳戶有合法理由監控您的安全資料。

預測和監控 Amazon 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 還支持 AWS CloudTrail 日誌記錄。

目錄

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 Amazon 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。

監控行為圖表的用量和成本 (管理員帳戶)

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 Management Console。然後前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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 天內從 Detective 核心來源 (CloudTrail 記錄檔、VPC 流程記錄和 GuardDuty 發現項目) 擷取的資料量。

EKS 稽核日誌

EKS 稽核日誌面板會顯示過去 30 天從 EKS 稽核日誌來源擷取的資料量。只有在行為圖表啟用 EKS 稽核日誌後，才能使用此來源套件的面板。

監控跨行為圖表 (成員帳戶) 的用量和成本

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 Management Console。然後前往 https://console.aws.amazon.com/detective/ 開啟 Detective 主控台。
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。所得即爲帳戶的預計 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。

使用記錄 Amazon Detective API 呼叫 AWS CloudTrail

Detective 集成了一種服務 AWS CloudTrail，該服務提供了用戶，角色或 Detective AWS 服務所採取的行動記錄。 CloudTrail 將 Detective 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Detective 主控台進行的呼叫，以及針對 Detective API 操作的程式碼呼叫。

- 如果您建立追蹤，您可以啟用持續傳遞 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Detective 事件。
- 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail主控台中最近的事件。

您可以使用所收集的 CloudTrail資訊來判斷下列項目：

- 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，請參閱使AWS CloudTrail 用者指南。

Detective 資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當活動在 Detective 中發生時，該活動會與其他 AWS 服務 CloudTrail 事件一起記錄在事件歷史記錄中。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 CloudTrail 件記錄的事件。

如需您 AWS 帳戶中持續記錄的事件 (包括 Detective 活動)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 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。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您也可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料，並採取行動。

如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

CloudTrail 記錄所有 Detective 操作，這些操作記錄在 Detective API 參考中。

例如，呼叫`CreateMembers`、`AcceptInvitation`、和`DeleteMembers`作業會在 CloudTrail 記錄檔中產生項目。

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：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 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
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

了解 Detective 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。

事件代表來自任何來源的單一請求。事件包括所請求動作的相關資訊、動作的日期和時間、請求參數等。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此條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 記錄項目。

```
{
      "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
      "Username": "JaneRoe",
      "EventTime": 1571956406.0,
```

```
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS: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\":\"AROAJZARKEP6WKJ5JHSUS
\",\"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	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。 每天 15 TB 反映正常資料量和資料量峰值。 若要重新啟用資料擷取，您必須連絡 AWS Support。

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

您可以將標籤指派給您的行為圖表。然後，您可以使用 IAM 政策中的標籤值來管理對 Detective 中行為圖表功能的存取。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 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。

檢視行為圖表的標籤 (主控台)

您可以從一般頁面管理行為圖表的標籤。

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)。

列出行為圖表的標籤 (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。

要獲取行為圖的標籤列表（Detective API， AWS CLI）

- Detective API：使用 `ListTagsForResource` 操作。您必須提供行為圖表的 ARN。
- 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
```

將標籤新增到行為圖表 (主控台)

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。

將標籤添加到行為圖（Detective API， AWS CLI）

您可以使用 Detective API 或 AWS CLI 將標籤值新增至您的行為圖。

若要將標籤新增至行為圖 (Detective API， AWS CLI)

- Detective API：使用 TagResource 操作。您可以提供行為圖表 ARN 和要新增的標籤值。
- 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"}'
```

從行為圖表中移除標籤 (主控台)

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。

從行為圖表中刪除標籤 (Detective API， AWS CLI)

您可以使用 Detective API 或從行為圖中移除標籤值。 AWS CLI

要從行為圖中刪除標籤（Detective API， AWS CLI）

- Detective API：使用 UntagResource 操作。您可以提供行為圖表 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)

您可以透過 AWS Management Console停用 Amazon Detective。

要禁用 Amazon Detective（控制台）

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. 選擇禁用 Amazon Detective.

禁用 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。

要禁用 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
```

禁用跨區域的 Detective（開啟 Python 腳本 GitHub）

Detective 提供中的開放原始碼 GitHub 指令碼，可讓您針對指定的區域清單中的管理員帳戶停用 Detective。

如需有關如何設定和使用 GitHub 指令集的資訊，請參閱the section called “Amazon Detective Python 腳本”。

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。

- 最新文件更新：2024 年 5 月 15 日

變更	描述	日期
新的安全湖原始碼版本	除了來源版本 1 (OCSF 1.0.0-rc.2) 之外，Detective 現在會針對 Detective 支援的安全湖來源擷取來源 2 (OCSF 1.1.0) 的資料。	2024年5月15日
新的安全湖泊記錄來源	您可以使用 Detective 與安全湖整合，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已合併到 Amazon Detective 使用者指南中。Amazon Detective 管理指南將於 2024 年 5 月 08 日結束標準支持。	2024年4月15日
增加了對 Amazon GuardDuty 調查結果	Detective 現在提供下列GuardDuty 執行階段監視尋找項目類型的支援。`Execution:Runtime/MaliciousFileExecuted` `Execution:Runtime/SuspiciousTool` `DefenseEvasion:Runtime/PtraceAntiDeb`	2024年4月5 日

	ugging Execution :Runtime/Suspiciou sCommand DefenseEv asion:Runtime/Susp iciousCommand	
刪除了 Amazon GuardDuty 會員要求	您不再需要成為 GuardDuty 客戶即可啟用 Amazon Detective。在 GuardDuty 啟用 Detective 功能之前，已在您的帳戶中啟用 48 小時的要求已被移除。	2024年2月2日
增加了對 Amazon GuardDuty 調查結果	Detective 將 GuardDuty EC2 執行階段監控尋找類型的支援延伸至 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] 頁面針對您要調查的特定資源執行 Detective 調查。Detect ive 會根據在調查結果和調查結果群組中的活動建議資源。Detective 測調查可讓您調查具有入侵指標的 IAM 使用者和 IAM 角色，以協助您判斷資源是否涉及安全事件。	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 測調查可讓您調查具有入侵指標的 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 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）區域添加到可用 Detective 與 Security Lake 整合的 AWS 區域列表中。	2023 年 12 月 8 日
新功能	Detective 調查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
新功能	根據預設，Detective 會自動為調查結果群組產生調查結果群組摘要 (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
新功能	Detective 與 Security Lake 整合可讓您查詢和擷取 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 虛擬私有雲端 (Amazon VPC) 流程日誌收集日誌和事件。	2023 年 11 月 26 日

已將受管政策資訊新增至安全性章節	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
檢視調查結果概觀	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
Amazon Detective 端點和配額	Detective 現在可於以色列 (特拉維夫) 區域使用。	2023 年 8 月 25 日
增強調查結果群組視覺化	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
增強調查結果群組	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
增加了對 Amazon GuardDuty Lambda 保護的	Detective 現在為 GuardDuty Lambda 保護提供支援。	2023 年 5 月 26 日
將 AWS 安全性發現項目新增為新的選用資料來源套件。	Detective 現在將 AWS 安全性發現作為選用的資料來源套件提供。透過選用的資料來源套件，Detective 可以從 Security Hub 擷取資料，並將該資料新增至您的行為圖表。	2023 年 5 月 16 日
增加了對 Amazon GuardDuty EKS 運行時監控查找類型的支持	Detective 現在提供 GuardDuty EKS 執行階段監視尋找類型的支援。	2023 年 5 月 3 日
增加了對 Amazon GuardDuty RDS 保護查找類型的支持	Detective 現在為 GuardDuty RDS 保護查找類型提供支持。	2023 年 4 月 20 日

增加了對其他 Amazon GuardDuty 查找類型的支持	Detective 現在會提供下列其他 GuardDuty 尋找類型的設定檔：`DefenseEvasion: EC2UnusualDNSResolver` `DefenseEvasion: EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	2023 年 4 月 12 日
在 Detective 主控台中新增了新主控台面板，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。	Detective 提供受管政策，以安全選擇您需要的許可。	2023 年 4 月 3 日
顯示 EKS 叢集的 VPC 流量	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
調查結果群組現在包含 Detective 行為圖表的動態視覺化呈現	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
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。	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

為 EKS Amazon EKS 工作負載新增了整體 VPC 流量	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
已將受管政策資訊新增至安全性章節	Detective 現在支持通過 AmazonDetectiveFullAccess 策略 GuardDuty 獲取調查結果操作。安全性章節現在提供下列針對 Detective 的新受管理原則的詳細資訊： AmazonDetectiveMemberAccess 和 AmazonDetectiveInvestigatorAccess。	2023 年 1 月 17 日
新增了資料保留	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
在摘要頁面上新增了調整範圍時間的選項。	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
搜尋調查結果或實體	Detective 現在提供不區分大小寫的搜尋。	2022 年 10 月 3 日
新增了設置範圍時間戳記的功能	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

新增了與調查結果群組相關的術語	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
已新增與 Amazon EKS 稽核日誌相關聯的新設定檔	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
添加了新選用的資料來源	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
適用於 Detective 的新服務連結角色和受管政策	Detective 現在有服務連結角色，即 `AWSServiceRoleForDetective` 。服務連結角色用於代表您存取組織資料。角色使用新 `AmazonDetectiveServiceLinkedRolePolicy` 受管政策。	2021 年 12 月 16 日
增加了集成 AWS Organizations	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

使用調查結果概觀取代調查結果設定檔	調查結果設定檔包含分析相關資源活動的視覺化。新的發現項目概觀包含從中擷取的尋找項目詳細資訊 GuardDuty，以及相關實體的清單。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
移除支援 GuardDuty 尋找類型的限制	Detective 不再限於選定的 GuardDuty 尋找類型集。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
從相關調查結果設定檔面板至調查結果詳細資訊的連結	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 小號項目允許您將 AWS 內容發送到 Splunk。該項目現在允許您添加 Detective URL 以導航到配置文件以 GuardDuty 查找結果。	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
新增使用者、角色和角色工作階段的資源互動標籤	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
更新了行為圖表資料量的配額值	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

在 Python 指令碼選項中添加了標籤值	當您使用 Detective Python 指令碼 (`enableDetective.py`) 啟用 Detective 後，您可以將標籤指派給行為圖表。	2021 年 5 月 19 日
增加了通過資料量檢查的成員帳戶的自動啟用	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
已將受管政策資訊新增至安全性章節	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 `AmazonDetectiveFullAccess`。	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
增加了對其他 Amazon GuardDuty 查找類型的支持	Detective 現在提供下列其他 GuardDuty 尋找類型的設定檔：`CredentialAccess:IAMUser/AnomalousBehavior` `DefenseEvasion:IAMUser/AnomalousBehavior` `Discovery:IAMUser/AnomalousBehavior` ,`Exfiltration:IAMUser/AnomalousBehavior` ,,`Impact:IAMUser/AnomalousBehavior` ,`InitialAccess:IAMUser/AnomalousBehavior` ,,`Persistence:IAMUser/AnomalousBehavior` ,`PrivilegeEscalation:IAMUser/AnomalousBehavior`	2021 年 3 月 29 日

增加了 AWS GovCloud (US) 區域的差異	Detective 現在可在 AWS GovCloud (US) 區域中使用。在 AWS GovCloud （美國東部）和 AWS GovCloud （美國西部），Detective 不會向會員帳戶發送邀請電子郵件。Detective 也不會自動移除 AWS中關閉的成員帳戶。	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
增加了對其他 Amazon GuardDuty 查找類型的支持	Detective 現在會提供下列其他 GuardDuty 尋找類型的設定檔：`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 轉向 Detective GuardDuty 的選項	在中 GuardDuty，「Detective 中調查」選項會從「動作」功能表移至「尋找項目詳細資訊」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 搜尋發現項目、 AWS 角色、使用 AWS 者和 EC2 執行個體。	2020 年 8 月 27 日

從設定檔面板連結至其他主控台	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
VPC 流程資料的活動詳細資訊	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
成員帳戶現在可以查看他們的用量和預計成本	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
現在每個帳戶 (而非每個行為圖表) 均可免費試用	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
新的開源 Python 腳本 GitHub	的新amazon-detective-multiaccount-scripts存放庫 GitHub 提供開放原始碼 Python 指令碼，您可以使用這些指令碼來管理跨區域的行為圖表。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

《Detective 行政指南》的內容現已整合到 Detective 使用者指南中。

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。